The Privacy Shield is a Soft Update of the Safe Harbor

*Max Schrems**

'*La décision 2000/520 est invalide*' - a very short and simple sentence, spoken by the President of the CJEU on his last working day, but a shockwave for the data protection and privacy world, especially in the United States. Many have doubted that the Court would dare to decide what was in my view inevitable, given the law before it.

The Court has not only further strengthened the right to data protection and reminded the European institutions that the right to data protection is now a fundamental right, not to be put on the negotiating table with trade partners, but it has also taken a very clear standpoint on what is generally called 'mass surveillance'. For the very first time the CJEU has found that the essence of fundamental rights was breached – even in two cases.

Much could be said about what many call a landmark ruling, which (awkwardly) carries my name, but I would like to use this opportunity to highlight the following aspects:

First, I would like to voice my frustration with the weakness of the political level in the European Commission that lead to the absolutely laughable proposal for a new EU-US data sharing agreement called 'Privacy Shield'. If reviewed in detail, the proposal is a soft update of Safe Harbor, which does not address any of the material issues identified by the court.

In the private sector the 'Privacy Shield' does not even regulate the vast majority of processing operations by US controllers, as the proposed 'Notice & Choice' principles only limit the 'change of purpose' and any forwarding of data to a third party. All typical processing operations (eg collection, storage, profiling, linking of data) are not even covered by the 'Notice & Choice' principle. This is especially disturbing, as the CJEU has called for 'essentially equivalent' protection and the European Commission and the US government had every freedom to establish EU style rules in a new system, as there are no conflicting US laws that would hinder a US company to self-certify to a truly equivalent standard.

---

* Max Schrems is a privacy activist whose case against Facebook eventually led the Court of Justice of the EU (CJEU) to strike down the EU-US Safe Harbor agreement. For an extensive analysis of the *Schrems* case, see the case note by Neal Cohen, 'The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework' (2015) 3 EdpL 240.

In the much more complicated area of government surveillance, the proposed deal explicitly includes a statement that the United States continues to engage in 'bulk surveillance' for six cases. If this is compared to the underlying regulation in the Presidential Policy Directive 28[1], one can see that the US does not apply this limitation to six purposes to data that is *collected* in bulk, but not *used* in bulk.

The proposed Ombudsperson for US surveillance is a political undersecretary in the US Foreign Ministry, who will not even confirm or deny that a person was under surveillance, but only inform the person that all US laws have been complied with, or that non-compliance was remedied.

If compared with the findings of the CJEU, this proposed system is unfortunately not just questionable, but an outright affront to the highest court of the European Union. We need a fair deal that ensures data flows between the United States and the European Union. Regretfully, the European Commission has issued a proposal that will very likely lead to a similar decision by the CJEU in the near future, instead of ensuring legal certainty and fair completion for EU and US businesses and proper protection for data subjects. We will need to continue the Transatlantic dialogue, as this matter will not be off the table for long.

Secondly, I would like to highlight the greater meaning of the CJEU's judgement. While the public and academic debate has initially very much focused on the relationship between the United States and the European Union and the commercial and political aspects, this judgement will be highly relevant case law for the debate on mass surveillance within the European Union.

Unfortunately much of the EU Member States' surveillance is done in the area of 'national security', where EU law does not limit the actions of national governments. This leads to the rather absurd situation that the CJEU was able to weigh in on US surveillance, but it is much more questionable if it would have jurisdiction in cases involving EU Member States. However, already in the first months after the judgement was delivered other top courts have referred to this decision as relevant case law: The European Court of Human Rights has referred to the CJEU decision in *Vissy v Hungary* and the German Constitutional Court has recently referred to it in a decision on surveillance capabilities of the German Federal Criminal Police Office (*Bundeskriminalamt*). I am therefor confident, that this decision will not only be relevant for data transfers to third countries, but also function as a red line within the political union we live in – as it was always intended.

Thirdly, I would like to highlight, that we are now entering an era in which data protection not an exotic and out of touch topic, but becomes a fully enforceable and serious subject matter that needs proper enforcement. My case is often taken as an ex-

1 Editor's note: The Presidential Policy Directive 28 (PPD-28) was issued by President Obama in 2014 and provides US signals intelligence agencies with a set of guidelines on the collection, retention and dissemination of personal information about non-US persons.

ample how a 'student' can take on big multinationals, when in fact this was only possible as an expert in the field of law and under considerable monetary efforts, huge media support and extreme time commitments, but this will not be – and should not be – the norm. Some Data Protection Authorities have started to leave the 'cuddle zone' and transform into serious enforcement agencies. The upcoming EU General Data Protection Regulation (GDPR) will give them the necessary tools to ensure that the law delivers proper data protection practices on the ground. At the same time, it will be essential to empower data subjects to enforce their rights, this is eg foreseen in the GDPR, which will allow non-governmental organisations (NGOs) to bring cases on behalf of data subjects. In this respect, I am currently reviewing options for a European enforcement NGO that will hopefully lead to many more CJEU decisions on the upcoming GDPR.

Finally, I want to use this opportunity to thank the manifold support by the academic community and especially Professor Franziska Boehm, Professor Herwig Hofmann and the legal team that supported this case, namely Gerard Rudden, Noel Travers and Paul O'Shea.