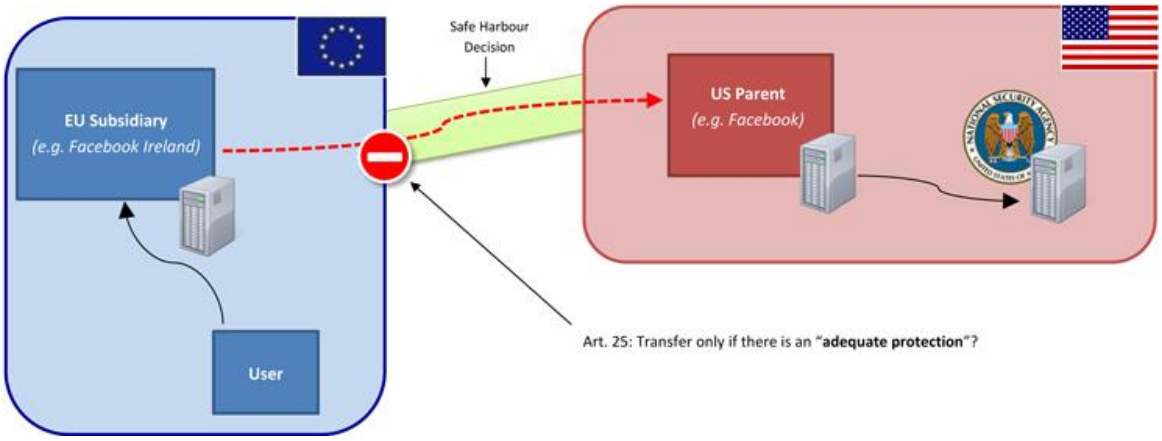
23. 3. 2015

European Court of Justice hears NSA/PRISM case
EU-US personal data flows under "Safe Harbor" on the table

On Tuesday March 24th the Court of Justice (CJEU) will hear a case referred by the Irish High Court on the NSA/PRISM spy scandal, which may have major implications for EU-US data flows and US internet companies operating in Europe (case number: C-362/14).
Large internet companies (in the current case Facebook) have, pursuant to US law, allowed the US government to access European user data on a mass scale for law enforcement, espionage and anti-terror purposes.[1] Aiding these forms of US "mass surveillance" may however violate EU privacy laws and fundamental rights.

Facebook & PRISM. Like Facebook, Apple, Google, Yahoo, Skype or Microsoft all relevant participants of the PRISM program (Wiki) have outsourced their non-US or European operations to Ireland or Luxemburg, consequently EU law applies to them. The current case deals with "Facebook Ireland Ltd" and its involvement in the PRISM spy scandal, but may be relevant for all other companies involved in the US spy scandal.



The European subsidiaries of US tech giants collect personal information within the EU and then forward ("export") EU data to the United States. Under EU law such a "data export" to a third country is only legal if the exporting company (in this case "Facebook Ireland Ltd") can ensure an *"adequate protection"* for such data in the US.[2] In the current case, the plaintiff claims that the NSA's PRISM program and other forms of US surveillance are the exact antithesis of "*adequate protection*".

CJEU track record. The CJEU is the supreme court of the European Union. The court's rulings are binding in all member states of the European Union. In the very recent "data retention" ruling[3] the CJEU has ruled that "mass storage" of meta data for six months to two years is violating Article 8 of the Charter of Fundamental Rights (CFR). In contrast the PRISM program, allows access on a mass scale even to content data and without any judicial redress for non-US

[1] e.g. 50 U.S. Code § 1881a or Executive Order 12333.
[2] Article 25 of Directive 95/46.
[3] See cases C-293/12 and C-594/12

persons. The CJEU also made headlines with the recent "Google Spain" decision,[4] where it ruled that EU citizens have a right to have obsolete search results removed (dubbed "*right to be forgotten*"). In the very similar "SWIFT" situation (Wiki) the financial services provider based in Belgium decided to stop data flows to the US and kept all EU data within Europe.

EU-US "Safe Harbor". The plaintiff argues that the United States does not provide the "*adequate protection*" required under Article 25 of the EU Data Protection Directive. EU-US data transfers are therefore mainly governed by the so-called "Safe Harbor" system, an executive decision by the European Commission that allows US companies to "self-certify" adherence to EU privacy laws. This system was introduced in 1999, but since then harshly criticized for not providing proper protection of European data, once it reaches the United States. The criticism included a number of reviews e.g. by the European Data Protection Authorities, the European Commission and even a resolution of the European Parliament. So far the EU and the US could not agree on a solution to the problems identified.

Submissions. In summary 12 parties (seven EU member states, the European Commission and the European Parliament[5], the two main parties in the Irish proceeding and an 'amicus curiae' notice party in those proceedings) have submitted written observations to the CJEU. It is expected that additional parties will participate in the oral hearing.
The rules of the CJEU prohibit publishing or citing from the submissions to prevent public pressure on the member states, but it can be said that there seems to be little disagreement that "mass surveillance" in the US is a fact – despite denials from the IT industry. This was also found as a matter of fact by the Irish referring court. While many submissions have not debated the implications under the Charta of Fundamental Rights, there seems to be no party that suggests that the extreme form of mass surveillance under e.g. the "PRISM" program is or could be legitimate in the view of EU fundamental rights. At the same time there is a wide variety of proposed solutions that range from:

1. waiting for a political compromise between the EU and the US,
2. the use of a special "emergency provision"[6] in the "Safe Harbor" to suspend data flows to individual companies like Facebook, Apple, Google, Yahoo or Microsoft and
3. asking the CJEU to find that the "Safe Harbor" system is invalid under EU law.

The plaintiff and a number of other parties argued that the "Safe Harbor" decision is invalid under EU law and should be annulled or at least found to be inapplicable by the CJEU. In summary the validity of the "Safe Harbor" Decision will surely be on the table.

Not the End of EU-US data transfers. Despite serious implications for US internet service providers, even a finding of invalidity of the "Safe Harbor" Decision, would not make EU-US data flows impossible. "Self-certified" US companies may lose the "privileged status" under Article 25 of the Directive, but would still be able to apply for data transfers under a number of other legal regimes in Article 26 of the same Directive, as it is the daily practice with most non-EU countries.[7] However a number of companies (e.g. Twitter in its recent Annual Report)[8] expect

[4] See case C-131/12
[5] See the Parliament's publication.
[6] Article 3 of the „Safe Harbor" decisions allows to suspend data flows in special cases.
[7] Non-privileged for example: Japan, China, India, Russia and most other major trading partners of the EU.
See the short list of "privileged" countries (e.g Canada, Israel or Switzerland) here: http://europa.eu/!DC68BG
[8] See http://files.shareholder.com/downloads/AMDA-2F526X/4048899054x0xS1564590-15-1159/1418091/filing.pdf, p 25.

that it may become harder for US companies to retrieve data from the European Union and it may be necessary to invest in secure European data centers.

Background. The case is the result of an Austrian Facebook user (Max Schrems) who filed a complaint against Facebook with the Irish Data Protection Commissioner (DPC). The Irish Data Protection Commissioner (DPC), in charge of enforcing EU data protection laws in Ireland, has refused to investigate a complaint, claiming that the legal arguments by the claimant were "*frivolous and vexatious*". The DPC claimed that it is "absolutely bound" by the "Safe Harbor" decision from 1999. This decision was taken despite the fact that same legal arguments were made not only by many other EU data protection authorities, but also the European Parliament and others. The plaintiff challenged the refusal of the DPC at Irish High Court, which referred the matter to the CJEU in June of last year.

Crowd Funded. The procedure is "crowd funded" by more than 2000 donors that have so far donated more than € 60.000 on www.crowd4privacy.org.
The plaintiff is being represented by an international team of lawyers including Prof. Herwig Hofmann (University of Luxemburg), Noel Travers (Senior Counsel at the Irish Bar), Paul O'Shea (Barrister) and Gerard Rudden of Ahern Rudden Solicitors, Dublin, and assisted by data protection law expert, Prof. Franziska Boehm (University of Münster).

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