CEPS Paper in
LIBERTY and SECURITY in Europe

Safe Harbour or into the storm?

EU-US data transfers after the Schrems judgment

Sergio Carrera and Elspeth Guild

No. 85 / November 2015

Abstract

In its recent *Schrems* judgment the Luxembourg Court annulled Commission Decision 2000/520 according to which US data protection rules are sufficient to satisfy EU privacy rules regarding EU-US transfers of personal data, otherwise known as the 'Safe Harbour' framework. What does this judgment mean and what are its main implications for EU-US data transfers? What is problematic about the US NSA large-scale surveillance programme from the perspective of EU data protection architecture? And what are the risks to companies that continue to transfer data from the EU to the US, and what should the EU do to address the Luxembourg Court ruling?

The Court has concluded that mass surveillance carried out by the US NSA PRISM programme is not consistent with EU data protection rules and goes beyond the proportionality and necessity principles in the name of 'national security'. Access on a generalised basis to electronic communications is tantamount to compromising the *essence* of the EU fundamental right to respect for private life. Any future arrangement for transatlantic transfer of data will therefore need to be firmly anchored in a framework of protection that is commensurate with the EU Charter of Fundamental Rights and the EU's data protection architecture.

SOURCE | Societal Security Network

ISBN 978-94-6138-488-1
Available for free downloading from the CEPS website (www.ceps.eu)

Safe Harbour or into the storm?
EU-US data transfers after the Schrems judgment

Sergio Carrera and Elspeth Guild*

CEPS Paper in Liberty and Security in Europe No. 85 / November 2015

The Court of Justice of the European Union (CJEU) handed down a judgment on 6 October 2015 that surprised many who work on EU-US data transfers. In the *Schrems v. Data Protection Commissioner* judgment (C-362/14) decided by the Grand Chamber,[1] the Court's most authoritative configuration, the CJEU annulled the Commission Decision 2000/520 of July 2000 stipulating that US data protection rules are "adequate" to satisfy the rules comprising the EU data protection architecture regarding the transfer of personal data from the EU to undertakings in the US.

The case dealt with Mr Schrems, an Austrian national and Facebook user who challenged the lawfulness of the automatic transfer of his data from Facebook Ireland to servers located in the US, arguing an inadequate level of data protection in light of the Snowden revelations about large-scale surveillance by the US National Security Agency (NSA).

What does the judgment mean?

The EU-US Safe Harbour framework allows businesses on both sides of the Atlantic to transfer personal data to one another, without requiring specific analysis of data protection regulation or any assessment of its compatibility with EU data protection law.

The programme was designed to reduce the administrative burden of complying with the 95/46 Data Protection Directive, to ensure that data flows to Europe are uninterrupted. It was based on voluntary participation by companies. Although the agreement has been in place since 2000, there has not be a particularly high take-up by companies of its provisions. In fact, much of the personal data transfer between the two continents has taken place outside the terms of the programme.

The EU-US Safe Harbour framework depends on a decision by the Commission that US personal data protection rules provide an "adequate level of protection" for personal data that is consistent with EU standards. That decision, which has been in effect for the past 15 years, has now been annulled by the CJEU in the recent *Schrems* judgment. This means that personal data transfers from the EU to the US cannot rely on the Safe Harbour agreement as protection against claims of a breach of EU data protection rules.

Does the judgment matter?

The answer is yes. EU data protection rules stipulate that transfers may only take place if the destination third country ensures an adequate level of data protection.[2] Mass surveillance carried out by the US NSA PRISM programme, which affects virtually all personal data transfers from the EU to the US, is not consistent with EU data protection rules. The CJEU notes that the Commission itself acknowledged this back in 2013 when it stated that the US authorities were able to access data transferred by EU states and process it

* Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs Programme at CEPS, and Associate Professor/Senior Researcher at the Faculty of Law of the University of Maastricht. Elspeth Guild is Associate Senior Research Fellow at CEPS and Jean Monnet Professor *ad personam* of European immigration law at Radboud University Nijmegen and Queen Mary, University of London.

[1] Case C-362/14, *Schrems v. Data Protection Commissioner*, 6 October 2015.

[2] Article 25(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995.

in ways that are incompatible with the purposes for which it was originally transferred, and going beyond the proportionality and necessity principles in the name of "national security".[3]

As there has been no substantive change in this regard to the US law permitting the NSA to continue its mass surveillance programme, no personal data transfer from the EU to the US is likely to comply with EU data protection rules. This state of affairs is equally true for personal data transfers under Safe Harbour as well as for those outside Safe Harbour.

The only difference between transfers within Safe Harbour and those outside it is that companies signed up to the Safe Harbour regime now no longer have the protection of the Commission Decision of equivalence regarding US data protection rules. Those companies that have been transferring data outside Safe Harbour are also in a worse position now as the Court has made it clear that their personal data transfers to the US are not in compliance with EU data protection rules since the data will be subject to the NSA mass surveillance regime.

What is problematic about the US NSA mass surveillance regime?

The NSA PRISM programme is based on a national security and law enforcement exception to data protection rules. As Advocate General Bot underlined in the analysis of the case,[4] any data transferred to the US is capable of being accessed by the NSA and any other US security agencies in the course of mass and indiscriminate surveillance, without differentiation, limitation or exception. Moreover, EU citizens have no effective remedies in US law against the processing, nor can they request rectification or erasure, of their personal data.

In the EU legal system, as a derogation from the general rule, the national security exception must be contained in law and is subject to a proportionality test. Rules must be adopted that limit the interference with the fundamental rights of persons whose data is in question and it must be justified that the interference with privacy is for a legitimate purpose, which national security is. This, in view of the Court, along with the need to ensure independent judicial review of the application of these derogations by public authorities, constitutes central components to ensuring the rule of law.[5]

Most important of all, any derogation in respect of personal data protection must be subjected to a test to determine whether it is strictly necessary. This requires extensive justification by the state and security authorities. Furthermore, under EU law the individual must be able to challenge a breach of his or her data protection right. Quite a lot would need to be done to amend, limit and control the NSA mass surveillance programme before it could begin to comply with the EU rules and the CJEU standards laid down in the *Schrems* judgment. Indeed, it would need to cease to be a mass surveillance programme; at best it have to be limited to a justified and targeted surveillance programme.

What is the risk to companies that continue to transfer data from the EU to the US?

The CJEU held that the EU Charter of Fundamental Rights requires that there are clear and precise rules governing data transfers so that people whose personal data is transferred have sufficient guarantees. Their data must be effectively protected against the risk of abuse and against any unlawful access and use. As currently operated, the US NSA programme constitutes, as the Court indicates, just such a system of unlawful access and use of personal data that is inconsistent with the Charter's right to privacy.

Every individual who suspects that his or her data is subject to treatment inconsistent with data protection rules must have the right to legal remedy. Any disgruntled individual in the EU must be able to challenge the transfer of his/her personal data to the US on the grounds that it is inadequately protected, including before the courts.

---

[3] Commission Communication, Restoring Trust in EU-US data flows, COM(2013) 846 final, 27.11.2013; Commission Communication, on the Functioning of the Safe Harbour from the Perspective of EU citizens and companies established in the EU, COM(2013) 847, 27.11.2013.

[4] Opinion of Advocate General Bot, 23 September 2015, Case C-362/14, Schrems.

[5] Paragraph 95 of the judgment.

Any company transferring personal data from the EU to the US after 6 October 2015 (and arguably from the Snowden revelations of June 2013 for those companies not signed up to Safe Harbour) will be doing so in breach of EU data protection rules. The remedy for the individual will be compensation and damages for loss and, depending on the national system, distress. A 2013 case from the UK where the breach was purely technical and there was no quantifiable loss to the individual still resulted in a compensation award of €1000.[6]

What about the right to respect for privacy and data protection?

The CJEU held that legislation permitting public authorities to have access on a generalised basis to the context of electronic communications is tantamount to profoundly compromising the *essence* of the fundamental right to respect for private life.[7] The Court also clarified the relationship of two provisions of the EU Charter – the right to respect for privacy (Article 7) and the entitlement to data protection (Article 8). The right to respect for privacy is fundamental. It is this right that makes rules on data protection to safeguard privacy and thus limit and exclude all interferences, except in so far as an interference is strictly necessary.[8] The CJEU also held that for establishing the existence of that interference

> …it is not relevant whether the information related to the private life of the person have [sic] suffered any adverse consequences on account of that interference.[9]

The parameters of proposed or claimed exceptions to data protection are not autonomous to the field of data protection, they are established and determined by the right to respect for privacy. Thus, any exception or derogation in a data protection regime is only valid *if* it is consistent with individuals' rights to respect for privacy. The two – privacy and data protection – cannot be separated and there is a hierarchical relationship between them: privacy is the superior right to which data protection is the mode of achievement of the right. This is confirmed by the right of the individual to a remedy in respect of his or her privacy. It is in determination of that right of privacy that the adequacy of a data protection regime must be tested.

In the same vein, the CJEU ruling also clarifies the central role played by national data protection authorities (DPAs) and the importance of ensuring their independence at times of ensuring the effectiveness of the right to privacy and of the EU data protection system. The Court held that whatever the European Commission may determine as regards the level of adequacy on data protection in any third country, national data protection supervisory authorities cannot see their supervisory powers reduced or circumvented, and have the competence to examine individual claims concerning the protection of their rights regarding the processing of their data.[10]

What next?

The way in which the CJEU has presented the judgment is particular. The main legal reasoning is deeply embedded in the EU treaties and the EU Charter of Fundamental Rights. This means that it is not possible to sort out the EU-US data transfer issue through another (new Safe Harbour) agreement between the two countries unless that agreement is accompanied by changes to the NSA PRISM mass surveillance programme that bring it into line with EU data protection rules; much less could the issue be resolved by EU secondary legislation.

There are alternative transfer tools,[11] such as those envisaged in Directive 95/46 (Articles 25 and 26). Yet it is very unlikely that any 'consent' by an individual to the transfer of his or her data to the US will be valid.

---

[6] *Halliday v. Creation Consumer Finance Ltd* [2013] All ER (D) 199 (Mar).

[7] Refer to paragraph paragraphs 94 and 95 of the judgment. See also Case C-293/12 and 594/12 *Digital Rights Ireland*. E. Guild and S. Carrera (2014), "The Political Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", CEPS Liberty and Security Series, CEPS: Brussels.

[8] Paragraph 92.

[9] Paragraph 87. The Court made here reference to *Digital Rights Ireland* judgment, paragraph 33.

[10] Paragraph 53 of the judgment.

[11] European Commission, Communication on the transfer of personal data from the EU to the US under Directive 95/46 following the judgment by the Court of Justice of the European Union, COM(2015) 566 final, 6.11.2015.

In light of the comprehensiveness and secrecy of the NSA mass surveillance programme, it is virtually impossible for an individual to have any idea of what kind of uses of his or her data he or she may be consenting.

Other options include contractual tools such as so-called Binding Corporate Rules (BCR) or sets of EU model clause transfers.[12] Yet data exporters and importers remain responsible for verifying that the EU data protection law is respected in the case of structural transfers, subject to the supervision of national DPAs. In fact, national DPAs such as those in Germany have expressed concerns regarding their use as they do not guarantee compliance with EU privacy standards or announce any new approvals of BCRs or data export agreements.[13] Indeed, as the Commission has recently argued under these contractual tools

> … it cannot be assumed that the data importer in the third country is subject to an adequate system of oversight and enforcement of data protection rules.[14]

The Article 29 Data Protection Working Party issued an Opinion on October 16th where it held that if no solution could be found before the end of 2015, "EU Data Protection Authorities will take all necessary steps, including enforcement action".[15] The European Commission has confirmed its plans to conclude discussions with the US on a renewed and stronger arrangement for transatlantic data flows with a higher level of protection.[16]

Still, it is not clear how this new arrangement will pass the legality test developed by the Court in the *Schrems* judgment. The Commission itself has pointed out that the biggest challenge in the judgment will be to guarantee that there are "sufficient limitations and safeguards to prevent access or use of personal data on "generalised basis" and to ensure that there is sufficient judicial control" of these practices in the US.[17]

Moreover, the judgment has brought some clarity to the definitional components of what an "adequate level of data protection" in a third country actually means for the purposes of EU law. The Court has held that this corresponds to a level that is "essentially equivalent" to that guaranteed by Directive 95/46[18] and the EU Charter of Fundamental Rights.[19] Any new legal framework will need to meet this CJEU standard of "essentially equivalent" protection.

For the moment, businesses should avoid the transfer of personal data from the EU to the US. Each transfer is potentially a damages or compensation claim in waiting. For companies that have systems in place that centralise personal data in the US entailing transfers from the EU it might be wise to limit the personal data exchanged to an absolute minimum and seek to avoid it as quickly as possible.

---

[12] See, for instance, Commission Decision 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46, OJ L 181, 4.7.2001; Commission Decision 2004/915 of 27 December 2004 amending Decision 2001/497 as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004.

[13] Sondersitzung der DSK am 21. Oktober 2015 in Frankfurt, 1 Positionspapier der DSK.

[14] COM(2015) 566 final, p.6.

[15] Statement of the Article 29 Working Party, Brussels, 16 October 2015.

[16] European Commission, Communication on the transfer of personal data from the EU to the US under Directive 95/46 following the judgment by the Court of Justice of the European Union, COM(2015) 566 final, 6.11.2015. See also European Commission, Speech/15/5916, Commissioner Jourová's remarks on Safe Harbour EU Court of Justice Judgment before the Committee on Civil Liberties, Justice and Home Affairs (LIBE), Strasbourg, 26 October 2015. Refer also to European Commission Statement, First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems), Strasbourg, 6 October 2015.

[17] Ibid.

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23/11/1995.

[19] Paragraph 73 of the judgment and paragraphs 142-145 of the Advocate General Opinion.

The recently appointed President of the CJEU, Koen Lenaerts, declared when asked about the judgment, that

> Europe must not be ashamed of its basic principles: the rule of law is not for sale. It is a matter of upholding the requirements of the European Union, of the rule of law, of fundamental rights.

In his view this lies at the basis of the EU's "core constitutional identity".[20] The *Schrems* judgment indeed sends a strong message to EU policy-makers about the need to firmly anchor any legislative acts on transfer of data upon a framework of protection commensurate with the EU Charter of Fundamental Rights and the EU's data protection architecture.

[20] ECJ President on EU Integration, "Public Opinion, Safe Harbour, Antitrust", *The Wall Street Journal*, 14 October 2015. See also paragraph 60 of the judgment.