Getting Privacy to a new Safe Harbour

Comment on the CJEU Judgment of 6 October 2015, Schrems v Data Protection Commissioner

by **Philipp E. Fischer***

Keywords: privacy; Safe Harbor; CJEU; Max Schrems; Data Protection Directive; surveillance; data transfer

Recommended citation: Philipp Fischer, Getting Privacy to a new Safe Harbour. Comment on the CJEU judgment of 6 October 2015, Schrems v Data Protection Commissioner, 6 (2015) JIPITEC 229 para 1.

A. Background

1 For a number of years, Facebook user and privacy law expert Maximilian Schrems[1] has insisted on a better data protection on Facebook. Since 2011, Schrems filed 22 complaints[2] against Facebook´s European headquarters in Dublin based on alleged infringement of the Irish Data Protection Act and the underlying European Union (EU) Data Protection Directive of 1995[3]. Following nearly three years, Schrems´ initiative "Europe vs. Facebook"[4] withdraw these complaints against Facebook; however, the "PRISM complaints"[5] were still pursued. The latter consisted of complaints against Apple[6], Facebook[7], Skype[8], Microsoft[9] and Yahoo[10]. In his lodged complaint with the Irish supervisory authority (the Data Protection Commissioner) regarding Facebook, Mr. Schrems upheld the view that, in light of the revelations made in 2013 by Edward Snowden concerning the activities of United States´ (US) intelligence services (in particular the National Security Agency - NSA), the law and practices of the US do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country. On 24 March 2015, the Court of Justice of the European Union (CJEU) heard[11] this procedure against Facebook, which had been referred[12] by the Irish High Court.

2 Facebook is bound to a legal basis called the "Safe Harbour" decision[13]. According to the EU Data Protection Directive of 1995, personal data may only be transferred to "third countries" (countries outside the EU and the EEA), if information is sufficiently protected in the country of destination. It is under the authority of the European Commission to decide whether other countries can guarantee this level of protection. In 2000, the EU Commission defined the level of protection set out by the Safe Harbour program - adopted by the US Department of Commerce - as adequate. US companies can therefore self-certify that they comply with European data protection rules. In order to do so they must prove their commitments regarding data

1 https://en.wikipedia.org/wiki/Max_Schrems.

2 http://www.europe-v-facebook.org/EN/Complaints/complaints.html.

3 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

4 http://www.europe-v-facebook.org/EN/en.html.

5 http://www.europe-v-facebook.org/EN/Complaints/PRISM/prism.html.

6 http://www.europe-v-facebook.org/prism/apple.pdf.

7 http://www.europe-v-facebook.org/prism/facebook.pdf.

8 http://www.europe-v-facebook.org/prism/skype.pdf.

9 http://www.europe-v-facebook.org/prism/microsoft.pdf.

10 http://www.europe-v-facebook.org/prism/yahoo.pdf.

11 Reference for a preliminary ruling from High Court of Ireland (Ireland) made on 25 July 2014 – Maximillian Schrems v Data Protection Commissioner, Case C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=161179.

12 http://www.europe-v-facebook.org/ref_ecj.pdf.

13 C(2000) 2441, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF.

protection before the US Federal Trade Commission (FTC). This includes the duty to inform users which personal information they transfer for what purpose, to disclose information on its transfer to third parties, to give users the right to access stored data, and to rectify data or to delete data. Among data privacy experts however, there were doubts[14] whether and to what extent US-based corporations would actually comply with this self-certification process, as companies are not obliged to provide evidence of these commitments and the EU itself does not oversee this process. The EU Commission also expressed its concerns: "Due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed: a) transparency of privacy policies of Safe Harbour members, b) effective application of Privacy Principles by companies in the US, and c) effectiveness of the enforcement."[15] As Facebook grants the US intelligence services access to their databases, the US is not a "safe harbour" for European citizens' personal data; thus on 23 September 2015, the EU Advocate General, Mr. Yves Bot, brought into question the continuation of Safe Harbour on which data transfers to the US are based on.[16]

B. Decision of the CJEU of 6 October 2015

3 In its judgement of 6 October 2015[17], the CJEU declared the Safe Harbour decision of 2000 void. Although the CJEU ruled that the validity of the decision of 2000 is not a subject of the referred question itself, it indicated in margin numbers 93 and 94, that mass surveillance practices are incompatible with European fundamental rights. The CJEU claimed - in a remarkable way - decision-making power on questions of fundamental rights of EU citizens, which the EU Commission had formerly dealt with: "It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid".[18] The CJEU held that "even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive." [19] Thus, the CJEU found that the nature of Art. 3 of the Safe Harbour decision is illegitimate in this respect as it reduces the competence of national data protection authorities to fully assess the adequate level of data protection of self-certified companies in the US.

4 In light of this decision, the Irish High Court decided on 21 October 2015 that the Irish Data Protection Commissioner should investigate "Facebook Ireland Ltd" over alleged cooperation of "Facebook Inc" with US spy agencies, such as under the NSA's "PRISM" program. The initiative "Europe vs. Facebook" legally requested Data Protection Authorities in Ireland[20], Belgium[21] and Germany[22] to enforce the CJEU´s judgement on Facebook by reviewing and suspending Facebook's data transfers over US spy programs.

C. Valuation

5 The CJEU nullified one of the potential legal bases of EU-US data flow. A broad discussion has begun among EU data privacy experts whether - after the decision of the CJEU - alternatives to Safe Harbour are still permissible. Companies that have so far transferred European users' personal data to the US on the basis of Safe Harbour must now turn to another legal basis, such as binding corporate rules (BCR)[23], standard contractual clauses (SCC)[24] or consent given by the person affected.

6 After Safe Harbour was invalidated, companies such as Facebook have started to use contractual agreements[25] as an alternative in order to lawfully transfer data; this alternative is permissible insofar as these companies are not complicit in illegal "mass surveillance". Gerard Rudden representing the complainant in Ireland stated that: "All relevant

14 Press release of the Conference of German Data Protection Commissioners from 24 July 2013, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9283.de.

15 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, http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf, p. 18.

16 http://curia.europa.eu/juris/celex.jsf?celex=62014CC0362&lang1=de&type=TXT&ancre=.

17 European Court of Justice, Case C362/14, JUDGMENT OF THE COURT (Grand Chamber) of 6 October 2015, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5248977b390cb4b77beacd6135154f1a0.e34KaxiLc3eQc40LaxqMbN4Oc38Oe0?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=156974.

18 Court of Justice of the European Union, PRESS RELEASE No 117/15, p. 2.

19 Court of Justice of the European Union, PRESS RELEASE No 117/15, p. 2.

20 http://www.europe-v-facebook.org/comp_fb_ie.pdf.

21 http://www.europe-v-facebook.org/comp_fb_be.pdf.

22 http://www.europe-v-facebook.org/comp_fb_de.pdf.

23 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf.

24 http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

25 http://www.europe-v-facebook.org/comp_fb_scc.pdf.

EU decisions include an exception for cases of mass surveillance. There is no 'quick fix' through alternative transfer methods for companies that are involved in the violation of European fundamental rights."[26]

7 The German data protection authorities are of the opinion that the standard contractual clauses are also "disputable"[27], because the reasons on which the CJEU based its decision on Safe Harbour apply also – at least partially - to standard contractual clauses. The CJEU found that the de facto poorly restricted access of intelligence agencies on electronic communication is inconsistent with European fundamental rights and that neither Safe Harbour, nor standard contractual clauses, would restrict this power of public authorities. Based on the argument of the Advocate General, Flemming Moos und Jens Schefzig[28] argue that even when concluding a contract based on the standard contractual clauses an adequate level of data protection cannot be guaranteed. The Council and the European Parliament had given the Commission the power to decide, on the basis of Art. 26 (4) of the EU Data Protection Directive of 1995[29], that certain standard contractual clauses offer sufficient safeguards as required by Art. 26 (2). The CJEU held however that only the CJEU can declare a decision by the EU Commission void. This would therefore also concern the Commission´s decisions on standard contractual clauses. Until such a ruling by the CJEU, the standard contractual clauses would remain valid. Practitioners are therefore of the opinion that, until a new "safer safe harbour" is created, the transatlantic data flows could go on unhindered based on this available legal mechanism.[30]

8 The distinction between the validity of the standard contractual clauses as such – which has to be affirmed according to the findings above – and the competence of national supervisory authorities to suspend trans-border data flows should be emphasised. SSCs and BCRs cannot override the arguments made by the CJEU on mass surveillance under the Charter of Fundamental Rights (CFR)[31]. The CJEU held that the existence of a Commission decision cannot eliminate or even reduce the powers available to the national supervisory authorities. Thus, the same issues that lead to the invalidation of the Safe Harbour decision, could be brought before any of the national supervisory authorities in the 28 member states, in the case that a data subject claims that these contractual solutions do not properly protect the fundamental rights of the data subject. The relevant Decisions 2001/497/EC[32], 2004/915/EC[33] and 2010/87/EU[34] all have a clause that cares for exactly this situation, and allow DPAs to suspend data flows if "it is established that the law to which the data importer is subject imposes upon him requirements to derogate from the relevant data protection rules which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses"[35]. Whilst a supervisory authority assesses an adequate level of data protection, it may de facto block trans-border data flows.

9 After a review of the ongoing discussions on the CJEU´s decision, the author of this comment notes a lack of precise distinction in especially these three matters:

I. The two-stage process of an assessment of lawfulness of trans-border data transfers from an EU/EEA country to a third country

10 The European Data Protection Directive and the corresponding implementation in the Federal Data Protection Act of Germany (BDSG) contain two requirements for a lawful data transfer to third countries: The first ("first stage") is the need for a legal basis for the transmission as such (Art. 7 Data Protection Directive, § 4 (1) BDSG, § 4 (2) BDSG, §§ 27 ff BDSG). The second ("second stage") assesses the question if the data recipient in a third country can prove an adequate level of data protection (Art. 25

26 http://www.europe-v-facebook.org/prism2_en.pdf.

27 https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

28 http://www.cr-online.de/blog/2015/10/05/eugh-count-down-fuer-safe-harbor-teil-33-auswirkungen-eines-potenziellen-urteils.

29 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

30 http://www.eu2015lu.eu/en/actualites/communiques/2015/10/06-cjue-schrems/index.html; https://www.datenschutzbeauftragter-info.de/safe-harbor-gekippt-wie-geht-es-weiter/; http://rechtsanwalt-schwenke.de/was-bedeutet-das-safe-harbor-urteil-des-eugh-fuer-sie/.

31 Charter of Fundamental Rights of the European Union, 2000/C 364/01, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

32 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en.

33 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN.

34 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

35 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001D0497&from=en, p. 4.

Data Protection Directive, § 4b BDSG). Unfortunately, it is still a common misconception that a data transfer to third countries can be lawful based only on ensuring (second stage) an adequate level of data protection.

11 Several online blogs[36] outline that the basis for a legitimate transfer could be consent given by the person affected. Such consent to be obtained by the person affected must be 1. freely given, 2. specific, 3. informed and 4. unambiguous (Art. 26 Data Protection Directive, § 4c Nr. 1 BDSG). The requirements for lawfully given consent should be clearly distinguished between the above mentioned two stages: for complying with stage two a user would have to be informed about the specific situation. The duty to inform according to § 4a (1) sentence 2 BDSG must be broadened and specified; there must be a notice which does not only designate the recipient country but also the lower level of protection so that the person can include this fact in its decision. Many US companies would then have to seek consent of persons affected in the EU for each transmission of data in advance, to inform these persons on the exact purpose and scope of the data processing and to indicate in its terms and conditions that US intelligence agencies have access to stored data. But this is problematic, as US law prohibits revelations of their cooperation with these agencies. Notifying the user that "data is transferred outside of the EU/EEA", as for example Facebook currently does in its terms and conditions[37], cannot be deemed appropriate. Mr. Schrems states: "To get a valid consent Facebook in our example would have to be very upfront and explain that all data that is used on facebook.com is subject to mass and indiscriminate surveillance by the US government."[38] According to the above-mentioned position paper of the German data protection authorities, the consent may "be given solely under strict conditions"; basically, the data transfer on the basis of consent "cannot be carried out repeatedly, en masse or routinely". According to Peter Schaar, former *Federal Commissioner* for *Data Protection* and Freedom of Information of Germany, a "blanket consent to extensive state surveillance by a third country, together with the absence of legal protection under EU law" would therefore be ineffective.[39]

II. The differences between the derogations set out in Art. 26 Data Protection Directive

12 In many cases, mass surveillance will not be of importance for trans-border data transfers. When data transfers previously relied on Safe Harbour, and a US controller or processor is not subject to US mass surveillance laws, a consent given by the person affected may be a reasonable option. Or for example, in the case that personal information is sent to the US for the purpose to "perform a contract" or for the "vital interests of the data subject". Most of the daily business transactions will therefore be able to use one of the derogations in Art 26 of the Data Protection Directive.

III. The legal basis for data transfers, the political debate about mass intelligence surveillance and the corresponding issue of infringement of the European Charter of Fundamental Rights

13 From a political view: for nearly two years, the EU and the US are negotiating a revision of the Safe Harbour Agreement. According to Reuters news agency, the discussions should be close to completion.[40] The CJEU´s decision will certainly have an impact on the ongoing negotiations. From a legal point of view: the CJEU´s decision makes it clear to national governments and EU institutions that European law is not allowed to crumble into dust only because of enhancing transatlantic trade. Through this judgment, the protection of fundamental rights in the EU has become a community project[41] and the CJEU´s decision is currently the third step on its long way to this. The first judgment dates back to April 2014 on data retention regulation. The second was that of May 2014 on the right to be forgotten and against Google. The third judgment is now attempting to end the discussion of the Internet as a legal vacuum. The court made it clear that future agreements relating to the traffic of data are a judicial subject.

36 e.g. http://www.heise.de/newsticker/meldung/Nach-dem-EuGH-Urteil-Alternativen-zu-Safe-Harbor-2837700.html and http://www.heise.de/newsticker/meldung/Safe-Harbor-Urteil-Gibt-es-ueberhaupt-noch-Alternativen-fuer-den-Datentransfer-in-die-USA-2840322.html.

37 https://www.facebook.com/policy.php.

38 http://www.europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html.

39 http://www.eaid-berlin.de/?p=789.

40 http://www.reuters.com/article/2015/08/05/us-usa-eu-data-idUSKCN0QA1XB20150805.

41 Süddeutsche Zeitung, 07.10.2015, Ressort: Meinungsseite.

D. Perspective

14 The question regarding which "future regulation" could solve the above-mentioned recurring problems of legal and political bandwidth when it comes to trans-border data flows should be raised. Peter Schaar states that "in the longer term, the only way is to enforce on a global level privacy rights guaranteed in Art. 12 of the UN Declaration of Human Rights[42], the EU Charter of Fundamental Rights and in other constitutions of democratic states"[43].

15 To reach that goal, one objective should be a consolidated definition of what a trans-border data flow is, to define its features by explaining various combinations (controller, processor, sub-processor, data subject), the reason for it, its legal basis and the function of the level of protection of the country of destination, and to consider the radically increased quantity of such flows.

16 Another objective should be to examine existing bilateral and multilateral treaties and the rules therein that tend to regulate the flow of data across national borders. The first data protection laws, mainly in Europe, did not contain provisions restricting trans-border data flows. It was only when data outsourcing became an option to avoid strict domestic privacy laws, that some countries, partly based on the Convention 108 of the Council of Europe[44], started to introduce rules on trans-border data flow. The history of regulation in different regions, through leading regional and international instruments of the EU, OECD, Council of Europe, APEC, and other bodies should be considered in this respect.

17 It is important to analyse whether there is a common type of approach within these rules. For example, European regulations are advanced and set out a high level of data protection. In the US, the emphasis is more on self-regulatory approaches, as seen currently in the Safe Harbour case, however, the increase in global data transfers also influences understandings in these areas and could be of importance in order to find a common denominator. It should then be possible to outline certain typologies of different regulatory approaches. The nature of these approaches also depend on different aspects of privacy, such as the history of privacy, theories of privacy and the varying understanding of privacy mainly between the US and Europe.

18 Constantly developing technological solutions will also be of importance as well as regulations developed by the private sector. It will additionally be relevant to examine to which extent trans-border data flows provide compelling challenges to cloud adoption and as a result offer a solution for any business seeking to transfer data that must exercise significant care and due-diligence to avoid infringing privacy regulations and protections by sending data to or through places that do not guarantee the same level of protection.

19 The next objective for stakeholders for the protection of people´s privacy should then be to find out whether the actual status quo is of a sufficiently harmonized nature. Particularly, the contents of three current major frameworks, the US, the EU and the APEC, have to be analysed and outlined to what extent these could form a basis for harmonised international rules.

20 Finally, it has to be answered whether an international harmonisation of trans-border data flows could be reached through an international compromise. Harmonisation has made some progress on a regional level, for example within the members of the European Union. It ought to be defined how the General Data Protection Regulation[45] could be of influence on international transfers by regulating the territorial scope of the Regulation, highlighting the question of the application of EU rules to controllers not established in the EU when processing personal data of EU citizens.

21 Christopher Kuner states that "there is a nature desire to find a single, high-level solution to the legal issues raised by transborder data flow regulation, and the inability to do so is frustrating"46. Data privacy experts and policy makers should thus concentrate their efforts more than ever to confront this task.

* Philipp E. Fischer, LL.M. (IP, London/Dresden) is a Ph.D. cand. (UOC, Barcelona) and works as a Data Protection Officer & Auditor (TÜV) in Munich.

42 http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

43 http://www.eaid-berlin.de/?p=789.

44 http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDATA-RAP03Abr_En.pdf.

45 http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

46 Kuner, C. (2013): Transborder Data Flows and Data Privacy Law, Oxford University Press, p. 186.