THE HAGUE UNIVERSITY OF APPLIED SCIENCES

The transatlantic data transfer - the case of EU - U.S. relations

Date: 30.05.2014

"To what extent does the transatlantic Safe Harbor Agreement between the U.S. and the EU ensure the protection of EU citizens' personal data under Directive 95/46/EC?"

Tatjana Arnold

11029587

Supervisor: **Mr. Nixon**

Second Marker: **Mr. Rawal**

Executive Summary

The transatlantic data transfer between the U.S. and the EU would have been extremely complex and expensive if the European Commission together with the U.S. Department of Commerce had not originated the Safe Harbor agreement in 2000. As recently as the beginning of 2014 the European Parliament, especially with input of the LIBE COM raised its concern about EU-U.S. data protection agreements, resulting in the call for the suspension of the Safe Harbor framework (APCO Forum, n.d.). The Safe Harbor deal enables U.S. organizations and companies to access personal data processed and stored in the EU in case they apply to "adequate" standards which mirror the ones of the EU. It was invented to build a bridge between the diverse EU - U.S. data protection approaches and to allow a continuous transatlantic data transfer. By the end of 2013, over 4.000 companies have joined the scheme, including Microsoft, Facebook and Amazon. This paper analyses the effectiveness and reliability of the scheme and tries to find out if the programme is able to ensure EU citizens' personal data effectively.

In Europe, data protection rules are based on Article 8 of the Charter of Fundamental Rights, Convention 108 and the Data Protection Directive of 1995. Directive 95/46/EC was established to further harmonize the data protection laws of its Member States and outlines the collection, storage, processing, use, and disclosure of an individual's personal data. The "Adequacy Decision" of this Directive determines whether a third country can provide an adequate level of data protection, similar to the one of the EU. With the expertise of supervisory authorities, the EU decided that the U.S. legal regime has profound shortcomings and hence the country did not receive the "adequacy" status. The EU sees privacy and data protection as a fundamental right while the view of the U.S. includes the presumption that privacy is a commodity subject to the market.

The varied approaches of privacy and data protection standards of the EU and the U.S. combined with an ongoing debate about the reliability of the scheme and the mass surveillance activities of U.S. secret services resulted in an active discussion if the programme should be suspended or rather re-negotiated.

This paper reveals that three of the seven principles it is based on are violated on regular basis (the Principle of Notice, Choice, and Enforcement). Overall the scheme is utterly criticized because of its lack of transparency, the lack of enforcement bodies and actions and the obsolescence of the existing Data Protection Directive. Furthermore it has been identified that the actions of the U.S secret services violate the Principle of Proportionality of the EU Directive. The Federal Trade Commission on the other hand argues that "consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues" (Brill, 2013). The think tank

Future of Privacy points out that the EU should not limit or suspend the programme, because it would rather weaken EU citizens' personal privacy. They conclude that the elimination of the programme would not prevent the NSA from accessing the data of EU citizens.

In order to improve the existing programme, the report identified the following recommendations for the European Commission. The EC is, until now, the only institution which has the authorization to suspend, limit or reverse the adequacy decision and therefore also the Safe Harbor agreement.

First, the Directive has to be renewed, as the existing legislation is clearly out-of-date and does not face the challenges of the 21st century. Furthermore the definition of adequacy needs to be revised as the present definition is unclear and leads to misinterpretations. Thirdly, the EC should be informed when a company needed to apply to the exceptions of the principles in order to meet national security, public interest or law enforcement requirements. Moreover, the self-certification mechanism should be suspended, as it has been violated regularly. One next step to protect the personal data of EU citizens is more transparency as this has been criticized extensively since its foundation in 2000. Non-members should be identified instantly and certified companies should always state their privacy policies on their website. Moreover, strong enforcement bodies and actions shall be installed, as a lot of companies had made false claims about their compliance with the agreement. Those companies should be suspended immediately. Another method of improving the system is to install warning systems which will inform the EC if new government regulations have been installed in the U.S. that might affect compliance with the seven Safe Harbor Principles.

Nevertheless, the increasing debate about privacy can also be seen as a debate for a change and a time where the EU together with the U.S. can form a long-term solution in order to allow a transatlantic data transfer that "both protects privacy and promotes international economic growth" (Wolf, 2014, p.32). These recommendations may help to foster privacy principles throughout the whole world and may be a starting point of securing EU citizens’ data more effectively.

Table of Contents

1. Introduction

Whenever an individual places an order online, books his next vacation or joins a social network, he divulges his personal data to a service provider and is often unaware that these daily activities are subject to international data transfers across national frontiers. With every new membership card, every new download of an app or new friendship on facebook, the individual transfers his personal data to so-called data-controllers (European Commission Justice, 2013) which are now capable of accessing every single detail the individual entrusted him with. In an age where a huge number of individuals share personal information and interests on social networks, we sometimes reveal much more of ourselves than we are aware of. More and more frequently we sell private information such as hobbies, political affiliation or favourite movies to search engines, social networks and other firms without knowing what actually happens to the data we disclose lightheaded. Through the interconnectivity of the computer technology in combination with the ubiquity of the Internet, those firms are capable of spreading personal data anywhere in the whole world at all times. A problem emerges as soon as this transfer is being violated. If data protection laws are being ignored, e.g. when data-controllers illegally sell collected data or when employees divulge this valuable source to third parties, the right to privacy is at stake.

In particular, since Edward Snowden's revelations about mass surveillance programmes of the U.S. secret services in June 2013, the right to privacy has been discussed heavily. Citizens together with policy-makers and journalists all over the globe are calling for new legislative frameworks to protect personal data. Moreover bilateral agreements between the EU and the U.S. are at risk because of the mass-surveillance programmes of the NSA and other secret services. One of these programmes is called the Safe Harbor scheme. The agreement created a mechanism which allows the "free transfer of personal data from EU Member States to companies in the U.S." (European Commission, 2013) if they signed up to a set of rules to meet European Data Protection Standards. The agreement has been found faulty since its beginning in 2000 and has to face even more criticism now, since the large-scale collection of personal information of the U.S. became public. An internal debate within the European Union emerged which opens up many questions about the effectiveness and reliability of "Safe Harbor".

This paper is going to analyse to what extent the Safe Harbor agreement is able to secure European citizens' data under the rules of the ECHR, Convention 108 and specifically under the Data Protection Directive 95/46/EC. To answer this question it is necessary to first describe the context and literature of resent criticism, followed by an introduction to the Data Protection Standards of the European Union with special emphasis on the Privacy Directive (=Directive 95/46/EC). In order to get an insight of the differences of two completely diverse

data protection approaches (EU vs. U.S.), the report is focusing on the legal basis of U.S. legislation that is of great importance for non-U.S. citizens. Afterwards the discrepancies of EU and U.S. law are going to be identified. After the legislative framework has been described and defined, the paper continues to focus on the features and the functioning of the Safe Harbor Programme, including a brief description of its history and the seven basic principles it is based on. The next point focuses on well-established criticism of the scheme including existing violations of the programme. After all facts have been specifically outlined the research question will be answered with regard to the importance of recent mass surveillance actions taken by U.S. secret services.

2. Acronyms

APEC:	Asia Pacific Economic Forum
DPAs:	European Data Protection Authorities
e.g.:	for example
EC:	European Commission
ECHR:	European Convention for the Protection of Human Rights and Fundamental Freedoms
EEA:	European Economic Area
EP:	European Parliament
EU:	European Union
FAQs:	Frequently Asked Questions
FISA:	Foreign Intelligence Surveillance Act (1978)
FTC:	US Federal Trade Commission
ITA:	US International Trade Administration
LIBE COM:	Committee for Civil Liberties, Justice and Home Affairs
MS:	Member States of the European Union
NSA:	National Security Agency
OECD:	The Organization for Economic Cooperation and Development
S&D:	The Progressive Alliance of Socialists and Democrats
U.S.:	United States of America

3. Literature Review

According to current information the Safe Harbor agreement could be at risk because the trust of EU citizens in U.S. data transfers has crumbled, also because the NSA, combined with other secret services, has accessed the personal data of EU citizens. Edward Snowden, computer specialist and former contractor for the NSA revealed that also Internet giants, such as Google, Apple or Facebook have accessed personal data of EU citizens. Peter Hustinx is calling for an end of the so-called "wild west-mentality" of the U.S. secret services and firms [PR Online, 2014). In June 2013, The Washington Post and The Guardian published that the Verizon telephone company had to hand over details of all US [...] international phone calls to the NSA, in compliance with the Patriot Act (Bowden, 2013, p.15).

This chapter summarizes the ideas of the most important literature that has been used for this paper. It formulates their strengths and weaknesses and tries to find a similarities and differences in their view on the Safe Harbor programme and its effectiveness.

The eBook "The Safe-Harbor agreement between the United States and Europe" by the two researchers, Duncon and Brown described in what way the American view of privacy differs from the one of Europeans and identifies the main characteristics of U.S. law. It was mainly used to get background information about the Safe Harbor scheme, especially why it was invented and provided detailed information about the fundamental seven principles of the scheme which are going to be explained later in this paper.

The amendments of the Foreign Intelligence Surveillance Act (Fisa) of 2008 "allow for the collection of communications where at least one end of the communication is a non-US person" (The Guardian, 2014). That means that even U.S. law allows NSA surveillance actions against EU citizens. Former NSA Director Hayden explained that "the US enjoys a "home field advantage" of unlimited access to foreign communications routed via US territory, or foreign data stored there" (Bowden *et al.*, 2013, p.22). Claude Moraes, S&D rapporteur of the EP examination of the NSA surveillance affair, indicates that "the existing agreement does not offer EU citizens any protection against either Foreign Intelligence Surveillance Act or Patriot Act in the US" (Neal, 2013). That is why the U.S. legislation has to be examined profoundly. The report is going to focus on the rules for non-U.S. citizens in U.S. law.

Directive 95/46/EC needed to be examined in order to analyse the Data Protection standards of the European Union. As the term "personal data" is used frequently in this thesis, the Directive was also used to provide a clear definition of the exact meaning. Broadly, personal

data can be data such as name, address, telephone number, credit card number or legal status. Art 2(2) defines the term as followed:

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (Art. 2(2) Directive 95/46/EC)*

Peter J. Hustinx's paper about the interaction between data protection authorities and national human rights could primarily be used because of Hustinx's extensive knowledge about European data protection.

The Safe Harbor programme had been critically reviewed by the European Commission in November 2013 and resulted in a report "on the functioning of the Safe Harbor from the perspective of EU citizens and companies established in the EU" (EC, 2013). The report includes findings of the EU-U.S. Privacy Group (2009), an ad-hoc EU-U.S. Working Group, and on a study of an independent contractor (2008). The report also builds up on previous Safe Harbor assessment reports of the EC (2002 and 2004) and adds special in-depth knowledge whether the requirements of the Safe Harbor can be still guaranteed. The main outcome of the study was that the programme has a number of crucial weaknesses, which diminish its reliability: It lacks transparency of privacy policies of participating companies and organizations and a number of U.S. companies do not apply to the seven privacy principles it is based on. Furthermore, the enforcement by the public authorities of the U.S. is claimed to be too weak. Combined with detailed studies from the reliable management consulting firm Galexia about the effectiveness of the Programme in 2013 and 2008, actual instabilities and strengths can be identified. In this context the question aroused whether data-controllers are even capable of keeping European citizens' data safe.

A different view of the effectiveness of the scheme was examined by the American think tank Future of Privacy. Internet privacy experts and other leading figures from academia, law, the industry and advocacy groups manage the company, adding expert advice to the topic. The report of 2013 "*The US-EU Safe Harbor - An Analysis of the Framework's Effectiveness in Protecting Personal Privacy"* includes interviews of company executives, which are listed in the programme. It points out that the EU should not limit or suspend Safe Harbor, because it would rather weaken EU citizen's personal privacy. They conclude that the elimination of the programme would not "prevent the NSA from accessing EU citizen's data". A number of EU countries, including Britain, see Safe Harbor as a useful mechanism by which to boost European regulation with tough US jurisdiction" (Oltermann, 2013). Julie Brill, the Commissioner of the FTC underlines that the programme is "a very effective tool for protecting the privacy of EU consumers [...] and should not be suspended" (Gardner, 2013).

The FTC argues that it would be much harder to protect EU consumers' privacy and "Safe Harbor has been an effective solution, not the problem" (FTC, 2014, p.4).

The article *"Delusions of adequacy? Examining the case for finding the United States adequate for cross-border EU-U.S. data transfers"* by Christopher Wolf identifies the theoretical and practical functioning of the EU adequacy decision of Directive 95/46/EC for the transatlantic data transfer and tries to outline the similarities and differences of the two privacy approaches of the U.S. and the EU. It reviews in how far US privacy law can be "deemed adequate under the EU privacy framework" (Wolf, 2014, p.1). Christopher Wolf concludes that the U.S. should have, despite legal shortcomings, received the statute of "adequacy" from the EC.

Viviane Reding, Vice President of the EC also calls for a review of the programme by the end of 2014 and marked it as a "loophole" that "may not be safe at all (Future of Privacy, 2013, p.10). In summer 2013, Dr. Imke Sommer, the current chair of the Conference of Federal and State Data Protection Commissioners commented on the affair and said that it is very likely that the principles of the Safe Harbor agreement combined with the principles of the EU Data Protection Directive are being violated.

4. Methodology

The aim of this chapter is to focus on different research approaches which were necessary in order to answer the research question. This chapter identifies the advantages and disadvantages of each method and explains why specific research methods could not be included in this project.

This thesis is a mix of qualitative and quantitative research methods. However, its focus lies on quality rather than on quantity. In order to fully answer the research question it was necessary to use a qualitative research approach which is rich in details and descriptive.

The majority of the conducted analysis is based on primary data retrieved from policy documents of the U.S. Department of State, the European Commission and the European Parliament. Findings and studies of think tanks, such as Future of Privacy, the French Research Centre for Computer and Law CRID, or consultancy firms such as Galexia were additionally reviewed. These sources can often provide data charts and therefore lead to quantitative information. They played an important role in answering the research question as they provide objective opinions and advise in this field. In addition to that, deputy reports, such as the one of Peter Hustinx, European Data Protection Supervisor and former president of the Dutch DPA could provide reliable data about the topic. Furthermore official letters from the FTC to the EC have been analysed such as the one from Julie Brill, the FTC Commissioner and the letter from Edith Ramirez, the Chairwoman of FTC to Viviane Reding.

This paper does not solely take into account governmental positions or the beliefs and opinions of supra-national institutions, but also personal opinions and interpretations. That is why this paper tries to include the voices of professors, such as Dr. Andreas Busch, chair of comparative political economy in Göttingen, privacy advocates like Caspar Bowden, or researchers at Universities such as Jeffrey Layne Blevins, Duncan Brown, or P.J. Murray. They add their opinion and knowledge through e.g. academic journals or articles.

As this topic is up to date and heavily discussed since Edward Snowden's revelations in June 2013, the paper also reviews articles from a number of well-known and unbiased international newspapers, such as The Guardian, The Inquirer, PCWorld, Heise, or Business Insider.

Due to the fact that the paper puts special emphasis on the legislative framework of Data Protection standards in the EU and the U.S., it was necessary to review Directives (95/46/EC), the ECHR and Conventions. Amendments and adjustments of already existing legislation, such as the amendment of the FISA Act needed to be analysed in order to detect the effects of U.S. legislation on EU citizens.

In order to gain an in-depth knowledge of the topic and to comprehend the point of view of experts, secondary sources in the form of literature have been reviewed. Books were used as qualitative research methods. The eBook that has been intensively examined is "*Information Privacy (Concepts & Applications)* by Kylan Courtney or the eBook from Andreas Busch *"The regulation of transborder data traffic: Disputes across the Atlantic".*

Furthermore, data for the report has been collected through direct contact with various parties including an interview with the data protection expert Christoph Schäfer. He is a data protection advisor and trainer and works as data protection officer at GDDcert. Moreover he is employed as TeleTrust Information Security Professional. A face-to-face interview was not possible and therefore a telephone interview was conducted.

Initially the report should include the expertise of deputies of the EP, including for example an interview with Jan Philipp Albrecht. As a member of the Greens Party and the Com LIBE he has the insight in current debates about data protection and has worked on the LIBE report together with Claude Moraes. He is one of the deputies in the EP who constantly tried to address the US privacy laws and who is also calling for stricter legislation in Europe. However, due to the upcoming European elections he did not have the time to respond. His co-worker Sonia Alfano, the Italian LIBE Com member and a Christian Democrat as well as Cornelia Ernst were also contacted but did not reply at all. The Electronic Privacy Center EPIC was also contacted via email, however, also they did not reply to my questions. It was also intended to include the expertise and the know-how of FTC employees, including the opinion of Jessica Rich, Director of the Bureau of Consumer Protection and Hugh Stevenson, Deputy Director of the Office of International Affairs at FTC. Despite my great effort to contact those experts I received helpful links and information to conclude this paper, however, an interview could not take place due to the lack of time on the part of those people.

In the beginning of writing this thesis it had been under consideration to conduct a survey. The survey could have been handed out to citizens of the EU and should have asked for their knowledge of data protection, EU legislation, and the effectiveness of the Safe Harbor program. In my opinion, this survey would not lead to reliable results. To answer questions about the Safe Harbor program it is necessary to have comprehensive and in-depth knowledge about the topic. A survey with a high number of participants with hardly any expertise would not have been effective in order to answer the research question. The point of this thesis is rather to gather qualitative information than to get feedback from a large number of survey participants.

5. Results

5.1. The data protection principles of the European Union and its member states

This chapter tries to identify the main data protection principles of the European Union and explains how the issue of privacy and data protection became part of the existing EU legislation. In order to answer the research question it was necessary to know the basics of the Data Protection Directive, its advantages and critical points and to focus furthermore on the Adequacy Decision.

5.1.1. Data Protection as a fundamental European right

The initial phase of data protection started with the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1953 and especially with the implementation of Article 8. As the treaty came into force in the beginning of the 50s, a time where automatic data processing was still unknown, the issue of data protection was hardly as important as it is today (Bussche & Stamm, 2013, p.1). Art. 8 demonstrates that "[e]veryone has the right to respect for his private and family life, his home and his correspondence" (European Convention on Human Rights, n.d.). The article also outlines specific circumstances and conditions under which these rights can be restricted, such as national security or public health concerns. Even though the right to respect family and private life was already achieved, a general right related to data protection was not even considered at that time. Because of technological progresses, globalisation forces, and an "evolving civil liberties awareness in society" (Bussche & Stamm, 2013, p.1), data protection gained more and more importance. After Germany implemented the world's first data protection act in 1970, the Council of Europe followed the German archetype and passed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also known under Convention 108) on 01 January 1981 in Strasbourg (Bussche & Stamm, 2013, p.2). Convention 108, signed by 47 member states, including all 28 members of the EU (European Union Agency for Fundamental Rights, 2013, p.14) is, until today, the only international instrument which is legally binding in the field of data privacy. It aims for a greater unification of its members based on human rights and fundamental freedoms. The principles are still effective today and shall be ensured by all members of the Council. Art. 5 outlines those principles as followed (Council of Europe, 1981):

Article 5 - Quality of data

Personal data undergoing automatic processing shall be:

1. obtained and processed fairly and lawfully;

2. stored for specific and legitimate purposes and not used in a way incompatible with those purposes;
3. adequate, relevant and not excessive in relation to the purposes for which they are stored;
4. accurate and, where necessary, kept up to date;
5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those date are stored.

The increasing data transfer across borders and between states made it critical to secure the right to privacy with regard to automatic processing of personal data without making a difference of an individual's residency or nationality (Electronic Privacy Center, n.d.). In order to safeguard personal data in the process of data sharing, restrictions have been imposed on states where its national legal regulation does not provide equivalent protection (European Union Agency for Fundamental Rights, 2013, p.16). Another development followed in 2000, when the EU Charter of Fundamental Rights was adopted. It was predominantly based on the ECHR. Article 8 was created as an addition to the right to respect for private and family life (Art. 7) and recognizes the right to the protection of personal data (Hustinx, n.d.). When the Lisbon Treaty came into force in 2009, the Charter turned into a legally binding document. According to Hustinx this was the time where the nature of data protection was transformed into a fundamental right. However, in this decade it was tremendously important for Europe to react to the perpetual evolving Information Society. On these grounds, harmonisation and stability among national laws was irresistibly required. The EU needed to adapt to a changing society, which was leading to the creation of the Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Hustinx, n.d.).

5.1.2. The Data Protection Principles under Directive 95/46/EC

Free movements of goods, services, capital, and people within the market also opened up the discussion about the free flow of data. When the World Wide Web emerged into existence in the 1990s, the speed and facilitation of how data can be transferred across frontiers increased the concern of EU-MS that EU citizen's privacy might be at risk. Therefore it was necessary to focus on a uniform level of data protection for all MS, in particular in cases where nation states already followed their own data protection rules. One of the main aims of the Data Protection Directive which was implemented in October 1995 by the Council and the European Parliament (European Union Agency for Fundamental Rights, 2013, p.18) was to expand the principles of Convention 108. In a time where data flows between countries all over the globe "became instrumental in the development of nearly all areas of

commerce" (Future of Privacy, 2013), the regulatory framework tries to find "a balance between a high level of protection for the privacy of individuals and the free movement of personal data [...]" (European Union, 2011). Harmonization and the aim "to decrease transaction costs for entities that operate across borders" (Fromholz, 2008, p. 462) were the greatest reasons to create a Directive which guaranteed a uniform legal basis for all MS.

According to Kylan Courtney seven global principles already existed in 1980 when the OECD wrote "Recommendations of the Council Concerning Guidelines Governing Protection of Privacy and Trans-Border Flows of Personal Data". Those principles are largely mirrored in the Data Protection Directive of the EU. The OECD rules were non-binding. Therefore transferring them into an EU Directive made them accountable and just then effective. The U.S. also ratified these rules, which include the first seven principles of the OECD (Courtney, 2012, p.40f.):

1. *Notice:* data subjects should be given notice when their data is being collected
2. *Purpose:* data should only be used for the purpose stated and not for any other purposes
3. *Consent:* data should not be disclosed without the data subject's consent
4. *Security:* collected data should be kept secure from any potential abuses
5. *Disclosure:* data subjects should be informed as to who is collecting their data
6. *Access:* data subjects should be allowed to access their data and make corrections to any inaccurate data
7. *Accountability:* data subjects should have a method available to them to hold data collectors accountable for following the above principles

Another three main principles can be determined: (1) legitimate purpose, (2) proportionality and (3) transparency. The Directive clearly outlines that "data should not be processed at all, except when certain conditions are met" (Courtney, 2012, p.42). Art. 6 (b) underlines that if data is collected for "specific, explicit and legitimate purposes [it should not be] further processed in a way incompatible with those purposes" (European Parliament and European Council, 1995). However, the Article also legitimates exceptions to the rule, e.g. if data is processed for statistical, historical or scientific purposes. Exceptions can take place in cases where MS are able to provide adequate safety for privacy. However, total legitimacy is only given if also Art. 7 can be applied correctly.

The proportionality principle comes into force through Art. 6 (c) which states that collected personal data shall be "adequate, relevant, and not excessive in relation to the purposes for which they are collected and /or further processed (European Parliament & European Council, 1995).

The principle of transparency is based on Art. 10 and 11. It includes the right for the individual to be informed in case his personal information is being processed. The Directive thereby includes that "the controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair" (Courtney, 2012, p.42). Art. 28 therefore created independent supervisory authorities, which had to be established by each MS. The Directive entrusts them with the task of monitoring and checking each MS for compliance. If data protection rules have been violated, the authority can answer with legal proceedings. The article 29 working party, one of the most important data protection advisory boards of Europe, was assigned to protect individual's personal data in the progress of processing. The group is made up of a representative of the European Commission, one of the supervisory authorities of each MS, and one representative of the authority established for the EU institutions (European Commission Justice, 06.08.2013). According to Art. 3 (2), the Directive does not apply in cases where "public security, defense, State security [...] and the activities of the state in areas of criminal law" (European Parliament & European Council, 1995) are concerned.

For detailed information see Table 1 (Appendix), which outlines the goals of each principle, the applicable articles in the Directive as well as its relation to the OECD recommendations.

5.2. International Data transfer

In order to answer the research question it is important to outline the rules of the international data transfer. This chapter analyses the international sphere of transatlantic data flow and explains the so-called "Adequacy - decision", which created an immense hurdle for the transfer of personal data across the Atlantic.

5.2.1. International Data transfer within the EU and EEA area

The international data transfer within the EEA area is easily applicable as the same rules should be applied in all 47 MS. The Directive has effect in all countries of the EEA plus Iceland, Norway, and Liechtenstein.

5.2.2. International Data transfer outside the EU

If a private entity decides to transfer personal data outside the EU it needs to understand the difference between "trusted countries" and "third countries" (Bussche & Stamm, 2013, p. 53). The Directive sets clear standard rules for the transfer of personal data from EU-MS to countries outside the EU. For international data transfers to those countries, the Directive includes so-called "*adequacy decisions*", which are enforced through Art. 25. If a country offers equivalent data protection laws or if a multinational organization can exhibit adequate data protection standards and controls they count as the "trusted ones". Then the same rules can be applied as if they would be part of the EEA or EU area. Adequate standards exists e.g. in Argentina, Canada, Jersey, Switzerland, Guernsey and the Isle of Man (Bussche & Stamm, 54).

On the other hand the European Commission may decide that a data transfer to third countries can be limited, as they cannot ensure adequate standards of data protection. If a non-EU country does not provide equivalent data protection standards, the transfer has to be taken under greater consideration and special precautions need to take place. Otherwise the standards outlined in Directive 95/46/EC can be undermined quickly (European Commission Justice, 16.07.2013). Even though the U.S. does not provide adequate national data protection legislation, agreements between them and the EU can still exist. Examples are the Safe Harbor Programme, which will be explained later on, the Passenger Name Record agreement or the SWIFT agreement which allows the access to the data of financial transactions.

5.2.3. Adequacy decisions

In order to find out if a country can be assessed as "adequate", case-studies of third countries have to be examined while all circumstances which surround a data transfer operation (Kong, 2010) have to be assessed. Art. 25 (2) of the Directive encourages specific considerations if a country is in doubt of having equivalent data protection standards, taking into account "the nature of the data, the purpose and duration of the proposed processing operation [...], the country of origin and the country of final destination [and] the rules of law, both general and sectoral [...]" (European Parliament and European Council, 1995). However, the Directive also includes six exceptional cases in which data can be transferred to third countries. Those exceptions are listed under Art. 26(1) but are only applicable when specific safeguarding measures have been created in advance of the data transfer (Art. 26(2)). That means that a third country must guarantee enforcement mechanisms in order to ensure compliance (Murray, 1997, p.75).

These exceptions are lawfully applicable when the data subject has agreed to a transfer or if the transaction is required for the performance or the conclusion of a contract between the individual and the controller. The Directive also allows a data transfer to third countries if the transfer is "required on important public interest grounds, or for the establishment, exercise or defence of legal claims" (Art. 26(2)(c)). Another reason why a country can be assessed as "adequate" is when the data transfer serves as a protection for vital interests of the individual as well as when the transfer is requested from a register, which is bound to a number of specific rules.

Nevertheless the Directive only mentions those exceptions and leaves the final "adequacy decision" to the supervisory authorities. The Article 29 Working Party serves as an advisor in this field who transfers its recommendations and opinions to the supervisory authorities and can therefore influence and guide their decisions. According to Murray it is still very difficult for MS to determine under which conditions and circumstances a third country can be assessed as "adequate" and what data protection measures can be regarded as sufficient (Murray, 1997, p.65f). Scholars criticize that "adequacy decisions" based on case-by-case studies are too complicated and time consuming. In the U.S. for example, it has to be examined if the legal basis of the appending federal state can be regarded as "adequate" combined with a study about the company's business practices. They believe that "business practices are unclear indicators of whether a third country adequately protects personal data" (Murray, 1997, p.69). Wolf claims that the EU should be more transparent and pro-active when it comes to the determination of its adequacy decision (Wolf, 2014, p.14). He also denounced that the decision has often “potential for political tensions” (Wolf, 2014, p.14).

5.3. The Data protection standards of the United States

In order to understand the differences of EU and U.S. data protection approaches and their view on privacy, this chapter focuses on the main ideas of U.S. law. This includes its special emphasis on self-regulation and two major amendment acts, which influence the protection of EU citizens' data on a large scale.

5.3.1. A different approach: Self-regulation

In comparison to the regulatory approach of the EU, the U.S. takes a totally different 'sectoral' approach, relying on "a combination of legislation, regulation, and self-regulation (Courtney, 2012, p.44). The U.S. approach is based on sector-to-sector solutions and shows the tendency to adopt legislation only when certain sectors require a change or when recent circumstances leave no other way.

During Bill Clinton's presidency in 1997, the Framework for Global Electronic Commerce was created. It was based on the fact that the private sector should be leading in privacy matters while companies shall be focusing on and implementing self-regulations to facilitate growth of the global electronic commerce (Courtney, 2012, p.45). According to Jean Slemmons Stratford and Juri Stratford, the U.S. approach provides porous applicable legislation and no single law exists that could provide "comprehensive treatment of data protection or privacy issues". Even though the Congress has established legislation of how personal data should be treated by businesses, these rules only "target personal data in a particular area, or subsector of the private sector, such as telecommunications [...]" (Murray, 1997).

The industry continues to regulate itself though a number of mechanisms, such as organizations or industry codes. Examples are privacy seal programs such as the Online Privacy Alliance, TRUSTe or BBBOnLine (Fromholz, 2000). Nevertheless, a couple of concepts of data protection came through, such as the Privacy Act (1974) or the Computer Matching and Privacy Act from 1988.

5.3.2. Privacy Act

The Privacy Act was established in 1974 to safeguard personal data of U.S. citizens against the misuse of personal data stored in databases by Federal Agencies but also to "provide individuals with certain rights over information contained in those databases" (Slemmons Stratford & Stratford, 1998). It provides a regulation for the public sector but fails to include a comprehensive regulation of the private sector. Another crucial point for Europeans is that the following three basic rights of the Privacy Act only apply to "citizens of the United States or an alien who has been lawfully admitted for permanent residence" (U.S. Department of

State, 2013). That means that European citizens have no legal rights when their personal data is transferred across the transatlantic border.

The first right enacted in the Privacy Act allows the American citizen to examine his or her records, followed by the right to request a correction of those records if "they are not accurate, relevant, timely or complete" (U.S. Department of State, 2013). Furthermore, the Privacy Act allows American individuals to take steps against the unauthorized invasion of their personal data.

An oversight agency, which would serve as a guardian does not exist under the rules of the Privacy Act. Former President Gerald Ford was extremely opposed to the idea of a privacy protection commission and thereby an increased bureaucracy. He said that he "prefer[s] an approach which makes Federal agencies fully and publicly accountable for legally-mandated privacy protections and which gives the individual adequate legal remedies to enforce what he deems to be his own best privacy interest" (Flaherty, 1989, p.311). Agencies, such as the Department of Commerce (DOC), the Federal Trade Commission (FTC), and the Office of Management and Budget (OMB) have been created as a framework for reaction. They shall "maintain and protect individually identifiable information and proprietary information" (Flaherty, 1989, p.322). However they only have advisory functions and their advice is non-binding. According to Christopher Wolf this sector-to-sector approach has the advantage of providing the appropriate level of protection “for the sensitivity and use of personal information (Wolf, 2014, p.27)

5.3.3. FISA Amendment Act of 2008

"There are no privacy rights recognised by US authorities for non-US persons under FISA" (Bowden *et al.,* 2013, p.25). This conclusion can be also drawn from a report of the EP focusing on the US surveillance programmes and their consequences for EU citizens' fundamental rights as well as from the interview with the German data protection expert Christoph Schäfer.

The FISA amendment act created procedures for targeting non-U.S. persons in section 702. U.S. national security agencies are now enabled to access an individual's data if it might be of importance for national security matters (Liu, 2013). §1801(e) (2) even allows the collection of information "with respect to a foreign-based political organization or foreign territory that relates to the conduct of the foreign affairs of the United States" (Bowden, 2013, p.6). Therefore the reason for data access can be purely out of political reasons or out of "ordinary lawful democratic activities", Caspar Bowden, an independent advocate for privacy rights and former Chief Privacy Adviser of Microsoft explains.

A report of the Congressional Research Service revealed that a number of organisations came to the conclusion that the FISA Amendment violates the 4th Amendment and therefore it cannot secure the protection "against unreasonable searches" (Liu, 2013). General Michael Hayden, former NSA Director, argues that "the 4th Amendment is not an international Treaty" (Bowden, 2013, p.22) and hence does not apply to non-US citizens. Bowden claims that this amendment is "completely unlawful under the ECHR" (Bowden, 2013, p.7) and fears that all EU data might be potentially at risk. His report, which is based on top secret documents published by The Guardian, summarizes the procedures used by the NSA to target non-U.S. persons, including EU citizens, confirming that "there are zero substantive privacy protections for non-US persons" (Bowden, 2013, p.20). The U.S. has consequently the legal power to ignore the fundamental right to privacy of non-Americans. Schäfer also revealed that "human rights are restricted and in some cases even annulled" (Interview, 2014)

5.3.4. Section 215 of the Patriot Act

In October 2011, just one week after the terrorist attacks of 9/11, George W. Bush implemented the Patriot Act with the aim to fight terrorism. The Patriot Act forms the basis for the explanation of ever growing surveillance methods. According to Schäfer this act is a means for self-legitimation. Gathering more and more information about individuals are, according to the U.S. government necessary for national security. Section 215 allows intelligence agencies to collect so called "tangible things" as long as "the records are relevant to an ongoing [terrorism or espionage] investigation" (Kelley, 2013). The definition of tangible things is extremely broad and could include any data from an individual such as Internet browsing patterns, library records, medical records or his or her driver's license (Electronic Frontier Foundation, n.d.). The U.S. government argues that the collection of U.S. phone records is therefore legitimate. However, section 215 gives the FBI or other secret services the right to "investigate non-United States persons based solely on their exercise of First Amendment rights" (ACLU, n.d). According to the Electronic Frontier Foundation, an individual's data can be investigated with no profound reason based on e.g. the religious or political meetings someone attends or the website he has visited. A report of the EP states that this legislation "discriminates between the protections of afforded by the Constitution to US citizens, and everybody else" (Bowden *et al.*, 2013, p.22). On these grounds the U.S. has redefined its approach to privacy rights of individuals. The Safe Harbor scheme does therefore not protect EU citizen's personal data from the Patriot Act.

5.3.5. The main differences between EU and U.S. data protection approaches

It can be summarized that profound differences exist between data protection standards and the regulation of cross-border data flows between the EU and the U.S. According to the lawyer Julia Fromholz, the divergent approaches can be best explained by different cultural mores as well as the continent's history. Europe's past, filled with World War II and post-war communism regimes has taught its citizens and policy-makers to be fearful and suspicious when it comes to privacy and data protection norms. Those regimes undermined effectively and cruelly individuals' privacy through inter alia mass surveillance programmes. Nowadays the EU highly regulates its data protection legislation with a set of comprehensive legal rights, while the U.S. follows a laissez-faire governance system with no single, overarching data protection law. Its trust in markets and self-regulation lead to narrowly applicable laws, while Europe's legislation is based on supra-national policies, uniting all 28 MS and all MS of the EEA area. According to Murray, the U.S. approach is a result of its philosophy that "laws should ensure citizen's access to government, while still protecting them from government" (Murray, 1997, p.41).

In contrast to the regulatory approach of the EU, the U.S. sectoral, reactive approach only allows the government to intervene "when the private sector fails" (Movius & Krup, 2008) and leaves companies and associations to regulate themselves. In the U.S. several laws try to restrict government access to personal records (e.g. Privacy Act), while only a few laws exist which regulate the business world. Europe's legislation on the other hand covers both the private and the public sector.

Another crucial difference between those two approaches is that the U.S. has no single government agency that serves as a safeguard of privacy protection. For this purpose Europe has established independent DPAs in each MS.

As the EU sees privacy and data protection as a fundamental right, an eminent discrepancy of beliefs exists. The view of the U.S includes the presumption that privacy is "a commodity subject to the market and [...] cast in economic terms (Movius & Krup, 2008).

The U.S. makes a massive distinction between the protections of personal data between US.-citizens and non-Americans. That causes the discrimination of individuals outside the U.S. as they cannot rely on sufficient legal protection. It can be concluded that EU citizens' personal data transferred to the U.S. is not automatically secure because of specific law adjustments including the FISA amendment of 2008 and Section 215 of the Patriot Act. Even though the U.S. has ratified the principles of the OECD rules, they are non-binding and therefore they are not effectively accountable.

These unequal legal protection standards between the EU and the U.S. gave a platform for multiple discussions weather bilateral agreements such as the Safe Harbor-Programme agreement can even be enforced correctly in order to ensure the safety of European citizens' data. However, it can be concluded that both the EU and the U.S. want privacy protection; the difference of their approaches is mainly "in form, not in substance" (Wolf, 2014, p.18).

5.4. International Transfer of Personal Data - The Transatlantic Safe Harbor agreement

When the Directive became legally-binding in 1995, the U.S. was sure that they would be granted the exception clause of article 26 [...] and the data transfer could continue to flow (Busch, 2012). However, the profound differences in data protection standards mentioned above and the lack of a supervisory authority lead to the decision of the EC that the U.S. could not be assessed as "adequate" and the transatlantic data transfer had to be prohibited instantly. This blockade created trade barriers and strained competition and would have been extremely threatening to both the transatlantic economy and the trade relationship.

That is why David Aaron, U.S. Undersecretary for Commerce came up with the idea of a safe harbor-agreement, where companies could commit to "adequate" protection standards which are equivalent to the ones of the EU Directive (Busch, 2012). According to Galexia, the main idea of the agreement was to find a balance between the comprehensive legislative framework of the EU and the sectoral, self-regulatory approach of the U.S. However, only one year after the foundation of the Safe Harbor scheme, the importance of the transatlantic data-transfer shifted from an economic one to a security sphere (Busch, p.14) as the U.S. feared terrorist attacks. The first public draft, negotiated by the US Department of Commerce and the European Commission was released in 1998 and finalized in 2000 (Galexia, 2008).

5.4.1. The functioning of the Safe Harbor Programme

U.S. companies and organizations voluntarily self-certify that they abide to the rules of Directive 95/46/EC and are, simply by signing the agreement, able to process personal data collected in the EU. The FTC has to publish a list of all complying organisations on its website and can take enforcement actions against companies who do not abide to the rules. This chapter is focusing on the seven Safe Harbor Principles, the number of participating companies, the self-certification scheme, the adequacy decision, and enforcement bodies.

5.4.1.1. The Safe Harbor Principles

Companies of the U.S. are only capable of accessing and receiving personal data about EU citizens when they are committed to the seven principles of the scheme while adhering to the 15 FAQs. They voluntarily agree to commit to those principles, which were established for simplification (Bussche & Stamm, 2013, p.54). However, once they have agreed to them, the rules are binding and the company is "not dependent on a prior permit of by the competent supervisory authorities" (Bussche & Stramm, 2013, p.55).

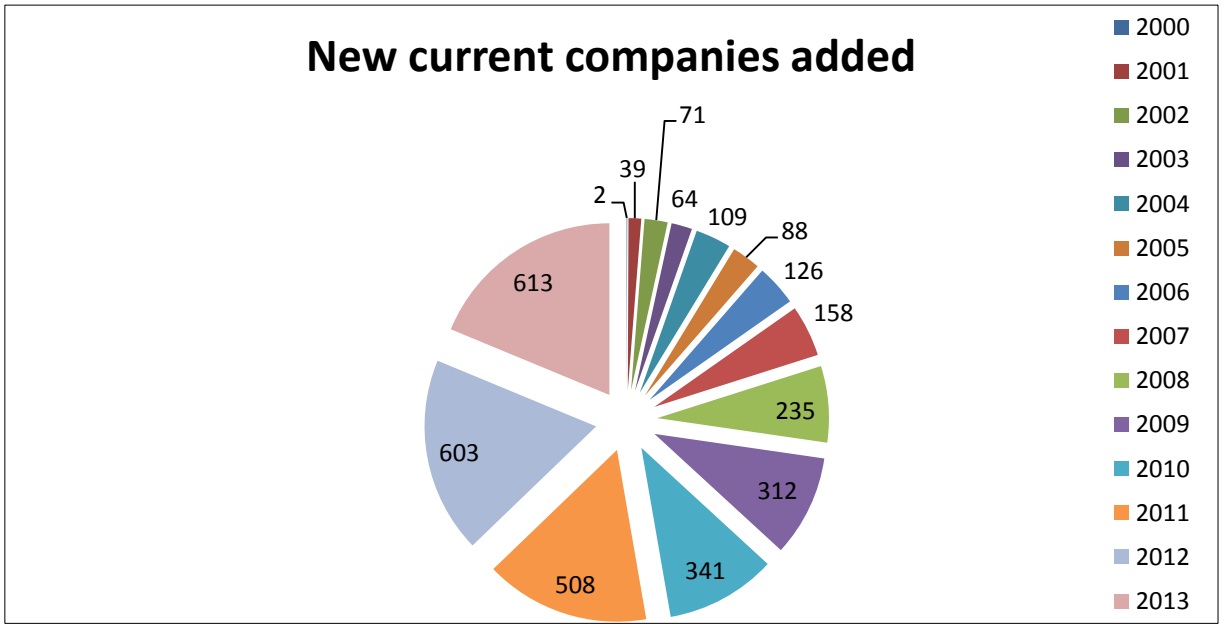
1. *NOTICE:* it is the participant's duty to inform the data subjects "why information about them is being collected and what it is being used for" (Schriver, 2002, p.15).
2. *CHOICE:* it is the company's responsibility to offer the individual the choice whether he wants his personal information to be disclosed to a third party. This principle is also called opt-out (Bussche & Stramm, 2013, p.54).
3. *ONWARD TRANSFER:* the transfer can only be preceded when the first principles are applied correctly (Schriver, 2002, p.15).
4. *SECURITY:* It is the company's duty to provide adequate data protection and prevent the loss of already collected data (Courtney, 2012, p.46).
5. *DATA INTEGRITY:* The purpose why personal data has been collected for in the first place has to be reliable and relevant. The company is responsible of taking "reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current" (The Commission of the European Community, 2000).
6. *ACCESS:* the individual has the right to have access to his or her personal information and is able to correct, amend, or delete inaccurate information.
7. *ENFORCEMENT:* companies must provide efficient mechanisms to assure its compliance with the principles. This can be done through self-assessments or outside compliance reviews (export.gov, 2012). Its privacy policy has to be "clear, concise, and easy for individuals to understand" (Future of Privacy, 2013, p.8). The FTC and the Department of Transportation have been charged as the main enforcement authorities of those principles (Brown & Blevins, 2002, p.7). The FTC can "intervene against unfair or deceptive practices" (European Commission, 2013, p.4). According to the EC they can execute enforcement actions, such as inquiries.

Annex II of the Decision 2000/520/EC of the EC (former Commission of the European Community) includes the 15 FAQs which were designed for clarification. It is possible to read the full version of the FAQs in the Appendices of this paper. Those FAQs cover "significant exceptions to the seven principles" (Brown & Blevins, 2002, p.7). FAQ 2, e.g. comprises Journalistic exceptions. Bowden sees those FAQs as loopholes of the scheme. He said that

U.S. trade lobbies together with the US negotiators in the Department of Commerce created the FAQs for US companies to interpret the Agreement to marginalize EU privacy rights" (Bowden et al.,2013, p.26). He even blames the bureaucracy of Safe Harbor for the lack of lodging a complaint for many years.

5.4.1.2. The Number of Participating Companies

By the end of 2013, 4.327 companies have joined the scheme, including Microsoft, Facebook and Amazon (Future of Privacy, 2013, p.6). According to the think tank Future of Privacy, the amount of companies joining the scheme could grow to a total number of 6,000 members until 2015. Graphic 1 shows the continuous growth of companies who have signed the agreement between 2000 and 2013. The programme had its difficulties in the beginnings, blaming the resistance of companies to join on logistical challenges, bureaucratic delays, and a general reluctance (Future of Privacy, 2013, p.13). In 2002, already 235 new companies signed the agreement; by 2007 it was established well enough so that also large business



Graphic 1: New current companies added (retrieved from Future of Privacy, 2013, p.8)

players joined the programme. The increasing awareness that privacy was an important issue in Europe and the knowledge that data is a valuable good on the market lead to the upstream of participants, including 603 new participants in 2012 and 613 new members in 2013. It is crucial to know these numbers as they reflect the growing importance of the international data transfer between U.S. and EU companies.

Under those circumstances the supervisory authorities have to analyse more and more data transfers and are extremely overstrained. The Working Party suggested that the authorities

should focus primarily on companies which are assumed to pose the biggest threats to data security (Murray, 1997, p.74). Consequently it is indispensable for the authorities to build on transparency and trust of U.S. companies compliance to ensure data protection for every European.

5.4.1.3. Self-Certification-Mark

he Safe Harbor programme, enforced by the U.S. Department of Commerce, is now one of the best-known mechanisms to allow a cross-border data transfer with a country which was primarily assesses as "inadequate".

Picture 1: Safe Harbor Self Certificate (retrieved from exportgov, 2013)

Picture 1 on the right hand shows the Self Certificate mark each company can place on their website to proof that they apply to the principles of the Safe Harbor agreement. The Certificate has to be renewed each year in order to proof the company's consisting compliance.

5.4.1.4. Adequacy Decision

The same adequacy procedures have to be applied as written in Directive 95/46/EC. According to the European Directive supra note 5, not all companies can participate in the programme because a number of sectors (e.g. telecommunications, financial institutions, energy or transport) do not fall under the jurisdiction of the Department of Transportation or the FTC. However, it is still possible for them to get approved, for example when they "use standardized contractual clauses approved by the [EC] or adopt approved binding corporate rules that govern international transfers of personal data" (Future of Privacy, 2013, p.9). Furthermore it is the Commission's right to suspend or limit the programme at any time, for example when Privacy Principles cannot be secured through the U.S. or when the requirements of the U.S. legislation overtake the principles of the agreement (European Commission, 2013, p.4).

5.4.1.5. Enforcement bodies

FAQ 5 clearly outlines that each company must cooperate with the DPA of the EU in order to apply to the Enforcement Principle. The following three enforcement bodies are indispensable for the effectiveness and reliability for this programme.

EU Data Protection Panel

The EU Data Protection Panel, an informal body, was created to investigate complaints from individuals which feel that their privacy has been violated. Its members are representatives of the DPA of each MS. If the panel is not competent in a specific area, committees have been installed which can solve disputes and have the power to impose sanctions.

Privacy Seal Companies

Normally, privacy seal companies are independent, non-governmental arbitration boards, which serve as dispute resolution mechanism and help a company with the verification of letters. The most famous ones are TRUSTe, the Direct Marketing Association, AICPA Web Trust or Square Trade. Alternative dispute resolution providers are BBB EU Safe Harbor Program or the American Arbitration Association (export.gov, 2013).

Federal Trade Commission

The FTC focuses on the commercial sector and has the authority "to prosecute unfair and deceptive practices that violate consumers" (FTC, 2013, p.1). The consumer protection agency was able to take actions against Internet giants such as Facebook, Google, Twitter or Myspace. FTC argues that its enforcement actions against those giants has helped to protect "over a billion consumers worldwide [and] hundreds of millions of [...Europeans] (FTC, 2013, p.4). According to FCT, they did not receive any referrals from the EU MS authorities for the first ten years of the program. That is why they investigated any Harbor violations on their own initiative. The Article 29 Working party and the EU DPAs regularly meet with the FTC in order to improve the collaboration (FTC, 2014, p.7). Julie Brill explained that if those Internet giants violate the orders against them, they have to expect huge fines, such as the $22.5 million penalty against Google in 2012 (Brill, 2013, p.5)

5.4.2. The official debate

Some might argue that the agreement has achieved its goals of promoting a transatlantic data transfer while protecting privacy. Others might disagree and request suspensions or improvements of the programme. This section is going to examine voices of the most important critics and advocates.

5.4.2.1. EU assessment 2013

A number of DPAs are concerned about the data transfer of the current scheme (European Commission, 2013, p. 5). As the basis of the agreement is build on transparency and trust in enforcement mechanisms, a lack of those enforcement practices would diminish the

assertiveness of the whole programme. The European Commission does not feel as they could rely on self-certification or on the adopted U.S. approach where companies can regulate themselves.

Violation of Safe Harbor Principles

The Commission sees a serious threat that the *principle of Notice* might be violated when companies cannot provide accessible information about their privacy policies sufficiently (European Commission, 2013, p.6). If a company cannot assure transparency, the FTC is unable to oversee difficulties or infringements. Therefore also the *principle of enforcement* cannot be guaranteed accurately. FAQ 6 explicitly includes the obligation for companies to publish their privacy policies and their statement that they adhere to the seven principles of the agreement. A study of Galexia in 2008 showed that only 348 out of 1,109 listed organisations met the fundamental requirements of the Framework. The EU assessment report of 2004 showed that a large number of companies could not provide the data subject with "clear and transparent information about the purpose for which their data were processed" (European Commission, 2013, p.12).

Another disconcerting fact is, that a lot of companies provide misleading or even false information on their website, e.g. in 2008, 20 companies showed that they earned the Self-Certificate of the scheme even though they did not meet the basic requirements of the Framework (Galexia, 2008, p.4). The EC report reveals that by the end of 2013 "about 10% of companies claiming membership in the Safe Harbor" (European Commission, 2013, p.7) even though they are not listed by the Department of Commerce.

Some companies violate the *Principle of Choice* as individuals do not get the chance to opt out "if their data were to be disclosed to a third party or to be used for a purpose that was incompatible with the purposes for which it was originally collected (European Commission, 2013, p.12). The Commission together with DPAs criticise that the programme lacks a full evaluation of the practice of each company.

Furthermore, the EC study revealed that around 30% of members have violated the *Enforcement Principle* because they were unable to "identify an independent dispute resolution process for consumers" (European Commission, 2013, p.8). A couple of companies have more than one dispute resolution provider and therefore often do not clearly express which one they have selected. Furthermore also TACD claims that the programme cannot provide sufficient protection for EU citizen's data as effective means of enforcement are missing and are not able or willing to take actions against privacy regulations. Julie Brill on the other hand defends the enforcement mechanism by the U.S. authorities, arguing that

ten enforcement actions had been successful since 2009, including sanctions on the Internet giants Google and Facebook (Gardner, 2013).

Until 2012 "no company's procedures have been challenged as failing to meet these guidelines" (Courtney, 2012, p.46). The EU assessment report of 2004 already identified the need "for the Department of Commerce to adopt a more active stance in scrutinising compliance with this requirement" (The Commission of the European Communities, 2013, p.6), e.g. should tighten its controls and take infringement actions against non-compliant companies. In March 2013 it was made mandatory for a company to publish its privacy policy for customers. Table 2 describes the results of a study made by Galexia in 2008, which focuses on the availability of privacy policies and the number of organisations which do or do not provide the requirements.

Availability	**Number of organisations**
Not Available – Contact Required Requires contact with the organisation, often an email address is supplied or the location requires a password.	246
Not Available – Absent The website does not have a privacy policy or access to the privacy policy is permanently broken. In this study access was attempted using both Internet Explorer and Mozilla Firefox. Searches included home pages, contact sections, 'about us', FAQs etc.	175
Available – Findable using search The Department of Commerce self-certification entry was incorrect, but the privacy policy could be found using simple site searches.	208
Available – Accurate link provided Accurately linked or clearly on the home page (includes correcting basic typos)	966

Table 2: Availability of privacy policies (retrieved from Galexia, 2008, p.11f.)

By the end of 2013, the amount of Safe Harbor members which offer a public privacy policy increased to around 90% (Connolly, 2012, p.3), while also the "proportion of Safe Harbor members that include basic information about the Safe Harbor and/or a link to the Safe Harbor website is now over 80% (Connolly, 2012,p.3).

5.4.2.2. Another opinion - the advocates of the scheme

Hugh Stevenson, deputy director of the FTC's Office of International Affairs states that the scheme was not working perfectly, however "this program has grown as privacy enforcement in general has grown" (Gardner, 2013) and there will be further improvements in the upcoming months and years. According to Cédric Burton, senior associate at Wilson Sonsini Goodrich&Rosati LLP, "[m]any Safe Harbor-certified companies have an extremely strong compliance program in place" (Garner, 2013).

The think tank Future of Privacy disagrees with the EC's perception and argues that U.S. companies have increased its privacy standards since the implementation of Safe Harbor. They also find that the FTC together with other dispute resolution providers can take effective enforcement actions against non-compliant companies. Julie Brill also argues that the Safe Harbor programme has given the FTC "an effective and functioning tool to protect the privacy of EU citizen data transferred to America" (Brill, 2013, p.5).

Moreover the chairman of the executive board of the European Telecommunications Network Operators' association ETNO supports the programme and argues that an increasing bureaucracy on the industry would not automatically lead to benefits for the consumer (EurActic, 2014).

The think tank believes that the arguments of most critics are "inaccurate or reflect a misunderstanding of how the Safe Harbor was designed to work" (Future of Privacy, 2013, p.33). The FTC clearly outlines that they want to continue the transatlantic data flow between the EU and the U.S. and foster greater transparency while increasing their efforts of enforcement actions. The chairwoman Edith Ramirez said that "[they] will continue to make Safe Harbor a top enforcement priority [and] that it can be expected to see more enforcement actions on this front in the coming months" (Ramirez, 2013, p.4)

Nevertheless, the EC's report clearly outlines that at least three of the seven principles are regularly violated by listed members of the scheme: the Principle of Notice, the principle of Choice and the Enforcement Principle. They are all pivotal and indispensable in securing transferred personal data of EU citizens.

5.4.2.3. The debate of the effects of the NSA surveillance on Safe Harbor

The question of if the mass surveillance actions by the U.S. government are proportionate and necessary in order to meet the interest of national security has been strongly discussed since Edward Snowden's revelations last year. Normally data protection rules can be limited on grounds of national security under the scheme; however the programme seems now to be

a "conduit for the transfer of the personal data of EU citizens [...] to U.S. intelligence agencies" (EC, 2013, Press Release).

The European Commission is concerned that personal data cannot be protected efficiently once they are transferred to the U.S., because "all companies [...] which grant access to U.S. authorities to data stored and processed in the US, appear to be Safe Harbor certified (EC, 2013, p.16). Therefore the EC believes that Safe Harbor serves as transmitter to allow US intelligence authorities to collect individual data which were originally processed in the EU. In 2000, when Safe Harbor was created it was unimaginable that intelligence agencies would have this large scale access to EU citizens' personal data. Julie Brill however believes that the access of personal data for national security is an issue that has to be addressed outside the scheme and is not relevant to its effectiveness (Gardner, 2013). She also argues that Europe has to keep in mind that "consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues" (Brill, 2013, p.2) and therefore national security matters should be also discussed separately. FTC has the opinion that the national security exemptions have been also created by the EU in its existing data protection laws [and] the EC has even "proposed such exemptions for government surveillance in its draft data protection regulation (Brill, 2013, p.6).

The think tank supports the statement of Julie Brill that the Directive never applied to issues of national security or law enforcement. Article 3 of the Directive states that the Directive "shall not apply to the processing of personal data [with respect to] operations concerning public security, defen[s]e, State security [...] and the activities of the State in areas of criminal law" (European Parliament & European Council, 1995). On these grounds it can be summarized that the Directive only protects EU citizens' personal data in the commercial context and leaves national security matters to its exception clause (Future of Privacy, 2013, p.34). According to the FTC this shows that the Safe Harbor programme should be seen as a separate discussion point to the mass surveillance activities for national security matters and should be approached differently because it was never designed to address national security issues.

The think tank Future of Privacy subscribes to the view that a suspension of Safe Harbor would have a negative impact on the security of EU citizens' data; however they also recommend a reform of the program (Future of Privacy, 2013, p.12). Brill concludes that Safe Harbor is "a very effective tool for protecting the privacy of EU consumers, and it shouldn't be suspended or renegotiated" (Garner, 2013).

However it can be argued that the EU MS have the authority to suspend the program when there is only a "substantial likelihood that the Safe Harbor is being violated. The EP member Jan Philipp Albrecht also calls for a stop of the program "unless there is an express re-authorization following a review" (Future of Privacy, 2013, p.10). His colleague from the European People's Party Manfred Weber calls for a reform of the programme, otherwise "the EU will have to suspend the Agreement" (EurActiv, 2014).

6. Does the Safe Harbor Agreement ensure the protection of EU citizens' personal data?

The European Union had tried throughout time to position itself as a leading figure of privacy and data protection rights. Initially neither DPAs nor U.S. companies were very enthusiastic about the programme as both negotiation partners wanted their legal approaches to be adopted by the Safe Harbor scheme. However, it seemed that the final version of the programme could provide a pragmatic escape from two totally diverse legal frameworks (Fuster *et al.*, 2008, p.2). This research paper discovered a number of sincere problems. This chapter is going to analyse in how far and to what extent those problems affect the protection of EU citizens' personal data. As the EC's assessment report of 2013 showed: three of the seven principles of the scheme, which are based on the fundamental principles of Directive 95/46/EC, are violated on regular basis: The Principle of Choice, Notice, and Enforcement.

- **The problem of defining "adequacy"**

The first major obstacle that still has to be dealt with is the problem of defining "adequacy". In order to further integrate global e-commerce and to increase the opportunities for growth, it can be summarized that the EU seems to be willing to compromise in the field of data protection standards. Art. 25 and 26 of the Data Protection Directive shows how European citizens' personal data can be transferred to countries which do not provide equivalent data protection standards. One outstanding point is that compliance with the Safe Harbor scheme does not automatically mean that U.S. companies have the exact same protection standards as the ones of EU MS. They only have to adhere to "equivalent" standards. It is for example not compulsory to submit non-compliance to DPAs, as it would normally be the case for EU companies. A definition of "adequate" does not exist which makes it very difficult for MS to determine under which conditions and circumstances a third country can be assessed as "adequate" and what data protection measures can be regarded as sufficient. Contradictory interpretations are inevitable and automatically lead to privacy protection breaches as privacy policies can differ from each other.

- **U.S. law versus EU law**

The fundamental differences between EU and U.S. law lead to the conclusion that the Safe Harbor programme is powerless in its functioning to safeguard EU citizens' personal data. One of the fundamental discrepancies between EU and U.S. law is the presumption of the U.S. government that privacy is a commodity subject to the market rather than a fundamental right for every human being. This profound difference leads to an uncertainty if EU citizens' data are a hundred percent safe once they have been transferred across borders. The reasons are, amongst others, laws such as the FISA amendment of 2008 and Section 215 of the Patriot Act. As mentioned above Safe Harbor is unable to protect EU citizens' personal

data from the U.S. Patriot Act or the FISA amendment. The U.S. authorities do not recognize any privacy rights for non-U.S. citizens under FISA (Bowden et al, 2013, p.18) because of the lack of fourth amendment protection for non-Americans. These unequal legal protection standards for EU citizens in and outside of the EU lead to the conclusion that the Safe Harbor program is powerless in safeguarding EU citizens' personal data. Mass surveillance activities and law enforcements resulted in the loss of EU citizens trust in the U.S. approach and its high reliance on self-certification and self-regulation.

Once personal data is transferred to the U.S. the human rights written under the ECHR can no longer be guaranteed. An international agreement, such as the Safe Harbor agreement cannot remove this risk.

- **EU Data Protection Directive is out of date**

One of the most important aspects as to why the Safe Harbor scheme cannot be reliable anymore is that the main rules of the EU Data Protection Directive are out of date. Hustinx argues that the Directive was created in 1995, a time where neither social networks existed in this mass-phenomenon nor where data collection was a billion dollar business (PR Online, 2014). However, a draft report of a new Data Protection Directive already exists and should lead to an improvement of data security standards and adapt to the existing structure of cross-Atlantic data flows. The international data transfer should, according to this new draft directive only be transferred if "individuals' right to a high level of protection are met" (EC, November 2013).

- **Lack of transparency**

Another problem of the scheme and therefore a threat for the security of EU citizen's data is that transparency of privacy policies is not given by all Safe Harbor participants at all time. A couple of companies did not implement the Safe Harbor Privacy Principles correctly. Francoise Gilbert, managing director of Calif.-based IT Law Group, said that Europeans have repeatedly complained about the inaccurate, incomplete, inappropriate or deceptive certifications on the website of the U.S. Department of Commerce (Blevins, 2014).

- **Lack of enforcement**

From time to time the EU has repeatedly tried to discuss the problem of enforcement actions of the scheme. It becomes clear that the laissez-faire principle of the U.S. and its reliance on self-regulation which had been transferred into the Safe Harbor scheme has failed. Even though the FTC has increased its efforts to monitor listed companies, the lack of enforcement is still one of the biggest threats to the survival of the programme and to the security of EU citizens' data. The European Commission finds that there is "no full evaluation of the actual

practice in the self-certified companies" (EC, 2013, p.8) and therefore the credibility of the self-certification scheme is decreasing. Another critical point is that there is no single U.S. government agency that serves as a safeguard mechanism. Not only the EC but also the Transatlantic Consumer Dialogue (TACD) has find the Safe Harbor scheme faulty. TACD claims that the programme cannot provide sufficient protection for EU citizen's data as effective means of enforcement are missing and are not able or willing to take actions against privacy regulations.

- **Is the programme only a loophole?**

Both Reding and Bowden marked the scheme as a "loophole" that may not be safe at all. According to Bowden, US companies are even able to marginalize EU privacy rights. Bowden actually goes further and states that U.S. trade lobbies together with the US negotiators in the Department of Commerce created the FAQs for US companies to interpret the Agreement to marginalize EU privacy rights" (Bowden et al.,2013, p.26). The EC believes that the Safe Harbor principles are violated as the U.S. programmes go "beyond what is strictly necessary and proportionate to the protection of national security" (EC, 2013, p.17). The proportionality principle in Art 6 of Directive 95/46/EC is therefore not guaranteed. Moreover also the EU-US Working Group on data collection finds that neither US nor EU citizens can be secured through the seven Safe Harbor principles under the U.S. surveillance programmes (EC, 2013, p.26).

Throughout these investigations it became clear that the Safe Habor agreement has failed to clearly provide data protection for European consumers in the light of the fast developing Internet structure and mass surveillance actions by U.S. secret services but also U.S. law enforcement acts. Ultimately neither the European Commission nor the U.S. Department of Commerce want to end the agreement irrevocably. This research shows that the Safe Harbor programme has been one important tool in advocating privacy standards and forced even huge Internet companies to apply to European standards. Nevertheless this research revealed that the weaknesses are too strong and that the existing form of the programme cannot be maintained in the exact same way. The programme needs to be renewed drastically in order to protect EU citizens' data effectively. If this is not the case the EC has still the right to suspend the programme.

7. Conclusion

The goal of this research report was to find out if the Safe Harbor agreement is able to effectively protect EU citizens' data once it crosses the Atlantic. Through the review of primary and secondary data it became visible that this is a controversial issue with neither one clear mindset nor one simple solution to it. These investigations illustrate that the Safe Harbor programme was doomed since its beginnings. Nevertheless, the EC does not seem to be willing to suspend the programme even though the arguments are alarming. A wake-up-call had been made, first steps at political stage have been initiated and critics will continue to address and denunciate the agreement in the future if inefficient re-negotiations might take place. Originally the Safe Harbor agreement was designed to save companies time and money. However, this agreement might have been executed at the expense of a fundamental European human right: the right to privacy. On the other hand, the uprising debate about privacy can be also seen as a debate for change and a time where the EU together with the U.S. can form a long-term solution in order to allow a transatlantic data transfer that "both protects privacy and promotes international economic growth" (Wolf, 2014, p.32). This might be the starting point for a global initiative that can foster strong data protection standards throughout the world. If the Safe Harbor Programme continues to exist within a different legal framework it can be used as an agreement for further interoperability. The increasing criticism and the ongoing debate in the media in Europe and abroad can actually result in great reforms and improvements of the scheme. If Safe Harbor is going to be renegotiated effectively, it might be able to further safeguard EU consumers' personal data in a time where the nature of data protection is not bound to any borders.

8. Recommendations

This last chapter tries to give recommendations to the EC, the only institution with the power to re-negotiate the agreements or to suspend the programme in order to ensure greater security standards.

If the Safe Harbor agreement were suspended by the EC, personal data could not be transferred across the Atlantic anymore, which will affect many Internet and technology companies as well as multinationals. The EC is could either suspend the programme, or renegotiate it. One argument pro suspension is that the legislative framework of the U.S. does not secure EU citizens' data efficiently. Therefore the existing scheme is not able to adequately safeguard personal data transferred to the U.S. The downsides of this decision would be an increase in bureaucracy costs, taking into account that U.S. companies would have to "revert to model contracts, which are strict and expensive to implement" (Future of Privacy, 2013, Dec. 20). According to Blevins, "[d]ata privacy compliance would be a more time-consuming and expensive proposition for U.S. companies" (Blevins, 2014). Mr. Schäfer also criticized this option in the conducted interview. On the other side Francoise Gilbert argued that numerous companies, including Germany, already choose to use those contracts instead of Safe Harbor (Blevins, 2014). Gilbert also argued that those contracts are more trusted and a company does not have to fear to get investigated by the FTC.

As the different legal regimes of the EU and the U.S. will continue to exist and because of the complexity of the transatlantic data-transfer, a more flexible approach, such as the Safe Harbor agreement could still "enhance privacy protection, spur innovation and trade, and help [...] achieve interoperability between two systems" (Wolf, 2014, p.32). That is why this paper favours the idea to strengthen the programme and to renegotiate its content. Fundamental changes need to take place if EU consumers' data shall be secured in the future.

Article 4 of the Safe Harbor Decision allows the EC to "adapt the decision at any time in the light of experience with its implementation". The following points provide specific ideas of how the programme can be improved and what has to be done in order to safeguard personal data more efficiently.

1. Renew the Data Protection Directive

As Directive 95/46/EC is clearly out of date a reform is indispensable to face the challenges of the 21st century. In March 2014 the EP has already adopted a proposal for a new EU General Data Protection Regulation. 621 votes in the EP Parliament were in favour of this Regulation and only 10 against while 22 stayed absent (Hunton & Williams LLP, 2014). This result highly intensifies the call for action on the EC and is a first answer to improve the

standards of EU's common data protection standards and a force against privacy breaches. In the proposed Regulation the individual would have the “right to be forgotten, which would then allow each EU consumer to ask for the deletion of their personal information (Wolf, 2014, p.29). This is, in my opinion, one excellent first step to further transfer the power of the company or the government to the individual and leads to more privacy.

In this regulation the EU has to guarantee highest data protection for EU citizens. Those rules should be also applicable to U.S. companies who want to transfer data across the Atlantic. Secondly, a clear definition of "adequacy" has to be set in order to diminish any contradictory interpretations and privacy breaches.

2. Access by U.S. authorities

It is vital for the functioning of the programme and for the protection of personal data that all participants of the scheme inform the EC frequently to what extent they collect or process transferred data to U.S. authorities. Furthermore, this paper agrees with the EC's idea that those companies have to indicate specifically when they applied the "exceptions to the Principles of the scheme to meet national security, public interest or law enforcement requirements" (EC, 2013). Furthermore those national security exceptions have to be proportionate. They have to clearly outline and justify why a lower level of data protection exists in specific cases.

3. Suspend the self-certification mechanism

Companies should not be allowed to self-certify themselves anymore. Of course only organizations who profit from the sale, collection, and aggregation of personal data will argue that the scheme is then burdened with a lot more bureaucracy and will impose immense costs. Nevertheless this is the most effective way of ensuring that EU citizens' personal data is secure.

4. Transparency

The fundamental basis of the scheme is transparency and therefore it needs to be strengthened and stipulated. It needs to be "ensured to the greatest extent possible without jeopardising national security" (EC, 2013, p.16).

4.1. Fast identification of non-members of the scheme

The EC recommends clearly flagging all companies which are not current members of the scheme on the website of the Department of Commerce. This is a very effective idea in order to inform EU companies that it is not allowed to transfer personal data to those specific U.S. firms.

4.2. Publication of privacy policies

All certified companies should always make their privacy policies publicly available on their website so that EU companies but also EU citizens know exactly what happens to their personal data.

5. Enforcement actions

If a company had made false claims about their compliance with the programme or if they have violated one of the principles the enforcement bodies should have the power to suspend them from the agreement. This suspension can be reversed when the company can prove that it applies to EU security standards. In this case the company should be monitored and investigated again after, e.g. one year (The EC also recommends one year). This decision is necessary as any false claims or principle violations weaken the whole system and lead to the ineffectiveness of the agreement.

6. Install warning notice

In order to foster transparency the EC should be informed by the Department of Commerce instantly if new government regulations have been installed that might affect compliance with the Principles of the Safe Harbor Programme. Bowden is a great advocate of this idea, which forces the public sector to install a prominent warning notice before collected data can be transferred to the U.S. for processing (Bowden, 2013, p. 30)

9. References

Books

Bussche, A., & Stamm, M. (2013). *Data protection in Germany*. München: Verlag C.H. Beck.

eBooks

Bennett, C. J. (2000). *An International Standard for Privacy Protection: Objections to the Objections*. Retrieved March 21, 2014, from http://easy.squareis.com/http/dl.acm.org/ft_gateway.cfm?id=332200&ftid=2990&dwn=1&CFID=305155490&CFTOKEN=88979015&____x=1352

Brown, D., & Blevins, J. L. (2002, December 1). *The Safe Harbor agreement between the United States and Europe: a missed opportunity to balance the interests of e-commerce and privacy online*. Retrieved March 19, 2014, from http://easy.squareis.com/http/web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=a33f5758-5d95-4f96-8c7f-0906371e7acd%40sessionmgr4001&vid=5&hid=125&____x=1248

Busch, A. (2012, December 1). *The regulation of transborder data traffic: Disputes across the Atlantic*. Retrieved March 15, 2013, from http://easy.squareis.com/http/web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=a33f5758-5d95-4f96-8c7f-0906371e7acd%40sessionmgr4001&vid=4&hid=125&____x=1248

Courtney, K. (2012). *Information Privacy (Concepts & Applications)* (1st ed.). Delhi: Learning Press.

Flaherty, D. H. (1989). *Protecting Privacy in Surveillance Societies*. Retrieved March 23, 2014, from http://books.google.de/books?id=YIZjmNfmuX0C&printsec=frontcover&hl=de&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Fuster, G. G., De Gert, P., & Gutwirth, S. (2008, July). *SWIFT and the vulnerability of transatlantic data transfers*. Retrieved April 2, 2014, from http://easy.squareis.com/http/web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=e46f1dc9-fdab-46ac-8f47-2862c83b4fd2%40sessionmgr112&vid=4&hid=4114&____x=1248

Kong, L. (2010). *Data Protection and Transborder Data Flow in the European and Global Context*. Retrieved March 24, 2014, from http://easy.squareis.com/http/ejil.oxfordjournals.org/content/21/2/441.full.pdf+html?____x=1369

Thompson, G. B., & Hamilton, L. S. (2002, October 1). *How Safe Are the Harbors? The United States Struggles with Internet Data Privacy*. Retrieved March 29, 2014, from

http://easy.squareis.com/http/web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=7cf0c82d-e4e2-49a2-aaf0-cc3dce26e2a8%40sessionmgr115&vid=4&hid=123&____x=1379

Online sources

ACLU (n.d.). *Reform the Patriot Act | Section 215 | American Civil Liberties Union*. Retrieved March 25, 2014, from https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215

Alberti, P. (2013, October 8). *Data protection: Claude Moraes calls for suspension of EU-US 'safe companies list'*. Retrieved March 24, 2014, from http://www.socialistsanddemocrats.eu/newsroom/data-protection-claude-moraes-calls-suspension-eu-us-safe-companies-list

APCO Forum (n.d.). *U.S.-EU Safe Harbor Agreement - Recent Developments and Implications*. Retrieved March 19, 2013, from http://www.apcoworldwide.com/content/PDFs/eu-us_safe-harbor-agreement.pdf

Baker, J. (2013, November 27). *EU will not suspend safe harbor data privacy agreement with the US | PCWorld*. Retrieved March 17, 2014, from http://www.pcworld.com/article/2067480/eu-will-not-suspend-safe-harbor-data-privacy-agreement-with-the-us.html

Bfdi.bund (2010, April 29). *Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen*. Retrieved March 18, 2014, from http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile

Blevins, B. (2014, January 21). *Future uncertain for Safe Harbor, enterprise data privacy compliance*. Retrieved May 14, 2014, from http://searchsecurity.techtarget.com/news/2240213585/Future-uncertain-for-Safe-Harbor-enterprise-data-privacy-compliance

Bowden, C. (2013, September 30). *FISA, PRISM and Data Protection*. Retrieved March 25, 2014, from http://ic.epfl.ch/files/content/sites/ic/files/Caspar_Bowden_slides.pdf

Bowden, C., Bigo, D., Scherrer, A., & Davoli, A. (2013, September) *The US surveillance programmes and their impact on EU citizens fundamental rights*. Retrieved March 26, 2014, from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

Brill, J. (2013, October 29). *Re-Establishing Trust Between Europe and the United States*. Retrieved April 27, 2014, from http://www.ftc.gov/sites/default/files/documents/public_statements/data-protection-privacy-security-re-establishing-trust-between-europe-united-states/131029europeaninstituteremarks.pdf

Busch, A. (2008, June). *Regulating privacy across the Atlantic: Of pyrrhic victories, arena switching, and policy U-turns*. Retrieved March 27, 2014, from http://regulation.upf.edu/utrecht-08-papers/abusch.pdf

Centre de Recherche Informatique et Droit (CRID); prepared by Dhont, J., Pérez Asinari, M. V., & Poullet, Y. (2004, April 19). *Safe Harbour Decision Implementation Study*. Retrieved March 17, 2014, from http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf

Council of Europe (1981, January 28). *ETS no. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Retrieved March 20, 2014, from http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Data Protection Working Party (2007, June 20). *Opinion 4/2007 on the concept of personal data*. Retrieved March 17, 2014, from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Dr. Imke Sommer (2013, July 24). *Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe*. Retrieved March 17, 2014, from http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

Electronic Frontier Foundation (n.d.). *Section 215 of the USA PATRIOT Act | Electronic Frontier Foundation*. Retrieved March 20, 2014, from https://w2.eff.org/patriot/sunset/215.php

Electronic Privacy Information Center (n.d.). *EPIC - Council of Europe Privacy Convention*. Retrieved March 20, 2014, from http://epic.org/privacy/intl/coeconvention/

EurActiv (2014, January 29). *EU threatens suspension of data deal with US | EurActiv*. Retrieved April 27, 2014, from http://www.euractiv.com/infosociety/eu-threatens-suspension-data-dea-news-533093

EurActiv (2013, December 18). *Data 'Safe Harbour' under threat as US castigates EU Parliament over Snowden | EurActiv*. Retrieved March 25, 2014, from http://www.euractiv.com/infosociety/data-safe-harbour-threat-us-cast-news-532441

European Commission (2013, November 27). *Restoring Trust in EU-US data flows - Frequently Asked Questions*. Retrieved April 27, 2014, from europa.eu/rapid/press-release_MEMO-13-1059_en.htm

European Commission (2013, November 27). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*. Retrieved March 17, 2014, from http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

European Commission (n.d.). *FREQUENTLY ASKED QUESTIONS relating to transfers of personal data from the EU/EEA to third countries*. Retrieved March 19, 2014, from http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

European Commission Justice (2012, October 9). *How will the "safe harbor" arrangement for personal data transfers to the US work?* Retrieved March 19, 2014, from http://www.ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm

European Commission Justice (2013, July 16). *Transferring your personal data outside the EU*. Retrieved March 20, 2014, from ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm

European Commission Justice (2013, August 6). *Article 29 Working Party*. Retrieved March 22, 2014, from ec.europa.eu/justice/data-protection/article-29/index_en.htm

European Commission Justice (2013, November 25). *Who can collect and process personal data?* Retrieved March 19, 2014, from ec.europa.eu/justice/data-protection/data-collection/index_en.htm

European Convention on Human Rights (n.d.). *Article 8*. Retrieved March 20, 2014, from http://www.echr.coe.int/Documents/Convention_ENG.pdf

European Parliament (n.d.). *Peter J. Hustinx*. Retrieved March 27, 2014, from http://www.europarl.europa.eu/document/activities/cont/200901/20090122ATT46920/20090122ATT46920EN.pdf

European Parliament/NEWS (2014, March 12). *US NSA: stop mass surveillance now or face consequences, MEPs say*. Retrieved March 23, 2014, from http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say

European Parliament & European Council (2000, July 26). *2000/520/EC: COMMISSION DECISION OF 26 JULY 2000 PURSUANT TO DIRECTIVE 95/46/EC*. Retrieved from policy.mofcom.gov.cn/english/flaw!fetch.action?libcode=flaw&id=55ca2ba7-16af-4536-8c0b-1431bf8bbb61&classcode=360;520

European Parliament & European Council (1995, October 24). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Retrieved March 20, 2014, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Union (2005, July 25). *DATA PROTECTION PANEL*. Retrieved March 9, 2014, from http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_en.pdf

European Union (2011, February 1). *Protection of personal data*. Retrieved March 20, 2014, from europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

European Union Agency for Fundamental Rights (2013). *Handbook on European data protection law*. Retrieved March 20, 2014, from http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

Export.gov (2012, July 5). *U.S.-EU Safe Harbor FAQ 7 - Verification*. Retrieved March 26, 2014, from http://export.gov/safeharbor/eu/eg_main_018379.asp

Export.gov (2013, December 18). *Safe Harbor Data Privacy Links*. Retrieved March 10, 2014, from http://export.gov/safeharbor/eg_main_018241.asp

Export. gov (2014). *Export.gov - Main Safe Harbor Homepage*. Retrieved March 19, 2014, from http://export.gov/safeharbor/index.asp

Fromholz, J. M. (2000, February). *The European Union Data Privacy Directive*. Retrieved March 23, 2014, from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1281&context=btlj

FTC (2013, November 12). *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission - Review of the U.S.-EU Safe Harbor Framework*. Retrieved April 12, 2014, from http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-

enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf

Future of Privacy (2013, December 20). *The LIBE Committee Wants To "Suspend" The Safe Harbor… Along With Thousands of EU Employee Salaries*. Retrieved May 13, 2014, from http://www.futureofprivacy.org/2013/12/20/the-libe-committee-wants-to-suspend-the-safe-harbor-along-with-thousands-of-eu-employee-salaries/

Future of Privacy Forum (2013, December 11). *The US-EU Safe Harbor - An Analysis of the Framework's Effectiveness in Protecting Personal Privacy*. Retrieved March 17, 2014, from http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf

Galexia (2008, December 2). *The US Safe Harbor - Fact or Fiction?* Retrieved March 17, 2014, from http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

Gardner, S. (2013, December 16). *U.S. Officials Respond to EU Concerns Over Safe Harbor Data Transfer Program | Bloomberg BNA*. Retrieved April 1, 2014, from http://www.bna.com/us-officials-respond-n17179880742/

Hunton & Williams LLP (2014, March 12). *MEPs back 'immediate suspension' of 'safe harbour' data transfers and threaten to veto US trade deal*. Retrieved May 13, 2014, from http://www.out-law.com/articles/2014/february/meps-back-immediate-suspension-of-safe-harbour-data-transfers-and-threaten-to-veto-us-trade-deal/

Hustinx, P. J. (n.d.). *(Future) Interaction between Data protection authorities and national human rights institutions.* Retrieved March 21, 2014, from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-07-17_Interaction_DPA-NHRI_EN.pdf

Kelley, M. (2013, September 5). *PATRIOT Act Author: NSA Abused Its Power - Business Insider*. Retrieved March 26, 2014, from http://www.businessinsider.com/patriot-act-author-nsa-abused-its-power-2013-9

Krempl , S. (2014, January 16). *NSA-Affäre: EU-Parlament fordert Kündigung des Safe-Harbour-Abkommens.* Retrieved March 19, 2013, from http://www.heise.de/newsticker/meldung/NSA-Affaere-EU-Parlament-fordert-Kuendigung-des-Safe-Harbour-Abkommens-2087185.html

Liu, E. C. (2013, April 8). *Reauthorization of the FISA Amendments Act*. Retrieved March 1, 2014, from http://www.fas.org/sgp/crs/intel/R42725.pdf

Logothethis, G. (2013, February 15). *What a transatlantic trade agreement will mean for the United States and Europe*. Retrieved May 24, 2014, from http://hellenicleaders.com/blog/what-a-transatlantic-trade-agreement-will-mean-for-the-united-states-and-europe/#.U4NN-lPzz08

Movius, L. B., & Krup, N. (2008, September 8). *U.S. and EU Privacy Policy: Comparison of Regulatory Approaches*. Retrieved March 23, 2014, from http://file:///C:/Users/Tatjana/Downloads/405-2004-1-PB.pdf

Murray, P. J. (1997). *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?* Retrieved March 25, 2014, from http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1563&context=ilj

NABARRO (2013, August 6). *Is "Safe Harbor" no longer safe? EU to review regime for personal data transfers to the US*. Retrieved March 25, 2013, from http://www.nabarro.com/Downloads/IP-IT-Is-Safe-Harbor-no-longer-safe.pdf

Neal, D. (2014, March 12). *European Parliament wants an end to NSA PRISM data haul- The Inquirer*. Retrieved March 25, 2014, from http://www.theinquirer.net/inquirer/news/2333792/european-parliament-wants-an-end-to-nsa-prism-data-haul

Oltermann, P. (2013, September 27). *Britain accused of trying to impede EU data protection law | Technology | The Guardian*. Retrieved March 25, 2014, from http://www.theguardian.com/technology/2013/sep/27/britain-eu-data-protection-law

PrivacyTrust (2013). *Safe Harbor Certification*. Retrieved March 20, 2014, from http://www.privacytrust.org/guidance/safe_harbor.html

Ramirez, E. (2013, November 12). *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework*. Retrieved April 27, 2014, from http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf

Reding, V. (2014, January 15). *Future of the Safe Harbour Agreement in the light of the NSA affair*. Retrieved March 19, 2014, from europa.eu/rapid/press-release_SPEECH-14-27_de.htm

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009, May). *Review of the European Data Protection Directive*. Retrieved March 22, 2014, from http://www.huntonfiles.com/files/webupload/PrivacyLaw_review_of_eu_dp_directive.pdf

RP Online (2014, January 2). *EU-Datenschützer: Hustinx fordert Ende der 'Wildwest'-Methoden von Staaten* [Translation: EU Data Protection: Hustinx calls for end of "wild-west" methods of states] Retrieved April 12, 2014, from http://www.rp-online.de/politik/ausland/hustinx-fordert-ende-der-wildwest-methoden-von-staaten-aid-1.3918905

Slemmons Stratford, J., & Stratford, J. (1998). *Data Protection and Privacy in the United States and Europe*. Retrieved March 23, 2014, from http://www.iassistdata.org/downloads/iqvol223stratford.pdf

Schriver, R. R. (2002). *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*. Retrieved March 25, 2013, from http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3848&context=flr

The Commission of the European Communities (2000, July 26). *2000/520/EC: Commission Decision pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*. Retrieved March 26, 2014, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

The Commission of the European Communities (2004, October 20). *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*. Retrieved March 26, 2014, from http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf

The Guardian (2014). *The NSA files* | *World news* | Retrieved January 15, 2014, from http://www.theguardian.com/world/the-nsa-files

U.S. Department of State (2013, June 11). *The Privacy Act: U.S. Department of State - Freedom of Information Act*. Retrieved March 22, 2014, from http://foia.state.gov/Learn/PrivacyAct.aspx

Wolf, C. (2014). *Delusions of Adequacy? Examining the Case for Finding the United States Adequate For Cross-Border EU - U.S. Data Transfers / Washington University Journal of Law & Policy*. Retrieved May 8, 2014, from http://digitalcommons.

10. Appendices

10.1. Student Ethics Form

Your name: Tatjana Arnold

Supervisor: Paul Nixon

Title of Project: European Data Protection - The case of EU - US relations

Research Question:

"To what extent does the Safe Harbor agreement between the U.S.A. and the EU ensure the protection of EU citizens' personal data under Directive 95/46/EC?"

Aims of project:

Context:

In an age where a huge number of individuals share personal information and interests on social networks, we reveal much more of ourselves than we are aware of. Through the interconnectivity of the computer technology in combination with the ubiquity of the Internet, firms are capable of spreading personal data anywhere in the whole world at all times. A problem emerges as soon as this transfer is being violated. If data protection laws are being ignored, the right to privacy is at stake.

In particular, since Edward Snowden's revelations in June 2013, the right to privacy has been discussed heavily. This paper focuses mainly on the bilateral Safe Harbor deal, which entered into force in 2000 even though it had to face criticism back then. The agreement, where companies in the U.S. sign up to a set of rules to protect the data privacy of E.U. customers is voluntary. Limitations to data protection rules are permitted in case of national security. The European Commission, the only institution with the power to suspend the agreement, claimed that the large-scale collection of personal data under U.S. surveillance programs has called the whole framework into question. Overall the scheme is utterly criticized because of its lack of transparency, the lack of enforcement bodies and actions and the obsolescence of the existing Data Protection Directive.

Aim:

The aim of this project is to find out if the Safe Harbor agreement can ensure EU citizens' personal data, especially under the set of rules of Directive 95/46/EC.

Will you involve other people in your project?

YES ~~/ NO~~

What will the participants have to do?

I will conduct an interview. I have formulated a number of interview questions in advance and sent them to the interviewee. These questions might be still re-formulated while talking to the interviewee or others will be added later on.

What sort of people will the participants be and how will they be recruited?

The interviewee will be recruited via mail. A number of policy makers have been contacted via email. I have also asked a EU data protection officer and TeleTrust Information Security Professional to answer my questions. He is a professional and expert in the field of data protection and can put special in-depth knowledge to my topic.

What sort stimuli or materials will your participants be exposed to, tick the appropriate boxes and then state what they are in the space below?

Questionnaires[ ]; Pictures[ ]; Sounds [ ]; Words[ ]; **Other[x]: Interview**

What procedures will you follow in order to guarantee the confidentiality of participants' data?

I will not store the data of the participant after I have handed in my thesis. His/Her personal data (name, addresses etc.) will not be stored in such a way that they can be associated with the participant's data later on. The information I have about him/her will not be published anywhere else besides in the content of this dissertation. I ask for the permission of the interviewee to record the telephone call and also ask if he/she wants me to use acronyms instead.

Student's signature: ..... Date: 07.05.2014

Supervisor's signature: ..... Date: .....

10.2. Interview with Christoph Schäfer

10.2.1. Transcript of Interview

08.05.2014, 9 a.m. via mobile phone

Personal Information

Data protection expert, data protection advisor/trainer, data protection officer at GDDcert, TeleTrusT Information Security Professional (T.I.S.P.)

Tatjana: Hello Mr. Schäfer, how are you? Thanks for taking your time for me today. I am thankful and happy that you could make it.

Mr. Schäfer: Good morning Miss Arnold. Yes, no problem. I see what I can do.

Tatjana: As I told you already in my previous email, this interview will be used for my final dissertation, my Bachelor Thesis. I am a student of European Studies in The Hague and the focus of my thesis lies on the transatlantic data transfer between the EU and the U.S. I focused on the Safe Harbor agreement and still need the insight knowledge of a professional and an expert. That is why I contacted you. I want to record this interview, because it will be much easier for me to transcribe all information and it will help me to recall things again. Do you agree that I record this telephone call? If not I will not record our conversation.

Mr. Schäfer: Yes, of course you can record this conversation. I also have already signed the "Consent Form" you sent me via email.

Tatjana: Okay, thank you very much. From now on our conversation will be recorded. Furthermore I need to know if I can use your name in this paper or if I should use another name?

Mr. Schäfer: No problem, you can use my name.

Tatjana: Okay, good. Then we can start with the questions I have prepared for today.

1. **In what way do you have to deal with the Safe Harbor agreement?**
   I have to deal with it on regular basis as I have an advisory function for multiple companies who have service providers (located) in the U.S.A.

2. **Does the legal basis of the U.S. affect the security of EU citizen's personal data?**
   Which U.S. legal law do you mean exactly? I can read in your interview outline that you want to further investigate the Patriot Act and the FISA amendment later on. Well, first of all the U.S. has a constitution including the Declaration of Independence. The 4th Amendment of this constitution protects U.S. citizens as well as non-U.S. citizens against surveillance. It is forbidden to do a searching or to arrest someone without reasonable suspicion. This 4th Amendment only has force as long as the non-U.S. citizen stays in the United States. Basically, he/she should be protected. This is only the case if they are not under the suspicion of being terrorists or spies. The 4th amendment is not binding if the non-U.S. citizen stays outside of the U.S.
3. **Have you heard about the FISA Act? - If yes, can you explain what consequences emerge for EU citizens?**

The FISA Act is older than the Patriot Act, that's why we need to start here first. The FISA Act regulates the issue of espionage and the suspicion of espionage. Someone who is under suspicion of being a spy can, under the permission of a secret court be monitored and controlled. That means that this person cannot count on his basic rights of the constitution. In this case those rights are restricted. The court can approve and authorize such activities. If the FBI thinks that there is an increased need for action (e.g. someone might plan a terrorist attack) the surveillance of that person can be and normally is allowed by the secret court.

The case for persons abroad is different. The NSA (surveillance of telecommunications) and the CIA can, without a warrant and without the permission of a secret court, restrict constitution rights and monitor that person instantly.

3.1. Caspar Bowden (an independent advocate for privacy rights and former Chief Privacy Adviser of Microsoft) claims that this amendment is "completely unlawful under the ECHR.

Do you agree with this statement?

I think it is difficult to assess such extreme statements. On the one hand I know that we have fundamental rights/fundamental human rights and we have to be protected against state power and state surveillance actions. The FISA Act annulled basic human rights just if someone is under the suspicion of being a terrorist or a spy. Human rights are therefore restricted or in some cases even annulled. I would not support this statement to the fullest, but in principle I do agree with Mr. Bowden's statement.

4. **Have you heard about the Patriot Act? - If yes, can you explain what consequences emerge for EU citizens? Does this Act also affect the Safe Harbor scheme?**

First of all we have to look at the background of the Patriot Act. It came into force after the terrorist attacks of September 11 by the U.S. government under George W. Bush. From the point of view of today, I would argue that his security politics and the Republicans have surprised him by passing the Patriot Act. This act is much more extreme than FISA. Whoever is under the suspicion of being a terrorist loses all his basic civil rights. Secret courts exist, such as the Foreign Intelligence Surveillance Court. The public does not know how it comes to a decision and where those decisions are made, everything happens in secret.

This act is a mean for self-legitimation. If for example the NSA Director really thinks that a person has to be monitored instantly he just has to write a security letter and the surveillance action can start immediately.

5. **In how far do FISA and the Patriot Act affect the assertiveness of the Safe Harbor scheme?**

Both amendments lead to the ineffectiveness of the Safe Harbor programme.

To understand this, we have to know why the programme had been invented in the first place. As a European company I am now able to transfer data to third countries in the EU and the EEA. I can transfer the data also to countries with a legislation which is equivalent to EU law, comparable to Directive 95/46/EC.

In Germany data protection is a fundamental right. The U.S.A. on the other hand has a totally different comprehension of data protection and privacy. In Europe, data protection counts as a fundamental right, where the right to privacy is deep-seated.
In the U.S. the way of thinking about privacy is completely different. Therefore the comprehension of privacy in the EU and the one in the U.S. are totally diverse. In the U.S. data security laws do exist, but they are not comparable to the ones in the EU.

As a lot of EU firms work together with companies in the US, such as mother-or daughter companies or trade partners, the Safe Harbor agreement is of great concern for them.
e.g. Microsoft Office is used in a multiple number of companies within Europe, Cloud-Solutions are on the forefront and companies such as Google or Amazon use them too.

The EU wants the free trade of data; however, the Directive does not allow a data transfer between the EU and the U.S.A. as the country is not classified as being adequate. Safe Harbor was created in order to serve as a "backdoor" and to bypass the Directive 95/46/EC.
You have to know that Safe Harbor is only an agreement and not a Directive. It is a list of requirements, which were set up by the U.S. Department of Commerce. A firm only has to "say" that it applies to those requirements and self-certify that they apply to data protection standards equivalent of the ones of the EU. This self-certification can exist without legal consequences in case a company does not apply to those rules.

6. **Do you think that control agencies, such as the Federal Trade Commission are able to protect EU citizen's data, e.g. through sanctions?**

Sanctions? (he smiles). I do not believe that fines had ever been imposed on a company. The only effective way of controlling a company, which bypassed the rules, is to forbid the data transfer.
Microsoft for example processes data of EU firms in his cloud. If a U.S. court decides that this company/employee of this company is under the suspicion of collaborating with terrorist groups they are allowed to have access to this cloud, even if this data has been processed in the EU.
This decision does not fit together with the EU data protection standards and therefore the agreement cannot exist in this form anymore.

But who has the power to suspend or limit this agreement? This can only be decided by the founders of the agreement. The European Commission has the power to decide if the agreement can still exist. We have to know that Safe Harbor is not a law. It is not something the parliament could have voted on and until now the EC did not cancel or withdraw the agreement.
However at this moment a new EU data protection directive is being discussed. This is the time where the EU (European Parliament and EC) have to tackle this problem

7. **Do you believe that a new version of the agreement would guarantee the safety of EU citizen's personal data?**

This is something you need to discuss profoundly. There are two different points to consider:

1. Where is the data being processed? If I transfer data through fibre optic cables into the U.S. I know that the U.S. secret service can access and store my data (through programmes, such as PRISM). As long as you transfer data on this way (technical way) it is impossible to prevent the collection of personal data. This is why this data has to stay physically in Europe.
   This is why Microsoft already offers a cloud service in Ireland. That means that data of EU citizens is NOT transferred to the U.S. anymore. That is one example how the EU can physically protect itself because data does not has to be transported through fibre optic cables.

2. It's a fact that it is not possible to change the world with regulations. You would have to force the U.S to limit their mass surveillance actions. However, I do not have the feeling that anyone is able to get this under control

   Therefore I believe that physical security is of great importance. Legal protection just exist on paper and secret services are not bound to them

8. Do you see difficulties in the U.S. approach of self-regulation?

The European approach is completely different to the one of the U.S. Of course similar approaches exist in Europe as well, such as the legal approach of product laws.

You have to distinguish the kind of products or the kind of data you're talking about. If someone processes medical data, for example, it is not enough for Europeans in just trusting a company that they apply to EU law and its Directive.

The problem of self-regulation is that you cannot just say that they are definitely going to transfer data correctly, just because this would be contradictory to the company's interest (e.g. facebook). The American approach of self-regulation can be traced back the ideals of freedom. Europe on the other hand has a regulatory approach, which is completely different than the U.S. approach.

Just to make it clear and so you know where the problem lies I would like to tell you a little bit more about data protection details:

Firms want to use for example Microsoft Office Cloud for their company. Therefore the firm needs a form of agreement about the

Through the Safe Harbor agreement a security assessment can be ignored, because the agreement itself should guarantee a specific level of security. Therefore companies have to deal with less bureaucracy. If this is all functioning the way it should be has to be discussed.

The firm also has to weigh the interests of data protection and the interests of its company that this specific data transfer is extremely necessary for the company. But what kind of legal basis can this company base its decision on? It is not really in the mind of Europeans that a company can weigh money with data security interests.

That is why Microsoft installed a computing centre in Ireland. This is the place where the processing of personal data takes place. It is often the case that they have a so-called “support” in the U.S. who can have access to the computing centre at any time, if his help is needed and requested. This is also the reason why a so-called model clause exists. This clause allows that the processing of data stays in Europe, but co-workers who are based in the U.S. still have the power to access the computing centre, IF they are needed. This is one of the possibilities for Europe to protect itself with physical protection.

10.2.2. Informed Consent Form

Informed Consent Form

If you agree to take part in this study please read the following statement and sign this form.

I am 18 years of age or older.

I can confirm that I have read and understood the description and aims of this research.

The researcher has answered all the questions that I had to my satisfaction.

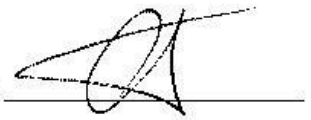
I agree to the audio recording of my interview with the researcher.

I understand that the researcher offers me the following guarantees: All information will be treated in the strictest confidence. My name will not be used in the study unless I give permission for it.

Recordings will be accessible only by the researcher. Unless otherwise agreed, anonymity will be ensured at all times. Pseudonyms will be used in the transcriptions.

I can ask for the recording to be stopped at any time and anything to be deleted from it.

I consent to take part in the research on the basis of the guarantees outlined above.

Signed:  Date: 8/5/2014

CHRISTOPH SCHÄFER

10.3. ANNEX II: Frequently Asked Questions (FAQs)

(source: European Parliament & Council: 2000, July 26)

FAQ 1 - Sensitive Data

Q: Must an organization always provide explicit (opt in) choice with respect to sensitive data?

A: No, such choice is not required where the processing is: (1) in the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide medical care or diagnosis; (4) carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (5) necessary to carry out the organization's obligations in the field of employment law; or (6) related to data that are manifestly made public by the individual.

FAQ 2 - Journalistic Exceptions

Q: Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, do the Safe Harbor Principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?

A: Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles.

FAQ 3 - Secondary Liability

Q: Are Internet Service Providers (ISPs), telecommunications carriers, or other organizations liable under the Safe Harbor Principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate their terms?

A: No. As is the case with the Directive itself, the safe harbor does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

FAQ 4 - Investment Banking and Audits

Q: The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. Under what circumstances is this permitted by the Notice, Choice, and Access Principles?

A: Investment bankers or auditors may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

FAQ 5 - The Role of the Data Protection Authorities

Q: How will companies that commit to cooperate with European Union Data Protection Authorities (DPAs) make those commitments and how will they be implemented?

A: Under the safe harbor, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Safe Harbor Principles. More specifically as set out in the Enforcement Principle, they must provide (a) recourse for individuals to whom the data relate, (b) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a) and (c) of the Enforcement Principle if it adheres to the requirements of this FAQ for cooperating with the DPAs.

An organization may commit to cooperate with the DPAs by declaring in its safe harbor certification to the Department of Commerce (see FAQ 6 on self-certification) that the organization:

1. elects to satisfy the requirement in points (a) and (c) of the Safe Harbor Enforcement Principle by committing to cooperate with the DPAs;

2. will cooperate with the DPAs in the investigation and resolution of complaints brought under the safe harbor; and

3. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

The cooperation of the DPAs will be provided in the form of information and advice in the following way:

- The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will inter alia help ensure a harmonized and coherent approach.

- The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the safe harbor. This advice will be designed to ensure that the Safe Harbor Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.

- The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for safe harbor purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.

- Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.

- The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.

- The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the Federal Trade Commission or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce (or its designee) so that the list of safe harbor participants can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Safe Harbor Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed USD 500 and will be less for smaller companies.

The option of co-operating with the DPAs will be available to organizations joining the safe harbor during a three-year period. The DPAs will reconsider this arrangement before the end of that period if the number of U.S. organizations choosing this option proves to be excessive.

FAQ 6 - Self-Certification

Q: How does an organization self-certify that it adheres to the Safe Harbor Principles?

A: Safe harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information:

1. name of organization, mailing address, e-mail address, telephone and fax numbers;

2. description of the activities of the organization with respect to personal information received from the EU; and

3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization is a member, (f) method of verification (e.g. in-house, third party)(1), and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organization wishes its safe harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ 9 and FAQ 5 as applicable and that it will comply with the advice given by such authorities.

The Department (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of safe harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. Such self-certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and safe harbor benefits will no longer be assured. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self-certify for the safe harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.

The undertaking to adhere to the Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the safe harbor. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the safe harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (1) continue to be bound by the Safe Harbor Principles by the operation of law governing the takeover or merger or (2) elect to self-certify its adherence to the Safe Harbor Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Safe Harbor Principles. Where neither (1) nor (2) applies, any data that has been acquired under the safe harbor must be promptly deleted.

An organization does not need to subject all personal information to the Safe Harbor Principles, but it must subject to the Safe Harbor Principles all personal data received from the EU after it joins the safe harbor.

FAQ 7 - Verification

Q: How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?

A: To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews.

Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

Organizations should retain their records on the implementation of their safe harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.

Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles, that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

FAQ 8 - Access

Access Principle:

Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated.

1. Q: Is the right of access absolute?

1. A: No. Under the safe Harbor Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

FAQ 9 - Human Resources

1. Q: Is the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the safe harbor?

1. A: Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in

the safe harbor, the transfer enjoys the benefits of the safe harbor. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

2. Q: How do the Notice and Choice Principles apply to such information?

2. A: A U.S. organization that has received employee information from the EU under the safe harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

FAQ 10 - Article 17 contracts

Q: When data is transferred from the EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the safe harbor?

A: Yes. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who determines the purposes and means of processing, who retains full responsibility for the data vis-à-vis the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the safe harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles).

Because adequate protection is provided by safe harbor participants, contracts with safe harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the safe harbor or otherwise not providing adequate protection.

FAQ 11 - Dispute Resolution and Enforcement

Q: How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organization's persistent failure to comply with the Principles be handled?

A: The Enforcement Principle sets out the requirements for safe harbor enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organizations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the

requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms.

Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record. As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Safe Harbor Principles(2). They should also co-operate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

Remedies and Sanctions.

The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances(3). Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee).

FTC Action.

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that is has reason(s) to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of Commerce of any such actions it takes. The Department of Commerce encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Safe Harbor Principles.

FAQ 12 - Choice - Timing of Opt Out

Q: Does the Choice Principle permit an individual to exercise choice only at the beginning of a relationship or at any time?

A: Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out". In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

FAQ 13 - Travel Information

Q: When can airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, be transferred to organizations located outside the EU?

A: Such information may be transferred in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (1) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (2) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the safe harbor provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Directive. Since the safe harbor includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to safe harbor participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

FAQ 14 - Pharmaceutical and Medical Products

1. Q: If personal data are collected in the EU and transferred to the United States for pharmaceutical research and/or other purposes, do Member State laws or the Safe Harbor Principles apply?

1. A: Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Safe Harbor Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

2. Q: Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the safe harbor, may the organization use the data for a new scientific research activity?

2. A: Yes, if appropriate notice and choice have been provided in the first instance. Such a notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

3. Q: What happens to an individual's data if a participant decides voluntarily or at the request of the sponsor to withdraw from the clinical trial?

3. A: Participants may decide or be asked to withdraw from a clinical trial at any time. Any data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

4. Q: Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Are similar transfers allowed to parties other than regulators, such as company locations and other researchers?

4. A: Yes, consistent with the Principles of Notice and Choice.

5. Q: To ensure objectivity in many clinical trials, participants, and often investigators, as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Will participants in such clinical trials (referred to as "blinded" studies) have access to the data on their treatment during the trial?

5. A: No, such access does not have to be provided to a participant if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring company.

6. Q: Does a pharmaceutical or medical device firm have to apply the Safe Harbor Principles with respect to notice, choice, onward transfer, and access in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices (e.g. a pacemaker)?

6. A: No, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers, to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

7. Q: Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he/she can identify the research subject under special circumstances (e.g. if follow-up medical attention is required). Does a transfer from the EU to the United States of data coded in this way constitute a transfer of personal data that is subject to the Safe Harbor Principles?

7. A: No. This would not constitute a transfer of personal data that would be subject to the Principles.

FAQ 15 - Public Record and Publicly Available Information

Q: Is it necessary to apply the Notice, Choice and Onward Transfer Principles to public record information or publicly available information?

A: It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.

Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the safe harbor.

(1) See FAQ 7 on verification.

(2) Dispute resolution bodies are not required to conform with the enforcement principle. They may also derogate from the Principles where they encounter conflicting obligations or explicit authorizations in the performance of ther specific tasks.

(3) Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used or disclosed information in blatant contravention of the Principles.

11. Appendix

11.1. Summary of Main Strengths of Directive 95/46/EC

(source: Robinson, 2009, p.40)

Table 1

Strengths	Evidence
Serves as reference model for good practice	Legislation that permits practical exercise of fundamental rights derived from ECHR, and considered a leading international model. Other privacy legislations adopt elements from the Directive e.g. Hong Kong, Canada, parts of Latin America
Harmonises data protection principles and to a certain extent enables an internal market for personal data	Implementation of legal rules across Europe for personal data processing that have greater compatibility than prior to the Directive's introduction
Flexible due to a principles-based framework	The Directive defines principles, without going into details for specific sectors/contexts. The exception to this rule is direct marketing
Technology neutral	No reference to specific technologies Security measures not specified Concept of personal data broad enough to be technologically neutral
Improves general awareness of privacy issues	Establishment and increasing numbers of privacy policies, privacy officers, etc. Consumer awareness regarding privacy

11.2. Summary of main weaknesses of Directive 95/46/EC

(source: Robinson, 2009, p.44)

Table 2

Weaknesses	Evidence
The link between the concept of personal data and real risks is unclear	The application scope of the Directive depends too strongly on whether or not the data processed can be defined as "personal" data. It is all or nothing: there is no room for "more or less personal" data (and accordingly "more or less protection"). Special categories of personal data processing are explicitly defined; but financial information and location data are not classified as sensitive. Strict application of the Directive's concepts sometimes leads to unpredictable or counterintuitive results.
Measures aimed at providing transparency of data processing through better information and notification are inconsistent and ineffective	Privacy policies not read in practice, as they are aimed at consumers yet written by/for lawyers Privacy policies do not play a role as a market differentiator Unclear purpose of notification Variety of 20 different notification processes, variety of exemption rules Uneven implementation of the process of registration
The rules on data export and transfer to third countries are outmoded	Definition of 'third countries' is perceived as outmoded in the light of globalisation Adequacy of countries is not relevant to business realities or to data protection Regulation in some other countries is stronger than the

	EU, but still not recognised as adequate
The tools providing for transfer of data to third countries are cumbersome	Length of time and effort required to get Standard Contractual Clauses, model contracts or Binding Corporate Rules approved is excessive Uneven practices of approval and authorisation; too little coordination between the Member States
The role of DPAs in accountability and enforcement is inconsistent	Unclear rationale for enforcement Uneven implementation of enforcement across Member States either for punishment or to affect behaviours Differing criteria for imposing sanctions
The definition of entities involved in processing and managing personal data is simplistic and static	Globalisation and increased re-use of personal data has outpaced the static definitions of controller and processor.

11.3. European Data Protection Principle

(source: Robinson, 2009, p.26)

Table 3

Goal	OECD Guidelines	Relevant article in the Directive
Legitimacy	Collection limitation principle	Article 6 (b) Article 7: criteria for Legitimacy
Purpose restriction (which implies data quality, purpose specification and proportionality)	Data quality principle, purpose specification principle and use limitation principle	Art. 6: purpose and use restrictions, and quality/accuracy requirements
Security and confidentiality	Security safeguards principle	Art. 16-17: Confidentiality and security of processing
Transparency	Openness principle	Art. 10 & Art. 11: the right to information regarding essential aspects of the data processing
Data subject participation	Individual participation principle	Art. 12: right to access, which is sometimes coupled with the right to correct or delete the data
Accountability	Accountability principle	Art. 22-23: rules on remedies and liability