University of Zurich
Faculty of Law

Seminar on Data Protection

Essay:
Safe Harbour Agreements and Cross Border Data Transfer

Prof. R. H. Weber (University of Zurich)
Prof. P. Schwartz (University of California, Berkley)

submitted by

Sascha Zaman

mail@sascha-zaman.com
http://sascha-zaman.blogspot.com/

6th Semester
Bachelor of laws
FS 12

Contents

Bibliography

BHEND-RUTISHAUSER JULIA, Safe Harbour: Globaler Datenumschlagplatz?, in: Digma (2011) 122

CAREY PETER, Data Protection – A Practical Guide to UK and EU Law, 3rd edn, Oxford 2009

DAMMANN ULRICH/ SIMITIS SPIROS, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997

DÄUBLER WOLFGANG/ KLEBE THOMAS/ WEDDE PETER/ SCHAAR PETER, Kompaktkommentar zum Bundesdatenschutzgesetz, 3rd edn., Frankfurt am Main 2009

EHMANN EUGEN/ HELFRICH MARKUS, EG-Datenschutzrichtlinie, Kurzkommentar, Cologne 1999

ENGEL ALEXANDRA, Reichweite und Umsetzung des Datenschutzes gemäß der Richtlinie 95/46/EG für aus der Europäischen Union in Drittländer exportierte Daten am Beispiel der USA, diss, Berlin 2003 <http://www.diss.fu-berlin.de/diss/content/below/index.xml>

FARRELL HENRY, Constructing the International Foundations of E-Commerce: The U.S.-EU Safe Harbor Arrangement, in: International Organization (2003) 277 (quot. as FARELL, Constructing the International Foundations of E-Commerce) <http://www.henryfarrell.net/cv.html>

FARRELL HENRY, Negotiating Privacy across Arenas – The U.S.-EU Safe Harbor Discussions, in: Common Goods: Reinventing European and International Governance (2002) 101 (quot. as FARRELL, Negotiating Privacy across Arenas) <*http://www.henryfarrell.net/cv.html*>

FDPIC, Erläuterungen zur Übermittlung von Personendaten ins Ausland <*http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de*>

GENZ ALEXANDER, Datenschutz in Europa und den USA, Diss, Wiesbaden 2004

KOBRIN STEPHEN J, Safe Harbours are hard to find: the Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance, in: Review of International Studies (2004) 111 <*http://mgmt.wharton.upenn.edu/people/publications.cfm?id=1334*>

MARNAU NINJA/ SCHLEHAHN EVA, Cloud Computing und Safe Harbour, in: Datenschutz und Datensicherheit (2011) 311

RÄTHER PHILIPP/ SEITZ NICOLAI, Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, in: Multimedia und Recht (2002) 425

ROSENTHAL DAVID/ JÖHRI YVONNE, Handkommentar zum Datenschutzgesetz, Zürich/ Basel/ Geneva 2008

SCHNEIDER JÜRG, Personendaten-Transfer in die USA, in: Digma (2009) 126

SIMITIS SPIROS (ed.) et al, Kommentar zum Bundesdatenschutzgesetz, 6th edn, Baden-Baden 2006

TALIDOU ZOI, Regulierte Selbstregulierung im Bereich des Datenschutzes, in: Europäische Hochschulschriften. Reihe II: Rechtswissenschaft, Diss, Frankfurt am Main/ Berlin/ Berne/ Bruxelles/ New York/ Oxford/ Vienna 2005

Abbreviations

Cf	See, compare (confer)
Decision	Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L215/7
Directive	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, [1995] OJ L281/31
Diss	Dissertation
DPA	(European) Data Protection Authority
ECJ	European Court of Justice of the European Union
Ed	Edited
Edn	Edition
Eds	Editors
EEA	European Economic Area
Eg	For example
Et al	And others
Etc	Et cetera = and so on
EU	European Union
FADP	(Federal) Act on Data Protection in Switzerland (SR 235.1)
FDPIC	The Federal Data and Information Commissioner in Switzerland
FDPO	Ordinance to the (Federal) Act on Data Protection in Switzerland (SR 135.11)
FF	And the following page(s)
Fn	Footnote
FTC	Federal Trade Commission
ITA	International Trade Administration
Lit	Literatura

N	Number
OJ	Official Journal of the European Union
Quot	Quoted as
U.S.	Unites States
WP	Working Paper authored by the Art. 29 Data Protection Working Party

1. Introduction

Data transfer between Europe and the USA has been an increasing topic in the media: whether it was the dispute between German DPA's and Facebook over the "like-button",[1] Austrian students demanding to know which data is stored by Facebook[2] or the recent struggle over Google's Privacy Policy.[3] Facebook's worth is estimated somewhere between 85 and 100 billion dollars,[4] most of its value coming from marketing. Personalized marketing with the use of collected and evaluated data from users has become an increasing business.

The European Commission (Commission) launched a survey in the European Union and asked people whether they were concerned about the whereabouts of their data. The result: 72 percent of internet users do not feel in complete control of their data and fear that they give away too much information.[5] Addresses, photos, credit card – and telephone numbers: with the fast development of new technologies, data is spread around the globe within seconds. Many times not even the providers themselves know exactly which data is stored where. With the increasing use of cloud computing,[6] the spread of data might reach a new high.

What bothers a lot of people in Europe is that most countries outside the European Union, the European Economic Area or Switzerland do not provide an equal level of data protection: once the data has left, pretty much anything

1 Cf <https://www.datenschutzzentrum.de/presse/20110819-facebook.htm>.

2 Cf <http://derstandard.at/1313024892837/Anzeigen-Datenschutz-Wiener-Studenten-klagen-gegen-Facebook>.

3 Cf <http://www.google.com/intl/en/policies/privacy/>.

4 Cf <http://www.faz.net/aktuell/wirtschaft/vor-dem-boersengang-der-wert-von-facebook-11636569.html>.

5 The survey can be downloaded at <http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm#359>.

6 For a short explanation on cloud computing cf <http://www.edoeb.admin.ch/themen/00794/01124/01768/index.html>.

can happen. This, although data transport from Europe[7] into any third country underlies specific restrictions under various data protections laws. In this context, both the European Union and Switzerland have negotiated so called "Safe Harbour Agreements" to regulate the data flow from Europe into the U.S. This essay will examine these Agreements, discuss their contents and review their enforcements.

The next chapter will shortly discuss how data transfer into third countries is generally regulated within the European Union/ EEA and in Switzerland (2.). Next, the Safe Harbour Agreements will be examined: how they were negotiated (3.), their contents (4.) and the reality that comes with their enforcements (5.). At last, a summarizing conclusion will be drawn (6.). In an essay of this scope, not all details can be discussed. Therefore referrals for further information will be provided wherever possible (all hyperlinks referring to websites were accessed the last time on March 13, 2012.)

2. Data Transfer into Third Countries

2.1. European Union

In 1995, the Directive 95/46 for protecting personal data was enacted. With the progressing integration of the European internal market, a need for an equivalent level of data protection arose: data like banking details or personal data of employees were sent throughout the European Union, but every Member State had different levels of data protection. This is why especially the Member States – contrary to the Commission – demanded an equal level of data protection within the European Union.[8]

Art. 25 and 26 of the Directive regulate the transfer of personal data out of the European Union/ EEA into third countries. In order to fulfill an absolute adequacy with the Directive it would have been necessary that all organizations

7 The term Europe in this essay refers – unless otherwise stated – to the EU, the EEA and Switzerland.

8 DAMMANN/ SIMITIS, EG-Datenschutzrichtlinie, 61 N 1 ff.

receiving data from within the EU/ EEA must provide an equal level of data protection.[9] The Commission realized soon that this was hardly an option and so Art. 25 I of the Directive in its version today constitutes that "the transfer to a third country of personal data... may take place only if... the third country in question provides an *adequate* level of protection" (the term adequate has been substituted for the term equivalent after heavy lobbying from business companies[10]).[11] If a third country has no adequate level of protection, a transfer into this country is only possible, if one of the derogations of art. 26 applies; the derogations are final.[12]

The Directive does not define the term *transfer to a third country,* which caused several problems especially with the developing use of the Internet. The ECJ had to decide in the case Lindqvist,[13] whether uploading information on a website means transfer to a third country, as theoretically everybody around the world has the possibility to see this data. The ECJ found that this is not the case, because this would have meant that every upload was a potential violation of the Directive: as soon as the Commission finds that only one country does not provide adequate data protection, all Member States would be required to stop uploads onto a website, if in this specific third country people have access to the Internet (consideration n 69 – 70). This very important decision by the ECJ limits the scope of the Directive to a large amount.

The Commission may find that a third country does or does not ensure an adequate level of protection (25 IV and VI of the Directive). The decision must not necessarily be "all or nothing": it may find that a state provides generally no adequate protection but does so in one specific sector.[14] Up until now, it

9 The Directive was extended to the EEA, cf "Miscellaneous information <*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT*>

10 Farrell, Negotiating Privacy across Arenas 120 fn 10.

11 Ehmann/Helfrich, EG-Datenschutzrichtlinie, 287 N 2.

12 Engel, Reichweite und Umsetzung 176.

13 Case C-101/01, *Lindqvist*, European Court reports 2003 I-1297.

14 Genz, Datenschutz 26.

found that the following states provide an adequate protection under the Directive: Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, Isle of men, Israel, Jersey, Switzerland, the U.S. Department of Commerce's Safe Harbour Privacy Principles and the Transfer of Air Passengers Name Record to the United States' Bureau of Customs and Border Protection.[15]

2.2. Switzerland

In Switzerland, the FADP regulates data transfer into third countries in art. 6. Its systematic is similar to art. 25 and 26 of the Directive: art. 6 I constitutes that no data may be disclosed abroad if the privacy of the data subject would be seriously endangered thereby, *in particular due to the absence of legislation that guarantees adequate protection*. The term disclosure is defined (contrary to the Directive) in art. 3 lit f FADP: making personal data accessible, for example by permitting access, transmission or publication. Contrary to the Directive, the FAPD is also applicable for legal persons (art. 2 I FADP). Yet, in Switzerland also, uploading data onto a website is not considered as disclosure into a third country under art. 6 FADP (art. 5 FDPO).

If a third country provides no adequate protection, data may only be transferred if protection is guaranteed otherwise (art. 6 II lit a and g FADP). If such guarantees cannot be made, data transfer may only occur if the they fall under art. 6 II lit b – f FADP.[16] The FDPIC – like the Commission – has published a list on his website with states that he finds to have a sufficient level of data protection under art. 6 I FADP.[17] The list is identical to the list published by the Commission except for New Zealand, which the FDPIC also finds to have an adequate level of protection. But the Art. 29 Data Protection Working Party (Art. 29 Working Party) has also published an opinion that New Zealand provides adequate protection under art. 25 of the Directive.[18]

15 Cf <http://ec.europa.eu/justice/data-protection/law/index_en.htm>.

16 FDPIC, Erläuterungen zur Übermittlung von Personendaten ins Ausland 5.

17 Cf <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de>.

3. Creation of the Safe Harbour Agreements

3.1. U.S.-EU Safe Harbour Agreement

a) Development since the Enactment of the Directive

The Safe Harbour Agreements, especially from a European point of view, are untypical legal documents and can be very confusing when examining them the first time. To understand them, it is helpful to review how they came into existence.

In the U.S. and Europe, the approach on how to regulate data transfer differs to a great extend: whereas in Europe, privacy is considered a fundamental right (and therefore must be protected through formal legislation),[19] in the U.S., the absence of formal legislation in the area of data protection (on a level like Europe has), is the result of a philosophical concept of a state that should only be involved if absolutely necessary.[20] Personal data in the U.S. is considered more of an alienable commodity subject to the market.[21]

After the Directive 95/46 had been enacted, it became clear that the U.S. – one of Europe's most important trade partner – would not match the requirements under the art. 25 of the Directive.[22] The finding however, on what grounds the Commission decided that the U.S. would not qualify as a state with adequate data protection, was informal and is not published.[23] Consequently, all data flows from Member States of the EU/ EEA into the U.S. should have been

18 WP 182, Opinion 11/2011 on the level of protection of personal data in New Zealand <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm>.

19 Cf art 8 I of the Charter of the EU (Charter of the Fundamental Rights of the European Union of the European Parliament, the Council and the Commission, [2000] OJ C364/8.

20 The U.S. has several individual regulations on data protection which only apply to a limited area, cf Genz, Datenschutz 39 ff.

21 Kobrin, Safe Harbours are hard to find 116.

22 Farrell, Negotiating Privacy across Arenas 106.

23 Genz, Datenschutz 129 fn 474.

stopped (art. 25 IV of the Directive), if they do not fall under one of the derogations of art. 26 of the Directive. Considering that this was a time when the internet started to boom exponentially, this could have meant serious political and economical consequences.

But the Directive gives the Commission the possibility to enter into negotiations with the U.S. and declare them as a state with adequate data protection, if some form of commitments by the U.S. could be achieved (25 V and VI of the Directive). The problem was that two very different approaches on how to handle data protection clashed into each other: the U.S. favored forms of self-regulation in this area. Major U.S. lawmakers considered the Directive as a threat to commercial interests and argued that European data protection standards should not be used to establish data protection in the USA.[24] Many also argued that the EU established extraterritorial legislation, as especially with the internet, the Directive would apply to every country around the globe.[25] But representatives of the EU demanded primarily formal legislation and considered self regulation in the U.S. insufficient.[26] Neither side could back down: formal legislations was politically not possible in the U.S. and the European representatives were bound by the Directive. Finally, after eighteen months of negotiations, the U.S. proposed a system, in which not the entire U.S., but rather a set of firms could voluntarily agree to uphold some forms of privacy principles and therefore enter a so called "Safe Harbour". With this proposal, the basis for a common ground was set.[27]

b) Commission's Decision

Consequently, the Commission decided in June 26, 2000 that U.S. companies certified under the so called "U.S.-EU Safe Harbour Agreement" provide adequate data protection under art. 25 I and II of the Directive, if they:

24 FARRELL, Negotiating Privacy across Arenas 108 ff.

25 KOBRIN, Safe Harbours are hard to find 122 ff.

26 FARELL, Constructing the International Foundations of E-Commerce 285 ff.

27 KOBRIN, Safe Harbours are hard to find 120.

1. Comply with the U.S.-EU Safe Harbour Principles (Principles);
2. Uphold the complimentary Frequently asked questions (FAQ's);
3. Publicly disclose their privacy policy and
4. Are subject to the jurisdiction of the FTC or the U.S. Department of Transportation (cf. Annex 7 of the decision).[28]

The conditions are met as soon as an organization discloses the US Department of Commerce its commitment and gives notice of the government body under which jurisdiction it falls (art. 1 III of the decision). The FTC publishes a list with all participating members of the U.S.-EU Safe Harbour Agreement (consideration n 7 of the decision, FAQ 6).[29]

But the Commission also made some reservations: under specific circumstances, national DPA's may still prevent data transfer to a specific organization, if (art. 3 of the decision):

1. The U.S. institution in charge found that the organization in question fails to comply with the Agreement or there is a substantial likelihood that it will do so;
2. The U.S. institution in charge cannot enforce its powers in adequate time or properly;
3. The continuing transfer would create an imminent risk and
4. The European authority in charge gave the organization an adequate opportunity to respond.

Further reservations were made in case the U.S. authorities in charge would not properly overview compliance with the Safe Harbour Agreements: the Commission will then inform the U.S. Department of Commerce and, if necessary, present drafts to alter the Agreement.

28 Art. 1 of the decision.

29 The list is published at <http://safeharbor.export.gov/list.aspx>.

3.2. The U.S.- Swiss Safe Harbour Agreement

In December 2008, the FDPIC signed an exchange of letters between him and U.S. Department of Commerce on the creation of a "U.S.-Swiss Safe Harbour Framework", which is based on the U.S.-EU Safe Harbour Agreement and therefore almost identical to it. The intension was to simplify the transfer of personal data from Switzerland into the USA.[30] Before the Agreement was enacted, the parties (data exporter and importer) had to agree on upholding the FADP, eg by contractual clauses (art. 6 II lit a FADP).

4. Contents of the Safe Harbour Agreements

4.1. The U.S.-EU Safe Harbour Agreement

a) Overview on the Safe Harbour Documents

According to the Commission's decision, the U.S.-EU Safe Harbour Framework consists of the following documents:

1. The Safe Harbour Principles (Annex I)
2. The Frequently Asked Questions (FAQ's) (Annex II)
3. A Safe Harbor Enforcement Overview (Annex III)
4. Memorandum by the Department of Commerce on Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law (Annex IV)
5. A letter from the FTC concerning its jurisdiction over consumer privacy issues (Annex V)
6. A letter from the Department of Transportation concerning its authority in protecting the privacy of consumers with respect to information provided to airlines (Annex VI) and

30 Cf FDPIC, Press Release from December, 9 2008 <http://www.news.admin.ch/message/index.html?lang=en&msg-id=23809)>.

7. U.S. government bodies recognized by the EU empowered to investigate complaints (Annex VII).

On the website of the ITA a slightly different order of documents is published: it consists of Annex I-VI, but additionally includes two letters from Acting Under Secretary for ITA Robert S. LaRussa: one addressed to his colleagues on the establishment of a U.S.-EU Safe Harbour Agreement and another to the Commission transmitting the Safe Harbour Privacy Framework. Annex VII on the other hand, is not published.[31] It was included by the Commission as a reaction to concerns in the U.S. that the Safe Harbour Agreement would classify U.S. citizens to 2nd class citizens with regard to data protection.[32] It now explicitly declares that the FTC may enforce the Principles for anyone, regardless of nationality or residency.

GENZ notes that only the Commission's decision makes the Safe Harbour Framework legally binding. Hence, the decision itself must also be considered part of the U.S.-EU Safe Harbour Agreement. The center of the Safe Harbour Agreement therefore consists of the seven Principles (Annex I), the FAQ's (Annex II) and the Commission's decision.[33]

b) The Principles, FAQ'S and Annexes III – VII

To qualify for the U.S.-EU Safe Harbour Agreement, an institution has three possibilities (Annex I): it may join a self-regulatory privacy program which adheres to the Principles, or it may develop its own self-regulatory privacy policies. When it chooses the latter, a failure to comply with its commitments must be actionable under Section 5 of the Federal Trade Commission Act or another regulation with equivalent regulations. A third way to qualify is that the specific organization is subject to other rules which effectively protect personal privacy. With regard to the different approaches on data protection in the U.S.

31 Cf <http://export.gov/safeharbor/eu/eg_main_018493.asp>.

32 GENZ, Datenschutz 151.

33 GENZ, Datenschutz 130.

and Europe, most organizations will not fall under the third option.[34] This enumeration for qualification possibilities also means that major economic institutes, such as financial and telecommunication companies, cannot join the Safe Harbour Agreements (Annex III and VII).

The Principles (Annex I) require the following:

Notice: Every organization must inform individuals why it collects or uses information about them and to which third parties it plans to transfer the information. Additionally, it must provide a mechanism to contact the organization.

Choice: The organization must offer an opportunity to choose ("opt out"), whether personal information may be disclosed to a third party or whether data may be used for further purposes as originally intended. These mechanisms must be simple and affordable.

With sensitive data (eg information about race, sex or religion), the individual must have an affirmative or explicit ("opt in") choice (the German translation only speaks of an *explicit* choice). If an organization receives information from a third party, it should treat the data as sensitive, if the third party did so as well.

Onward Transfer: If information is transferred to a third party, the organization must apply the "Notice" and "Choice" Principles. Where an organization wishes to transfer information to a third party that only acts as an agent, it may do so if the third party also fulfills the requirements of the Directive.

Security: Organizations must take reasonable precautions to protect data from loss, misuse etc.

Data Integrity: The collected personal information must be necessary. An organization should take reasonable steps to ensure that the data is reliable for

34 ENGEL, Reichweite und Umsetzung 139.

its intended use (*should* is translated in German with *must*). Furthermore, the data must be accurate, complete, and current.

Access: Individuals must have access to personal information and they must be able to correct, amend or delete wrong information, as long as this process is not disproportionate for the organization.

Enforcement: The organization must establish effective mechanisms for assuring compliance, recourse and consequences. Such mechanisms must include at least:

1. Affordable independent recourses by which the individual may not only investigate, but also resolve disputes. Damages must be awarded where the applicable law provides this possibility;
2. Control mechanisms to verify the correctness and implementation of the assertions the organizations made;
3. Obligations to solve problems which arose out of non-compliance by an organization with its self-declaration. Sanctions must ensure that organizations comply with the Principles.[35]

The FAQ's (Annex II) explain some of the Principles more detailed in a form of fictive questions – answers role-play. Although for Europeans rather unusual, they are legally as binding as the Principles (art. 1 I of the decision). The chronology of the FAQ's lacks a clear systematic.[36]

At last, **Annex III to VII** have a describing function: primarily they are – contrary to the Annex I and II – not addressed to data exporters and importers but the European Commission.[37] The letters explain in a general way the functions, jurisdiction and enforcement of both the FTC and the Department of Transportation, together with some examples of previous cases especially in the area of data protection.

35 For a detailed analysis of the Principles cf GENZ, Datenschutz 135 ff; ENGEL, Reichweite und Umsetzung 143 ff.

36 GENZ, Datenschutz 142.

37 GENZ, Datenschutz 142.

4.2. The U.S.-Swiss Safe Harbour Agreement

The U.S.-Swiss Safe Harbour Framework consists of equivalent documents to the U.S.-EU Safe Harbour Framework:

1. A letter from the U.S. Department of Commerce to the FDPIC together with five Annexes which provide the Safe Harbour Framework. The Annexes, almost identical to the U.S.-EU Agreement, consist of the Safe Harbour Principles (Annex I), the FAQ's (Annex II), a Safe Harbor Enforcement Overview (Annex II), a Memorandum by the Department of Commerce on Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law (Annex IV) and the U.S. government bodies recognized by Switzerland empowered to investigate complaints (Annex V);

2. A letter from the FTC to the FDPIC;

3. A letter from the Department of Transportation to the FDPIC and

4. An answering letter from the FDPIC to the Department of Commerce.[38]

Similarly to the U.S.-EU Safe Harbour Agreement, only the decision from the FDPIC (in the answering letter to the Department of Commerce) to accept the Safe Harbour Framework as adequate protection under art. 6 I FADP constitutes that certified organizations in fact provide adequate data protection. Hence, the Principles (Annex I), the FAQ's (Annex II) together with the answering letter of the FDPIC to the Department of Commerce build the core of the U.S.-Swiss Safe Harbour Agreement.

38 The letters are available at <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=en>.

The U.S.-Swiss Safe Harbour Agreement is only applicable for personal data (cf Annex I). And although almost identical, the U.S.-EU and the U.S.-Swiss Safe Harbour Agreements must be separated: organizations which are certified under the U.S.-EU Safe Harbour Agreement are not automatically certified for the U.S.-Swiss Safe Harbour Agreement.[39] This means that an organization, which is certified under the U.S.-EU Agreement, does not provide adequate protection under art. 6 I FADP, but may – under additional prerequisites – fall under the derogation of art. 6 II lit a FADP. To qualify, it must declare to uphold the Principles also for personal data from Switzerland, the person living in Switzerland must have the same rights as a EU citizen would have and the minimum requirements are actually upheld.[40]

5. Enforcement, Criticism and Appraisal of the Safe Harbour Agreements

5.1. Enforcement by European DPA's

According to the Commission's decision, data can be transferred to participating members of the Safe Harbour Agreement without any further requirements (consideration n 2 of the decision). But various DPA's interpret the Safe Harbour Agreements only as a presumption that the certified organizations provide adequate data protection. SIMITIS sees art. 3 I of the decision as a delegation from the Commission to the DPA's and therefore wants an individual check, whether the Safe Harbour Principles are actually upheld.[41] In 2010, the German "Düsseldorfer Kreis" (an informal gathering of the German DPA's) also demanded that every data exporter checks individually, whether the organization in question actually upholds the Safe Harbour Principles.[42] The FDPIC in his press release stated:

39 Cf <http://export.gov/safeharbor/swiss/index.asp>.

40 ROSENTHAL, Handkommentar, Art 6 N 49.

41 SIMITIS et al (-SIMITIS), BDSG § 4b N 79.

"*For companies in Switzerland this system* (The U.S.-Swiss Safe Harbour Agreement) *has the advantage that when dealing with certified US companies, they are no longer required to negotiate an agreement or notify the FDPIC.* "[43]

But in another document on the same website he also mentions that data exporters should verify the Safe Harbour list and, if necessary, install additional contractual clauses.[44] So if the data exporter comes to the conclusion that the U.S.-Swiss Safe Harbour Agreement is not upheld properly by the organization in question, data transfer can only occur under the derogations in 6 II FADP (eg via standard contractual clauses).[45]

One of the reasons for this uncertainty in the EU is that it is disputed whether the Safe Harbour Agreements are binding for national DPA's. The Directive merely constitutes that the Member States "shall take the measures necessary to comply with the Commission's decision" (art. 25 VI of the Directive). As this term is vague, many DPA's argue that they are not obliged to comply with the decision.[46] Many also question whether the Commission has the legal competence to make binding decisions for all Member States, based solely on a Directive.[47] In Switzerland, the FDPIC argues that in some scenarios data disclosure to an organization in a third country might be permissible under art. 6 I FADP, yet the transfer would still violate other articles of the FADP (this is also the case for the EU[48]).[49]

42 Resolution of the "Düsseldorfer Kreis" from April 28/ 29, 2010 <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html?nn=409242>.

43 FDPIC, Press Release from December, 9 2008.

44 FDPIC, Erläuterungen zur Übermittlung von Personendaten ins Ausland 6;

45 Schneider Jürg, Personendaten-Transfer in die USA 127; Bhend, Safe Harbour 125.

46 Däubler/ Klebe/ Wedde/ Schaar (-DÄUBLER), Bundesdatenschutzgesetz § 4b N 16.

47 Cf Simitis et al (-SIMITIS), BDSG § 4b N 70 ff.

48 Cf art. 25 I of the Directive: "...pursuant to the other provisions of this Directive...".

49 FDPIC, Erläuterungen zur Übermittlung von Personendaten ins Ausland, 6.

The uncertainty about the actual legal bindingness of the Safe Harbour Agreements makes it difficult for data ex- and importers to know, whether they can rely on the Agreements. Although their legal qualification (and therefore bindingness) may yet to be defined,[50] considering that one of the main ideas of the Safe Harbour Agreements was that organizations do not have to think on how to uphold European data protection laws after certification,[51] delegating the burden to verify whether an organization actually upholds the Safe Harbour Principles seems questionable. Accordingly, the majority of the doctrine seems to consider U.S. companies certified under the Safe Harbour Agreements as adequate and data can be transferred to them without any further requirements.[52]

In this context, the Commission has published a proposal on a new Data Regulation for the EU/ EEA in January 2012.[53] The proposal is constructed as a R*egulation* – contrary to the current *Directive* – which, if enacted, makes it directly applicable in every Member State (art. 288 of the Treaty on the functioning of the European Union).[54] This can be interpreted as an approach of the Commission to at least partially resolve some issues on the question whether the Commission's decisions are binding for the Member States. Art. 40 – 45 of the proposal regulate data transfer into third countries. The Commission still may find that a third country provides adequate level of protection. And if it does so, the transfer "shall not require any further

50 For a detailed analysis cf Genz, Datenschutz 158 ff and Talidou Zoi, Regulierte Selbstregulierung im Bereich des Datenschutzes 166 ff.

51 Räther/ Seitz, Übermittlung 429.

52 Carey, Data Protection 110; Engel, Reichweite und Umsetzung 137;
Genz, Datenschutz 156; Räther/ Seitz, Übermittlung 428.

53 The proposal as well as further information on the reform is available at <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.

54 Consolidated version of the Treaty of the Functioning of the European Union, [2008] OJ C115/47.

authorization." Whether the new regulation puts an end to the dispute must be awaited. A final solution might be to let the ECJ decide.[55]

5.2. Criticism

Ever since its enactment, the U.S.-EU Safe Harbour Agreement has been criticized from European DPA's and EU institutions.

Although the Commission's decision formally relied on the recommendations of the Art. 29 Working Party (consideration n 11 of the decision), the Party did not find that the U.S.-EU Safe Harbour Agreement provide an adequate level of protection per se: in its latest opinion shortly before the Commission's decision, it stated that it "remains concerned on a number of issues on which it believes a better standard in terms of data protection is achievable."[56]

SIMITIS criticizes that most of the Principles and FAQ's are written so vague that it is not in accordance with the Directive. He also criticizes the absence of a proper regulation on damages. He then notes that an organization wishing to participate has no obligation but to declare to uphold the Principles. Whether they actually fulfill the (especially technical) requirements, is not checked.[57]

MARNAU/ SCHLEHAN criticize the way organizations can join: most of the organizations choose a privacy policy instead of joining a self-regulatory privacy program, because that way they can write privacy policies based on their own demands. Also, they find it insufficient that various members of the Agreement limit the Safe Harbour Principles to one kind of Data. All other data transferred to them are not covered under the Safe Harbour Agreements. They further criticize the U.S. authorities, as the Website of the ITA lists all Safe Harbour members, even those, whose certification is not up to date. Finally,

55 DÄUBLER/ KLEBE/ WEDDE/ SCHAAR (-DÄUBLER), Bundesdatenschutzgesetz § 4b N 16.

56 WP 32, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles" <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>.

57 SIMITIS et al (-Simitis), BDSG § 4b N 73 ff.

they criticize the dispute resolution mechanisms, as many are – contrary to what the Principles demand – very costly for the individual.[58]

GENZ questions the effectiveness of a self-certification program which is not re-examined. He also criticizes the compliance program: although FAQ 7 foresees the possibility of an external compliance review, it is still in the hands of the organization when it wishes to be examined. With regard to the enforcement, he criticizes that the U.S. authorities can only act on unfair or deceptive acts and practices. He further argues that the FTC might not even have the authority to act solely on behalf of European citizens or even act on data protection matters at all. And lastly, the fact that under the Safe Harbour Principles an organization does not have to have the subject's consent to process data (but only has to inform him), is critical with regard to art. 7 I of the Directive.[59]

RÄTHER/SEITZ criticize especially that the Principles of Notice, Access and Enforcement are not implemented as it would be necessary under the Directive.[60]

A study in 2008 by CONNOLLY[61] revealed that the U.S. website claimed that nearly 1700 companies joined the Safe Harbour program. In reality, only 1597 were listed and 342 of those were marked as "not current". Only 348 actually upheld the most basic requirements. Many companies also make claims which might give readers a wrong impression (eg suggesting they have been *awarded* by the Department of Commerce although Safe Harbour requires only self-certification). Also, many organizations draft their own "Safe Harbour Marks" and publish them on their website.

58 MARNAU/ SCHLEHAHN, Cloud Computing und Safe Harbour 313 ff.

59 GENZ, Datenschutz 157.

60 RÄTHER/ SEITZ, Übermittlung 430.

61 CONNOLLY CHRIS, Safe Harbour – Fact or Fiction?
<http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/>.

5.3. Final Appraisal

Some of the Principles are formulated very vague (eg with terms like *affordable, should and reasonable*), which leaves great room for interpretation. For example, with the Principle of "Choice", an organization must only offer the subject a possibility to "opt-out", whether personal data may be transferred to any third parties or used for further purposes. Implicitly this means that data may be used for other purposes than originally intended, as long as the organization informs the individual afterwards (eg via changing its general terms and conditions). It is not written how organizations must define an affordable mechanism.

Furthermore, several FAQ's seem to limit the Principles. For example may an organization use sensitive data for other purposes than usually collected, if the individual has publicly disclosed the information (FAQ 1). FAQ 6 explicitly states that every organization must validate its self-certification every year, otherwise it will not benefit from Safe Harbour. Yet, on the website of the ITA, an organization which has no valid certification is only marked as "not current".[62] FAQ 7 explains the verification process: an organization has the possibility to either verify its compliance through self-assessment, or via an outside compliance review. Both *should* be done annually, and the documents *should* be retained. FAQ 8 lists the exceptions under which the organization does not have to grant individuals access to their data. It is also explicitly mentioned that organizations have the possibility to charge people for the Principle of "Access" (FAQ 8 Answer 6). FAQ 11 explains how the dispute resolution and enforcement mechanisms *should* be implemented. While three possibilities are listed, it also states that the list is not final. An organization may use other procedures constructed to its own fittings. And lastly, FAQ 12 explains that an organization may very well use data for direct marketing – as long as it informs the subject afterwards –, if prior information to the individual might be *impractical* (here, the German translation states "impossible"), RÄTHER/ SEITZ note in this context, the organization simply has to inform the

62 Cf http://safeharbor.export.gov/list.aspx.

subject, but it does not have to wait for an answer. In many cases, the subject may not even notice the information.[63]

Also, the self-certification process leaves the organizations a wide possibility on their commitments: Facebook for example joined the TRUSTe Privacy Program, verifies itself through it and has its dispute resolution via TRUSTe. Google on the other hand has no privacy program, verifies itself by in-house verification and has its dispute resolution via DPA's.[64] Google explains which data it *typically* collects. Yet it is not clear, what they do with it ("...Theses purposes *may* include any of the following"). Facebook on the other hand does not even mention what it intends to do with received data.

And finally, also other, less technical problems occur: even if someone from Europe has decided to sue an organization for a violation of the Principles, he or she would most likely still have to travel to the U.S. and bear the expenses. It is questionable, whether somebody would take these (financial) risks for a violation of the Safe Harbour Agreements.

6. Conclusion

Europe has data protection laws which restrict data transfers into third countries to a great extend. The U.S. does not provide adequate data protection from a European point of view. To regulate data flow into the U.S., both the EU and Switzerland have negotiated so called "Safe Harbour Agreements" with the U.S. authorities. The Agreements base on the idea that organizations may voluntarily uphold data protection principles – and therefore provide a "Safe Harbour" for European data. After being certified, the specific organization is regarded to provide adequate data protection.

The Safe Harbour Agreements do not entirely provide the same data protection as European countries do. Additional problems like the uncertainty of their

63 Räther/ Seitz, Übermittlung 430.

64 Cf <http://safeharbor.export.gov/companyinfo.aspx?id=12058> and <http://safeharbor.export.gov/companyinfo.aspx?id=13346>.

legal qualification, the vague terms in the Principles and FAQ's, as well as the loose enforcement of the Agreements, lead to a growing distrust not only in the Agreements themselves, but also in the U.S. authorities enforcing them.

Nevertheless: although the Safe Harbour Agreements may not bring the effects that were hoped for, blaming the Commission for not enforcing tougher regulation on the U.S. seems short sided. Eighteen months of negotiations do not speak for a simple solution. The Safe Harbour Agreements are also no victory for the U.S. They more likely seem to be the most achievable compromise between Europe and the U.S. The alternative, which was a very real scenario, was not to have an agreement at all, which could have caused severe difficulties in trade relations.[65]

It would be helpful if some clarity about the legal bindingness of the Safe Harbour Agreements (or transfer into third countries in general) would be enforced, so it is clear, in which countries data might be exported without further requirements. With this regard, the European Union recently has proposed a new data protection regulation by which it also intends to reform data transfer into third countries. Yet, it may be doubted whether the debates on the exchange of data will be over, especially with the increasing importance of the internet and data as its new currency.

65 FARRELL, Negotiating Privacy across Arenas 112.