(Un)Safe Harbour: Stop! Or the Court of Justice will shoot

In the following post, Diana Dimitrova of the KU Leuven Centre for IT & IP Law, discusses the implications of the Court of Justice of the European Union's (ECJ) ruling that the Safe Harbour scheme is invalid, and looks at the powers of national supervisory authorities in ensuring compliance with the rights to privacy and data protection.

About the case

In his case against the Irish Data Protection Commission (Irish DPC), Max Schrems challenged the Irish DPC's reluctance to investigate his complaint against the transfer of his personal data by Facebook Ireland to Facebook USA. The legal basis which allows the transfer to the USA is the so-called Safe Harbour scheme. Normally, if personal data are to be transferred outside the EU, and such a country is not deemed by the EU country's national authority to ensure an adequate level of protection of personal data, the transfer may take place only under certain conditions, e.g. if the Commission decides that a certain country offers an adequate level of protection because of international commitments and its domestic laws (Article 25 (6) Directive 95/46/EC). The Safe Harbour scheme is an example of such a Commission decision.

The case reached the Court of Justice of the EU (ECJ) through a preliminary ruling question from the Irish High Court. It asked whether EU national data protection authorities (DPAs), empowered by Directive 95/46/EC to investigate the legality of data processing activities such as data transfers to third (non-EU) countries, are "*absolutely bound*" by a Commission decision that a certain third country offers an adequate level of data protection, such as Decision 2000/520 on the Safe Harbour scheme. In other words, the question seeks to clarify whether DPAs must carry out their own investigations as to the legality of transfers, especially in view of the factual developments that affect the level of privacy and data protection compliance in a specific third country: in this case, the USA.

The Opinion of Advocate General Bot

Advocate General (AG) Yves Bot, a senior ECJ official who advises on cases, issued an Opinion in late September which examined not only the distribution of powers between the national DPA and the European Commission but also, of his own initiative, the legality and validity of the Safe Harbour scheme as negotiated by the European Commission with the USA in 2000. He focused on its compliance with primary and secondary EU law, namely Articles 7, 8, 47 and 52 (1) of the Charter of Fundamental Rights of the EU (CFREU) and Directive 95/46/EC on data protection in the EU.

As regards the powers of national DPAs, AG Bot concluded that the Commission decision may not prejudice their powers, especially their powers to investigate data subjects' complaints and assess the level of adequacy of data protection in third countries and even suspend data flows. A conclusion to the contrary would mean that citizens' rights to submit complaints and have them investigated independently would be reduced by the Commission's decisions and national DPAs' role as independent supervisors would be compromised, in breach of Article 28 Directive 95/46/EC, read in light of Articles 7 and 8 CFREU.

Thus, guaranteeing privacy and data protection, including adequacy decisions on level of data protection in third countries, is a shared competence between the Commission and national DPSAs, where Commission adequacy decisions should constitute only "a rebuttable presumption" of compliance.

As to his assessment of the Safe Harbour scheme, the most significant conclusions from AG Bot's reasoning are that:

1. Sadly, the 'mass and indiscriminate surveillance' carried out by the US Intelligence services, as found by the Irish High Court in its factual assessment, does not breach the terms of the Safe Harbour scheme. The scheme is framed in such a way that the 4th paragraph on Annex I to Decision 2000/520 allows broad exemptions from the Safe Harbour data protection principles, the purposes of which are not narrowly defined, as required by Article 52 (1) CFREU.
2. Such surveillance is *inherently disproportionate* due to its scope. The derogations go far beyond what it strictly necessary to achieve the purposes, which are not clearly defined. The parallel which AG Bot draws between the exemptions which EU national authorities enjoy exemplifies how Safe Harbour allows the US authorities to suspend the data protection principles much more easily.
3. Safe Harbour does not guarantee effective access to justice by EU citizens, whose data are being re-used by US intelligence services. Thus, they do not have an efficient way of exercising their data protection rights in the USA as they are also not protected by US laws. In addition, processing of their personal data by the USA intelligence services is not effectively controlled as required by Article 8 (3) CFREU and Article 28 Directive 95/46/EC.

Therefore, the Safe Harbour *per se* infringes the provisions of Directive 95/46 and of the CFREU. *It does not respect the essence of the rights to privacy and data protection.* Thus, the framework is legally unsound. It is furthermore unsound due to recent factual developments as found by the Irish High Court, i.e. the revelations of the mass surveillance carried out by US authorities, which the European Commission has not denied and thus simply cannot 'unknow' and ignore. Finally, AG Bot argues for invalidating the scheme as it is incompatible with fundamental rights.

ECJ judgement

Within only two weeks of AG Bot's opinion, the ECJ swiftly delivered its final judgement, in which it confirmed Bot's conclusion concerning the powers of national DPSAs and the immediate invalidity of Safe Harbour. A transitory period until a new solution is found for data transfers has not been granted.

The ECJ relates USA surveillance practices to the Data Retention Directive ruling, where it declared non-targeted surveillance of traffic data by EU law enforcement authorities as disproportionate and not "strictly necessary."

The ECJ noted that the Commission breached EU law when concluding its adequacy decision. The Commission did not even examine US domestic law or its international commitments and was therefore not able to assure that it "in fact 'ensures' an adequate level of protection." The Court finds that the Commission's Decision is legally unsound. Thus, it infringes Article 25 (6) Directive 95/46 since the Commission did not examine all the legal and factual background. The Commission Decision also reduces the powers of the national DPSAs as they may suspend data flows only under very limited circumstances, in breach of Article 28 Directive 95/46/EC read in lights of Article 8(3) CFREU.

Consequences

The Court upholds the positive obligation of EU and Member State authorities to *effectively guarantee* privacy and data protection of EU citizens and *the essence of these rights as such*. EU law must be interpreted and applied through the 'PRISM' of fundamental rights.

This should be taken into account by the EU and Member State authorities, especially in cases like passenger name record agreements, the Umbrella Agreement between US and EU on transfer of judicial data, and national surveillance laws, such as the one drafted in France.

More importantly, it reminds the European Commission that it may not (fail to) act in a way that results in infringements of fundamental rights and restricts the powers of national supervisory

authorities. It is under a positive obligation to check periodically whether its adequacy finding is still legally and factually justified, especially when doubts as to its adequacy arise.

In addition, the Irish DPA is now compelled to investigate Schrem's "frivolous and vexatious" complaint against Facebook. The DPA will have to examine the factual and legal situation in the USA with regards to rights to privacy and data protection, following the ECJ's reasoning as guidance.

Some may claim and fear that striking down Safe Harbour will distort the internet and international trade. However, as pointed out during the hearing of the case in March 2015, if Safe Harbour is suspended, this will put the affected companies in the same position as all non-self-certified US and other international companies. There are other legal means to enable transfer to third countries, while ensuring an adequate level of privacy and data protection of EU citizens. For the time being, companies can rely on mechanisms such as Member State authorisation of the transfer upon the conclusion of standard contractual clauses that offer adequate safeguards [Art. 26 (2) and (4) Directive 95/46/EC].

In light of the judgement in the present case, one should carefully consider the wording of Art. 26 (4), pursuant to which if the Commission decides that certain contractual clauses "offer sufficient safeguards […], Member States shall […] comply with the Commission's decisions." It appears that if national DPAs do not find the safeguards sufficient, they should be able to challenge such a decision, such as via the preliminary ruling procedure following a compliant, and *require* higher standards of personal data protection.

This post gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

October 6th, 2015 | Data Protection, EU Media Policy, Featured, Privacy | 1 Comment

---