Privacy Shield – Press Breakfast by MEP Jan Albrecht

European Parliament, Brussels, July 12th 2016
Statement by Max Schrems, Summary

Introduction

On October 6th 2015 the European Court of Justice (CJEU) has invalidated the so-called "Safe Harbor" decision (2000/520/EU) by the European Commission, which allowed EU-US data transfers. Under EU data protection law[1] and CJEU case law[2] data transfers outside of the EU are only permissible if a business can guarantee *"essentially equivalent"* protection and protection of the fundamental rights of the European Union (the rights to privacy and data protection and legal redress).

The European Commission has now issues a new decision named "Privacy Shield" that is meant to replace "Safe Harbor". Privacy Shield is a blanket adequacy decision under Article 25 of Directive 95/46/EC, when so far only a number of derogations under Article 26 were available to business that wished to transfer data to the United States.

Shortcomings in the Private Sector

In the private sector, the proposed rules are nowhere near the level of protection and principles of the European Union, despite the finding of the CJEU it has to be "*essentially equivalent*".

Backbone of EU law: purpose definition

When a patient shares personal information with a doctor, the patient reasonably expect that the doctor will only use this information for the treatment – not sell the personal data to a data dealer.

This expectation is enshrined as "purpose limitation" in EU law. Contrary to EU law, Privacy Shield allows very *broad and generic* purposes such as "*we use your data for all services we may provide to you and others*", which undermines this very crucial protection. Many other rules, for the deletion of data or the sharing of data are interlinked with this principle.

"Notice & Choice"

Privacy Shield is meant to be based on "Notice and Choice", which sounds promising. Contrary to this verbiage, and contrary to EU law, Privacy Shield does not give users much "choice". It actually gives companies a general blanked allowance to use the personal data of any person under the sun.

Only in two specific cases (data sharing with a third party and a change of purpose), users can object. Obviously, users would first have to know about the US business taking such steps, actively contact the company and conduct an "opt-out". In reality this will hardly happen, which is why EU law is based on an "opt-in" system, where companies typically have to ask customers for consent.

Many other such differences, which make Privacy Shield not "*essentially equivalent*" to EU law could be mentioned.

[1] See Articles 25 and 26 of Directive 95/46/EC
[2] See C-362/14 *Schrems.*

Private Sector Redress

In its judgment the CJEU has called for "*effective detection and supervision mechanisms*".

Privacy Shield does not provide such mechanisms, but rather sends users through a patchwork of options. Users have to contact the relevant US Company, then different private US arbitration bodies and their national authorities, who in turn contact the Federal Trade Commission and the Department of Commerce, to finally be able to address concerns with a "privacy shield board".

However, Privacy Shield does not ensure that any of these institutions is empowered to factually review the practices of any company. They lack the power to e.g. inspect the servers and software. The user will therefore typically be unable to proof allegations.

Also, none of the options available are directly enforceable for a customer. Findings of the institutions, which have a duty to investigate complaints, are only sanctioned by a removal from the program, if a company does not comply – but not directly enforceable by the individual. Even the decision by the so-called "privacy shield panel" must be brought before a US court for enforcement.

Further, the procedures will be held on US soil, before US lawyers, under US law and in English. Customers will have an inherent disadvantage, as typically seen with private arbitration. For this reason "arbitration" in consumer cases is prohibited within the EU since 1993.

It is hard to see how this system could fulfill the "*effective detection and supervision*" benchmark.

Shortcomings in on Mass Surveillance

In its judgement the CJEU has held that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*".

In Annex VI of the Privacy Shield decision, the US government explicitly confirms, that US services conduct "*bulk collection*" by using data from US companies. While the US highlights, what it called limitations (for example for only six broad purposes), the mere possibility of such mass surveillance is contrary to the CJEU judgement cited above.

Redress on Mass Surveillance (Ombudsperson)

As the new redress mechanism, customers may address an ombudsperson in the US. The ombudsperson is an undersecretary of the US state department, not a court or independent body.
While the new ombudsperson can raise issues within the US government, the reply to the individual is defined in Annex IV of the Privacy Shield decision. It will always contain the same two sentences:

- *First*, the US will not confirm or deny any surveillance.
- *Secondly*, say that all US laws were adhered to, or any non-compliance was remedied.

The proposed ombudsperson therefore provides for anything but a "*right to an effective remedy and to a fair trial*" as the CJEU has required in line with Article 47 of the Charter of Fundamental Rights.

Future of the "Privacy Shield"

While it seems that so far, there are no immediate challenges planed, it can be suspected that there will be no lack of possible plaintiffs. In addition to activists and NGOs, the Data Protection Authorities in the 28 member states can refer the question to national courts and the CJEU. Even the European Commission mentioned the possibility of a legal challenge on the validity of the Privacy Shield.

Options for Businesses

While businesses will soon be able to sign up to the Privacy Shield system, it seems that many would only do so in addition to other – more stable – transfers mechanism like so-called "Model Contracts".

It remains to be seen if a considerable number of US businesses will go through the expensive and somewhat complicated implementation procedure, if there is a high likeliness of legal challenges to the Privacy Shield system. Most expert lawyers recommend sticking with alternative mechanisms, or only using Privacy Shield as an additional option.

Unanswered Questions

Many obvious questions concerning Privacy Shield remain unanswered, for example:

- How can a system that effectively only requires opt-out for the transfer of data to a third party ("Notice & Choice") be "essentially equivalent" to EU data protection law, that requires consent (or another legal basis) even for the mere collection of data?
- Why shall US providers be granted access the European market, without following similar rules?
- How are private arbitration bodies an "*effective detection and supervision mechanisms"* when they cannot even investigate the facts by e.g. on-site reviews?
- How can the Commission claim that there is no "*have access on a generalised basis*" when the US explicitly names six cases where it allows "*bulk collection*"?
- How can an Ombudsperson, that will not even disclose if a person was subject to surveillance, provide for a "*right to an effective remedy and to a fair trial*"?

Statement

Schrems: "*Privacy Shield is the product of pressure by the US and the IT industry – not of rational or reasonable considerations. It is little more than an little upgrade to Safe Harbor, but not a new deal. It is very likely to fail again, as soon as it reaches the CJEU. This deal is bad for users, which will not enjoy proper privacy protections and bad for businesses, which have to deal with a legally unstable solution. The European Commission and the US government managed to make everyone miserable, when they could have used this opportunity to upgrade the protections that are crucial for consumer trust in online and cloud services."*