EDPS Pleading before the Court of Justice
Case C-362/14, *Schrems v Data Protection Commissioner*
Luxembourg, 24 March 2015

Mr. President, honourable members of the Court, Mr. Advocate General. Thank you for inviting us today.

To address your questions, we would like to make two points today: what we think are the fundamental issues in this case, and what is the correct role of the data protection authority in this situation.

The first fundamental issue in this case is the Safe Harbor itself, quite apart from the issue of mass surveillance. There have long been doubts amongst data protection authorities about the level of adequacy of the Safe Harbor, even while it was being negotiated.

None the less, after it was adopted, the Article 29 Working Party has tried to make the Safe Harbor work better. Data protection authorities have consistently criticised certain specific weaknesses, which were taken up in the 13 recommendations by the Commission in 2013. Today, some 18 months later, these criticisms have not yet been resolved by the US authorities, particularly those relating to national security.

In this respect, the second issue is the reach and scale of mass surveillance. This affects all transfers of personal data to the US, not just under the Safe Harbor. This phenomenon was inconceivable back in 2000. Then came 9/11, which changed everything. And now we have the revelations of 2013.

In the EDPS Opinion of 20 February 2014 we confirmed that the Safe Harbor principles have simply "not been designed for large-scale access of US intelligence authorities to data transferred under them" (para 52).

We agree with the latest statement by the Article 29 Working Party that "massive, indiscriminate and disproportionate access by US authorities to data originating from the EU cannot be considered to be in line with the Safe Harbor Principles and its possible limitations".
(WP29 letter to the Commission of 5 February 2015).

The limitation "to the extent necessary to meet national security" in the Safe Harbor is an exception to the principle of adequacy. It must be interpreted restrictively, and the broad interpretation given to it in the United States is unacceptable under the Treaty.

Finally, there has been another huge change since the Safe Harbor was adopted in 2000 - the adoption of the Lisbon Treaty, and the transformation of the Charter into primary law.

Putting all this together we would like to make a point about Articles 7 and 8 of the Charter.

This is that the infringement of these two Articles is so serious that it may even constitute a failure to respect the essence of each of these two distinct fundamental rights.

This can be appreciated by using your analysis of Article 52(1) in Cases C-293/12 and C-594/12, Digital Rights Ireland. In this case the Court clarified when the

essence of the rights under Article 7 and Article 8 is respected, and – for today's purposes - when it is not.

I turn first to the essence of the right of privacy and communications under Article 7 of the Charter.

In Digital Rights Ireland, at paragraph 39 this Court noted that the essence of the right under Article 7 is respected where there is no "acquisition of knowledge of the content of the electronic communications". The Data Retention Directive only covered traffic and location data.

In contrast, in this case there are serious concerns that intelligence agencies do access the content of communications. Such an interference is so serious that it could constitute a failure to respect the essence of the right of privacy.

Second, I would like to consider the essence of the right to protection of personal data under Article 8 of the Charter.

In Digital Rights Ireland, at paragraphs 39-40, this Court stated that the essence of the right under Article 8 of the Charter was not adversely affected because (i) the Data Retention Directive provided for certain safeguards and (ii) it was accompanied by the safeguards in the general framework of Directive 95/46 and Directive 2002/58.

In the same way, paragraph 68 of that ruling criticises the failure to require personal data to be retained within the European Union under the control of an independent data protection authority.

Our understanding is that this clause recognises that there should be no transfer of personal data outside the control of an independent data protection authority if there are no adequate safeguards as provided by EU law. In this respect, the way in which the exception on national security is now conceived and implemented in the US does not allow data protection authorities to evaluate the extent to which adequacy is compromised.

At present, therefore, there are serious concerns that the safeguards laid down in Article 8 paragraphs 2 and 3 of the Charter are wholly absent. These safeguards are "essential components" of the fundamental right to protection of personal data. Their absence could constitute a failure to respect the essence of Article 8 of the Charter.

I would now like to turn to our second point, the role of the data protection authority in this situation.

Parliament has described well our mandate under Article 41 of the Regulation, to monitor the EU institutions processing data and ensuring the application of the data protection rules and to advise them on all matters concerning the processing of personal data. These tasks are specified in our duties under Article 46 and our powers under Article 47.

One element which has not been described is our role concerning international transfers of personal data. Article 9 of Regulation 45/2001 is a mirror image of Article 25 of the Directive. We are therefore in the same situation as all data protection authorities concerning the supervision of transfers.

We would like to consider the implications for this case of the independence of data protection authorities.

This Court has stressed the "complete independence" of data protection authorities in a series of cases. Your case law insists that the right to independent supervision in Article 8(3) of the Charter is an "essential component" of the fundamental right to data protection.

This protection of independence has two effects.

First - and this relates to Question 1, second indent: independence under Article 8(3) of the Charter cannot be curtailed by narrow conditions in a Commission comitology Decision.

On the one hand, data protection authorities can apply Article 3 (1) (b) of the Decision in the event of disproportionate use of the national security exception.

On the other hand, if we construe the Safe Harbor as imposing strict conditions on data protection authorities which must be fulfilled cumulatively, as in Art 3 (1)(b), this would restrict their ability to exercise their powers with "complete independence" in this context.

Second – and this relates to Question 3, third indent: independence means that data protection authorities cannot be constrained to take a particular decision in given circumstances. They must have the power to undertake their own assessment of what is necessary to strike a fair balance in specific cases.

Discretion is an essential part of independence, and it must be a broad discretion, subject of course to judicial review of manifest error.

In this case, the country of destination is the subject of a Commission adequacy decision and the recipient of data from all Member States. A balance has to be struck between privacy and protection of personal data and disruption to the internal market.

Data protection authorities are entitled to form the view that a common, EU-wide approach negotiated by the Commission with the United States is the most effective means of carrying out their duty to protect fundamental rights.

Data protection authorities have therefore supported the Commission in its efforts to obtain an adequate revision of the Safe Harbor from the United States. In particular the Article 29 Working Party has highlighted its serious concerns about access for national security: in letters to the Commission of 10 April 2014 and 5 February 2015 and in the Working Document on surveillance of 4 December 2014, WP 228, (p. 41-42).

In a nutshell, the position of data protection authorities is as follows:

> The improvements by the US in upcoming months need to be sufficient
>
> If the revision process currently undertaken by the European Commission does not lead to a positive outcome, then the Safe Harbor agreement should be suspended
>
> In any case data protection authorities may suspend data flows according to their national competence and EU law
>
> The only effective solution is the negotiation of an international agreement providing adequate protection against indiscriminate surveillance,

including obligations on oversight, transparency, redress and data protection rights.

So where are we today?

The EDPS continues to attach great importance to a fruitful transatlantic dialogue.

However, the Safe Harbor itself continues to raise serious concerns. It has never been satisfactory, and the need to bring it into line with the concept of adequacy in the Directive has not yet been resolved.

Second, the reach and scale of surveillance may be so broad and so complete that the Safe Harbor fails to respect, here in the EU, the essence of the fundamental rights of privacy and data protection under Articles 7 and 8 of the Charter.

Thank you.

Christopher Docksey

Agent of the EDPS