Title: **Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities**

15 October 2015, www.europeanlawblog.eu

Author: Fanny Coudert, CiTiP – KU Leuven

Bio: *Fanny Coudert is a researcher specialised in Privacy Law at the Centre for IT and IP Law (CiTiP) of the KU Leuven and a member of Madrid Bar. She holds a double Law Degree from the Université Panthéon-Sorbonne and the University Complutense of Madrid (Spain) (maîtrise intégrée en droits français et espagnol) and a LLM in ICT Law from the later University. She has working experience as privacy auditor, lawyer and in-house counsel.*

Her research mainly focuses on the protection of privacy in the context of surveillance, privacy-by-design and the principle of accountability.

On 6th of October, in *Schrems vs. Data Protection Commissioner*, the CJEU, following the controversial Opinion of AG Bot, put an end to the specific regime regulating data flows to the US. The 4600 US companies using this agreement are now forced to rethink how to ensure the continuity of the protection when data are transferred from EU to the US. In this milestone ruling, the Court also reaffirmed the key role played by national Data Protection Authorities (DPAs) in the European system of data protection, and clarified the different competences of the Commission, the DPAs and the courts –including the ECJ- in assessing the adequate level of protection offered by a third country.

To make a long story short

The difficult question of cross-border data flows. In the *Schrems* case the CJEU had for the first time to deal with the regulation of personal data flows to a third country, the US. Article 25 of the 95/46/EC Directive (the Data Protection Directive) installed a strict regime for cross-border data flows, allowing for data to be transferred only if the recipient ensured an adequate level of protection, i.e. similar to the one provided by the EU data protection framework. This regime was meant to prevent data holders from taking advantage of disparate levels of protection and from transferring personal data to "data havens", which would result in a dilution of the safeguards offered by EU data protection law and in a distortion of competition. Both national Data Protection Authorities (DPAs) and the Commission were given the power to assess the level of protection surrounding a given set of cross-border transfers: the former when examining specific requests from data holders, the later through "Adequacy Decisions", binding on Member States.

The Safe Harbour, unique in kind. As the US privacy framework did not meet EU standards, the Commission came to an original solution. The US Adequacy Decision (Decision 2000/520/EC, "the Safe harbour") defines a series of "Principles" to which US companies self-certify and which are enforced by US regulators within the limits of their scope of competences. The Federal Trade Commission has, for instance, been active whenever data processing activities constituted unfair commercial practices. Controversial and criticised in Europe, the Safe Harbour was however never challenged and the Commission issued implementation reports in 2002 and 2004 that recognised its weaknesses. The Commission however preferred to work closely with US institutions to improve the enforcement of the Principles in the US rather than reviewing the content of the Decision.

When the NSA enters into play…. Mr Snowdens' revelations about the PRISM programme changed the status quo. It was suddenly made patent that the NSA had obtained unrestricted access to mass data stored on servers located in the US. All companies involved in the PRISM program appeared to be Safe Harbour certified, making the Safe Harbour scheme, in words of the Commission, "one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU". German Data Protection Authorities, Jan Albrecht, the rapporteur at the European Parliament for the General Data Protection Regulation, and Jacob Kohnstmann, Chairman of the Article 29 Working Party publicly stated that there was a "substantial likelihood" that the Safe Harbour was being violated (Commission Communication).

…**and the Commission fails to find a political solution..**. In August 2013, Viviane Reding, Vice-President of the Commission, called for a review of the Safe Harbour by the year-end, calling the Safe Harbour "a loophole" that "may not be so safe after all" (Commission Communication). The EC issued out a series of recommendations to improve the content of the Safe Harbour in December 2013. This included a close monitoring of the use of the exceptions contained in the Decision, the provision of information to individuals about potential further transfers to US intelligence services, and the recognition of individuals' rights to access, rectify and delete their data, as well as the right to redress in the context of US surveillance programmes. Discussions were reopened but soon stalled (euractiv). The attempt to elaborate a political solution reached a dead end.

…EU citizens decide to take action. In the meantime, Max Schrems, an EU privacy activist, decided to file a complaint to the Irish DPA in order to stop the transfer of his data by Facebook Ireland to Facebook Inc. located in the US.. Indeed, all adequacy decisions recognise the power of DPAs to suspend data flows in specific circumstances, in particular when the level of protection recognised by the adequacy decision has been compromised, the enforcement mechanisms are likely to fail and the continuing transfer is likely to cause a grave harm to the individual whose complaint is being investigated (see e.g. Article 3 of the Safe Harbour Decision). The Irish DPA refused to investigate his claim, arguing that national DPAs had no competence to challenge the validity of an Adequacy decision. Schrems then referred the case to the Irish High Court which decided to request a preliminary ruling on the question of whether national DPAs are absolutely bound by Commission's Decisions. In doing so, the High Court also noted that if the matter had to be solved under Irish Law, it would have mandated the DPAs to investigate the claim, as "the interception of electronic communications performed by the NSA and other similar agencies as exposed by Edward Snowden would raise significant issues" as to whether "the US ensures an adequate level of protection for the privacy and fundamental rights and freedoms of data subjects" (AG Bot Opinion). The Irish High Court was also of the opinion that it would be difficult for US practices to satisfy the requirements of Articles 7 and 8 of the EU Charter of fundamental rights, as interpreted by the CJEU in *Digital Rights Ireland*.

The Judgment

New powers for DPAs. The CJEU first examines the distribution of competence between the Commission and the DPAs when it comes to assessing the level of adequacy of the protection afforded by a third country. The Commission argued that the powers of the national DPAs were focused on the application of the relevant legislation in individual cases. Otherwise, national investigations, such as the one required by Schrems, would encroach on the Commission's power to

renegotiate the terms of that decision. The Court, however, follows the opinion of the AG and analyses the distribution of competence from the scope of the crucial role played by DPAs within the data protection framework. The Court had previously ascertained that the supervisory authorities are the guardians of fundamental rights and freedoms put at stake by data processing operations (Commission v. Hungary, C-288/12). Their independence is an essential element of the protection and cannot be restricted in any way.

The Court thus proceeds to clarify the system of check and balances. While Adequacy Decisions bind Member States until the moment they are declared invalid – an exclusive competence of the CJEU- national DPAs retain their full investigative powers and even have the duty to investigate claims lodged by individuals casting doubts about the adequacy of the protection afforded by the third country in question. In case the DPA finds the claim unfounded, the individual is entitled to refer the decision to national courts. On the contrary, if the DPA decides to give way to the complaint, it has the duty to refer the matter to national courts and ask for a preliminary ruling to the CJEU to assess the validity of the decision.

(In)Validity of the Safe Harbour Decision. Following the procedure it just established, the CJEU then examines the validity of the Safe Harbour Decision. Contrary to the AG Opinion, the CJEU does not focus its analysis on the assessment of the legitimacy of US surveillance programme – the factual basis of this analysis was highly contested by the US Mission to the EU and US scholars. Instead, it analyses the decision in light of the requirements imposed by Article 25 (6). The Commission should base Adequacy Decisions on the level protection afforded by domestic legislation or the international commitments of the third country in question. The Court found that the (unique) solution imagined by the Commission to compensate for the lack of safeguards established by US law does not conform to such requirements as the "Principles" only bind US companies that have self-certify and not US public authorities (Article 1 of the Safe Harbour Decision).

Furthermore, the Court scrutinizes the exceptions contained in the Decision that allowed derogation to all Principles, without any limitation, based on legitimate interests such as national security. In doing so, the CJEU takes the opportunity to recall the principles established by the *Digital Rights Ireland* judgement with regard to the legitimacy of surveillance measures. Laws should implement sufficient safeguards to limit the storage of personal data of targeted individuals, the access to the data by public authorities based on objective criterion and imposed restrictions on the further use of the data. Content of electronic communications can only be accessed in limited cases. Individuals should be granted the possibility to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data.

On the basis of these considerations, the Court notes that, in the Safe Harbour Decision, the Commission does not state that the US, in fact, ensures an adequate level of protection by reason of its domestic or its international commitments. It annuls Article 1 of the Decision.

Finally, the Court annuls Article 3(1) of the Decision that restricts the powers of investigation of national DPAs with regard to the implementation of Article 25 of the Directive, as the Commission exceeded its competences.

With two of its main articles declared invalid, the whole decision is found null and void.

And now, what?

The Commission is now faced with the hard task of finding a new political agreement with the US which will satisfy the criteria set by the CJEU. In the meantime, companies that were transferring data to the US under the Safe Harbour (including all Internet Giants) have to find creative solutions to meet the CJEU criteria as the use of the alternative instruments foreseen by the Data Protection Directive (contracts, binding corporate rules) is exposed to similar criticism from national courts, or at least to greater scrutiny from DPAs with regard to the mechanisms of protection installed to prevent (disproportionate) access to the data by US law enforcement authorities.

The Irish DPA will most likely be asked to investigate the complaint and to decide about the level of protection that surrounds data transfers operated by Facebook, a difficult task that many DPAs will be faced with in the (near) future. De facto, this judgement paves the way for new methods of collaboration between DPAs as anticipated in the draft General Data Protection Regulation through the one-stop-shop and the consistency mechanisms. DPAs have already announced that they will meet to fully assess the consequences of the judgement. Hopefully, this opens a new chapter in the (recent) history of the data protection framework, one in which national DPAs have strengthened powers to uphold individuals' rights.