SCHREMS V DATA PROTECTION COMMISSIONER (CASE C-362/14): EMPOWERING NATIONAL DATA PROTECTION AUTHORITIES

Marina Škrinjar Vidović*

Summary: On 6 October 2015, the Court of Justice of the European Union (CJEU) issued the final ruling in Schrems v Data Protection Commissioner (Case C-362/14). In its ruling the Court invalidated the Safe Harbour arrangement, which governs data transfers between the EU and the US. While the decision does not automatically put an end to data transfers from Europe to the United States, it allows each country's national regulators to suspend transfers if the company in the United States does not adequately protect user data. The paper analyses the most important aspects of the judgment: the Court's definition of the competences of national data protection authorities, the Court's interpretation of the criteria for 'adequacy' under Article 25(6) of Directive 95/46/EC and the reasoning of the Court for the invalidation of the Safe Harbour Agreement. Further, and in line with the findings of the Court, the paper analyses the relationship between state surveillance and data protection and examines the consequences of the Court's ruling.

1 Introduction

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued the final ruling in *Schrems v Data Protection Commissioner* (Case C-362/14).

In its ruling the Court invalidated the Safe Harbour arrangement, which governs data transfers between the EU and the US. While the decision does not automatically put an end to data transfers from Europe to the United States, it allows each country's national regulators to suspend transfers if the company in the United States does not adequately protect user data.

Consequently, US companies are no longer allowed to transfer private data from the EU to the US solely on the basis that they are members of the Safe Harbour scheme. Instead they will have to seek specific

* Marina Škrinjar Vidović, LLM (Utrecht). The author wishes to thank two anonymous reviewers for their comments and guidance.

contractual authorisation to export data.[1] US companies say this will increase costs, create delays and force them to duplicate US data servers in the EU.[2]

Obviously, the ruling will have a big impact on businesses that transfer personal data to a company of the same group or a service provider in the US. It affects giant social networks such as Facebook, search engines like Google, cloud hosting providers such as Microsoft, and thousands of other companies that do business in the EU and that transfer personal data to the US.

Accordingly, the judgment has attracted great public attention and has received the status of a 'landmark' and 'historical' decision in the area of data protection.[3]

However, perhaps the most important aspect of the ruling is that it raises the issue of mass surveillance and emphasises the need for balance between national security protection demands and respect for the protection of private data as a fundamental right. The recent increase in terrorist attacks worldwide has most certainly triggered broad measures allowing intelligence services to introduce even wider actions in the hope of preventing further violence, which makes this case even more relevant.

2 Background

The *Schrems* case was initiated by Maximillian Schrems, an Austrian student and a Facebook subscriber, who challenged Facebook's transfer of his personal data to the US under the Safe Harbour Agreement.

Schrems made a complaint to the Irish Data Protection Commissioner, due to the fact that all Facebook subscribers residing in the European Union are asked to sign a contract with Facebook Ireland, a subsidiary of the parent company Facebook Inc established in the US.

---

[1] For alternative bases for transfers of EU personal data to the US, see: Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) COM (2015) 566 final.

[2] See some of the related articles from the following sources: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/what-is-safe-harbour-all-you-need-to-know-about-the-data-transfer-scheme-a6683701.html; http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection> all accessed 28 November 2015.

[3] See some of the articles at <http://www.reuters.com/article/2015/10/07/us-eu-ireland-privacy-schrems-idUSKCN0S124020151007; http://www.wired.co.uk/news/archive/2015-10/06/what-does-the-end-of-safe-harbour-mean; http://uk.businessinsider.com/safe-harbor-emoji-explained-facebook-ecj-screms-2015-10, http://www.forbes.com/sites/thomasbrewster/2015/10/06/safe-harbour-invalid/> all accessed 28 November 2015.

Some or all of the data of subscribers to Facebook Ireland residing in the EU are transferred to Facebook Inc servers in the US, where they are kept. The substantive law governing these transfers of personal data is the Safe Harbour Agreement between the EU and the US. This Agreement was put into effect in 2000 by a Commission decision[4] which was adopted pursuant to Article 25 of the Data Protection Directive[5] (Directive). The Directive provides for the requirement that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of data protection. Article 25(6) of the Directive provides that the European Commission may find that a third country ensures an adequate level of protection. If the Commission adopts a decision to that effect (adequacy decision), the transfer of personal data to the third country concerned may take place.

In this regard, the Commission adopted the Safe Harbour Agreement for US businesses. Within the Safe Harbour regime, all US companies subject to the Agreement were authorised to proceed with data transfers without requiring the individual authorisation of national data protection authorities of the EU country in question. More than 4,000 US companies have been certified under the Safe Harbour programme.[6] Among those certified are some of the world's largest corporations and information service providers.

According to the established regime, a US company that seeks to comply with the Safe Harbour must: (a) identify in its publicly available privacy policy that it adheres to the Safe Harbour principles and actually does comply with them; and (b) self-certify, ie declare to the US Department of Commerce that it is in compliance with the Safe Harbour principles. The self-certification must be resubmitted on an annual basis.[7]

A number of mechanisms, combining private dispute resolution and oversight by the public authorities, exist to check compliance with the Safe Harbour principles. The adequacy decision permits the limitation of these principles, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and

---

[4] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance) [2000] OJ L215/7.

[5] 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 [1995] OJ L281/31.

[6] The full list of companies is available at 'US-EU Safe Habour List' (*Export.Gov*) <https://safeharbor.export.gov/list.aspx> accessed 28 November 2015.

[7] More information at 'Safe Habor' (*Export.Gov*) <http://www.export.gov/safeharbor/index.asp> accessed 28 November 2015.

> by statute, government regulation, or case law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation.[8]

As the *Schrems* case will reveal, it is questionable whether this provisions of the Decision are in accordance with the Data Protection Directive and the EU Charter of Fundamental Rights.[9]

Schrems claimed, in essence, that the law and practices of the US offer no real protection of personal data against US state surveillance. Concretely, he claimed that, according to the allegations raised by Edward Snowden, the US National Security Agency (NSA) through the PRISM programme obtained unrestricted rights to intercept and survey data (including personal data) held by Safe Harbour participants in the US, including Facebook.

The Irish Data Protection Commissioner rejected Schrems' complaint on the basis that, according to the Irish statute, the adequacy decision was final, and he was bound to allow the transfer of personal data under the EU/US Safe Harbour regime.

Schrems subsequently brought proceedings before the Irish High Court against the Irish Data Protection Commissioner for his refusal to investigate and suspend the data flows. The High Court found that if the matter were to be determined solely by Irish law, it would have to end the case. It recognised, however, that implementation of EU law must be carried out in the light of the EU Charter. Therefore, the Irish High Court, which doubted that Safe Harbour system was compatible with EU law (or indeed the Irish Constitution), stayed the proceedings and submitted the following two questions to the CJEU for a preliminary ruling:[10]

> Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data

---

[8] Lorna Woods, 'Schrems v Data Protection Commissioner: The Beginning of the End for Safe Harbour?' (*Information Law and Policy Centre at IALS*, 23 September 2015) <http://infolawcentre.blogs.sas.ac.uk/> accessed 28 November 2015

[9] Charter of Fundamental Rights of the European Union [2000] OJ C364/8, 18 December 2000; [2010] OJ C83/389, 30 March 2010.

[10] Case C–362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.

> subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC1) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/012), the provisions of Article 25(6) of Directive 95/46/EC3 notwithstanding?
>
> Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?

3 Judgment

Prior to the final ruling, the Advocate General Yves Bot issued on 23 September 2015 his non-binding legal opinion on the case according to which he indicated that the Safe Harbour Agreement for data transfer between the EU and US fails to protect the privacy of EU citizens and must be declared invalid. More concretely, he stated that the Commission's decision could not limit the powers of data protection authorities granted under the Directive and that the US system was inadequate, particularly as regards the safeguards against mass surveillance.

The opinion has triggered a lively debate, during which the US Mission to the EU issued a statement calling the Advocate General's opinion into question.[11]

However, the final ruling of the CJEU is very much in line with the Advocate General's opinion. According to the CJEU, national regulatory bodies, such as the Irish Data Protection Commissioner, can investigate whether or not the US affords an adequate level of protection, and could contradict the European Commission's decision that the Safe Harbour provides an adequate level of protection of personal data for EU citizens. Moreover, in accordance with the Advocate General's opinion, the Court has gone further and said that the adequacy decision is invalid since the Safe Harbour agreement does not offer a level of data protection equivalent to the level of protection in place in the EU. In particular, the Court found that the access enjoyed by the US intelligence services to the transferred data interferes with the right to respect for private life and the right to protection of EU citizens' personal data both guaranteed under the EU Charter.

In the following paragraphs the most important aspects of the judgment are analysed: the Court's definition of the competences of national

[11] 'Safe Harbor Protects Privacy and Provides Trust in Data Flows that Underpin Transatlantic Trade' (*United States Mission to the European Union*, 28 September 2015) <http://useu.usmission.gov/st-09282015.html> accessed 28 November 2015.

data protection authorities, the Court's interpretation of the criteria for 'adequacy' and the reasoning of the Court for the invalidation of the Safe Harbour Agreement.

3.1 The powers of data protection authorities

In line with the previous case law and the Advocate General's opinion,[12] in its ruling the Court emphasised the importance of the protection of personal data as a fundamental right to respect for private life, guaranteed by Article 7 of the EU Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof. The Court stated that the Directive, which must be read in the context of the Charter, has no provision that prevents oversight by the national data protection authorities of transfers of personal data to third countries which have been the subject of an adequacy decision. The Court had previously ascertained that the supervisory authorities are the guardians of fundamental rights and freedoms put at stake by data processing operations.[13] Their independence is an essential element of protection and cannot be restricted in any way.[14]

In line with the above, the Court held that individuals had the right to complain to and ask a national authority to investigate the protection of their personal data. Further, the Court explained the different roles of national data protection authorities, national courts and the CJEU in the process.[15]

According to the ruling, the data protection authorities remain responsible for oversight of data processing on their territory, which includes the transfer of personal data outside the EU. Thus, even if the Commission has adopted an adequacy decision, the national data protection authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the Directive.

At the same time, the Court states that Commission decisions are binding and benefit from a presumption of legality, as stated in recital 52 of the judgment:

> .... until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly

---

[12] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, Opinion of Advocate General Bot ECLI:EU:C:2015:627, recital 72.

[13] Case C-288/12 *Commission v Hungary* ECLI:EU:C:2014:237.

[14] Fanny Coudert, 'Schrems vs Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities (*European Law Blog*, 15 October 2015). <http://europeanlawblog.eu/?p=2931> accessed 28 November 2015.

[15] Schrems (n 10) recital 38-66.

> cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality ...[16]

Therefore, the CJEU distinguishes between the right and power of investigation of and challenge to Commission decisions, and the declaration of the invalidity of such decisions. While the former remains with national data protection authorities as described above, the latter, following longstanding jurisprudence,[17] remains within the CJEU.

The Court explains that data protection authorities must consider claims challenging adequacy decisions seriously. If a data protection authority thinks that a claim is unfounded, the complainant can challenge its decision before the relevant national court, which must refer the issue of the validity of the decision to the CJEU if it thinks it may be well founded. If, on the other hand, the data protection authority thinks the complaint is well founded, there must be rules in national law allowing the data protection authority to go before the national courts in order to have the issue referred to the CJEU. As mentioned in some of the reviews of the judgment, it is unfortunate that the Court did not consider the alternative route of the national data protection authority calling on the Commission to amend its decision, and bringing a failure to act proceeding directly before the CJEU.[18]

We can conclude that the judgment defines three aspects of the competences of data protection authorities with regard to the adequacy decision: they are obliged to *examine complaints* from individuals regarding the treatment of their personal information by other countries; they are entitled to *bring cases in front of the national court* to question the validity of adequacy decisions; and they are entitled to *suspend the transfer of personal information* to other countries when they believe it is appropriate.

The above defined powers of the data protection authorities have largely challenged the current understanding of the binding nature of the EU adequacy decisions.[19]

---

[16] Schrems (n10) recital 52.

[17] See Case 314/85 *Foto-Frost v Hauptzollamt Lübeck-Ost* ECLI:EU:C:1987:452.3

[18] Steve Peers, 'The Party's Over: EU Data Protection Law after the Schrems Safe Harbour Judgment' (*EU Law Analysis*, 7 October 2015) <http://eulawanalysis.blogspot.hr/2015/10/the-partys-over-eu-data-protection-law.html> accessed 28 November 2015.

[19] Eg see Stephen Lawson, 'With Safe Harbor Gone, the Hard Work on Data Transfers Starts Now' (*PCWorld*, 6 October 2015) <http://www.pcworld.com/article/2990023/with-

3.2 Definition of adequacy

Article 25(6) of the Directive gives the Commission the power to decide that transfers of personal data outside the EU receive an 'adequate level of protection' in particular countries. The CJEU stated that the Directive gives no definition of what is required in order to ensure protection under the adequacy decision, so it has to interpret the rules.

According to the CJEU, there are two aspects that have to be taken into consideration when examining an adequacy decision. Article 25(1) of the Directive states the requirement that the level of data protection has to be 'adequate' and Article 25(6) states that the protection has to be 'ensured'. The CJEU agreed with the Advocate General's opinion that Article 25 is 'intended to ensure that the high level of that protection continues where personal data is transferred to a third country'.[20] That requirement does not, however, mean that protection in third countries must be identical, but rather that it is 'essentially *equivalent* to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter'[21] and '*effective* in order to ensure protection essentially equivalent to that guaranteed within the European Union'.[22]

Therefore, the Court interprets the word 'adequate' as requiring a high level of protection of private data in the third country. That high level of protection does not have to be identical to the EU standard, but must, as cited above, be 'substantially equivalent' to that in the EU and must be 'effective'. Otherwise, the objective of ensuring a high level of protection would not be met, and the EU's internal standards for domestic data protection could easily be avoided. Also, the Court states that the means used in the third state to ensure data protection rights must be 'effective…in practice', although they 'may differ' from those in the EU.

Furthermore, the Court says that the Commission has to check periodically whether the original assessment that protection is adequate is still justified, and has to check in any event when new evidence gives rise to a doubt whether that is so. In this regard, the Court's judgment requires that any adequacy decision is based on a broad analysis of the third country domestic laws and international commitments.

As to the Safe Harbour adequacy decision, we have to mention that the European Commission issued communications on the implementa-

safe-harbor-gone-the-hard-work-on-data-transfers-starts-now.html> accessed 28 November 2015.

[20] Schrems (n 10) recital 72.

[21] Schrems (n 10) recital 73.

[22] Schrems (n 10) recital 74.

tion of the Safe Harbour Agreement in 2002,[23] 2004[24] and, following the revelations on US surveillance programmes, in 2013,[25] in which it repeatedly reported on weaknesses in transparency and weaknesses in the enforcement of the Safe Harbour arrangement; however, it failed to take action and review the adequacy decision. This is why the Court then states that in light of the importance of privacy and data protection, and the large number of persons whose rights will be affected if data are transferred to a third country with an inadequate level of data protection, the Commission has reduced discretion, and is subject to judicial review.[26]

3.3 Invalidation of the Safe Harbour

Following the above-established interpretation of rules and procedure, the CJEU examined the validity of the Safe Harbour Agreement.

Contrary to the Attorney General's opinion, the CJEU does not focus its analysis on an assessment of the legitimacy of the US surveillance programme – the factual basis of this analysis was highly contested by the US Mission to the EU and by US scholars. Instead, it analyses the decision in light of the requirements imposed by Article 25(6).[27]

In the judgment, the Court quoted the Commission's 2013 Review[28] of the Safe Harbour decision which found that US authorities could access personal data transferred from the EU, and then process the data for purposes incompatible with the original transfer beyond what was strictly necessary and proportionate for the purposes of national security, and that there was no administrative or judicial means to ensure access to the data and their rectification or erasure.

The Court held that the system of self-certification of a company, in which a company declares it will obey the data protection principles as envisaged under the Safe Harbour Agreement, could only constitute a reliable measure of adequacy if the same was backed by mechanisms

---

[23] Commission Staff Working Paper, 'The Application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce' SEC (2002) 196, 14 February 2002.

[24] Commission Staff Working Document 'The Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions issued by the US Department of Commerce' SEC (2004) 1323, 20 October 2004.

[25] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847.

[26] Steve Peers (n 18).

[27] Coudert (n 14).3

[28] Commission (n 25).

to identify and punish US companies which do not obey Safe Harbour principles. In line with the cited Commission's Review, the Court came to the conclusion that the Safe Harbour arrangement does not have in place that kind of mechanism and the rules could be overridden by national security requirements set out in US law.

Additionally, the Court concluded that in the context of state surveillance, while EU law, interpreted in the light of the Charter and the prior case law, limit state interference to what is strictly necessary, the adequacy decision allows US authorities to store all personal data on a general basis. Such a general collection and processing of data, ie mass surveillance, without the possibility of an effective remedy, the Court declared, constitutes a violation of the rights guaranteed under the Charter.[29]

Finally, Article 3 of the adequacy decision restricted data protection authorities' competence to take action to prevent data transfers in the event of an inadequate level of data protection in the USA. According to the previously defined roles and responsibilities of the data protection authorities, this was also declared contrary to the data protection Directive (read in light of the EU Charter).

According to the described findings, the Court declared the entire Decision invalid. The Court did not limit the effect of its ruling.

Following the judgment, the European Commission issued a guidance document[30] in which it noted that all the other adequacy decisions that the European Commission had issued for third countries pursuant to Article 25(6) of the Directive[31] contain a limitation on the powers of the data protection authorities identical to that in Article 3 of the Safe Harbour Decision, which the CJEU considered invalid. Therefore, the Commission announced it would prepare a decision replacing that provision in all existing adequacy decisions and also engage in a regular assessment of existing and future adequacy decisions, as the CJEU had required.

Following the judgment, the Irish supervisory authority is required to examine Schrems' complaint with all due diligence and, at the conclusion of its investigation, it has to decide whether, pursuant to the Directive, transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that the US does not afford an adequate level of protection of personal data.

---

29 Schrems (n 10) recital 95

30 See Commission (n 1).

31 See list of countries in 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries' (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 1 December 2015.

4 The context and implications of the ruling

The *Schrems* judgment is in line with the rest of the case law, where the CJEU has taken a hard line on the interpretation of EU data privacy law, such as:

- in the *Digital Rights Ireland* case,[32] where the CJEU declared the EU Data Retention Directive invalid on the basis that the Directive lacked safeguards that limit government collection and access to individuals' data, and that it also omitted controls over what the data can be used for;
- in the *Google Spain* case[33] ('the right to be forgotten'), where the CJEU established the principle of the applicability of EU data protection rules to a search engine;
- in the *Ryneš* case,[34] where the CJEU found that domestic video surveillance which films a public area cannot be exempt from the obligations contained in the EU Data Protection Directive by virtue of the 'household exemption';
- in the *Weltimmo* case,[35] where the jurisdiction of the national data protection commissioners is even more enhanced: the CJEU ruled that more than one national data protection authority could have competence to regulate multinational business, irrespective of where that business has its registered office in the EU.

One must note that all of the cited judgments were brought within a short time, which corresponds to the start of negotiations for the new EU data protection regulation.[36]

At the heart of the *Schrems* case is the question whether the US ensures an adequate level of data protection in order to prevent the abuse of private data. Basically, the problem was that the rules of the Safe Harbour principle could be overridden by national security requirements set out in US law. This is a question that was discussed well before the *Schrems* case began. As mentioned above, back in 2002 and 2004, and then again in 2013, the Commission issued implementation reports in which it recognised weaknesses in the Safe Harbour system. On all oc-

---

[32] Case C-293/12 *Digital Rights Ireland Ltd* ECLI:EU:C:2014:238.

[33] Case C–131/12 *Google Spain and Google* ECLI:EU:C:2014:317.3

[34] Case C–212/13 František Ryneš v Úřad pro ochranu osobních údajů EU:C:2014:2428.

[35] ,Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság ECLI:EU:C:2015:639.

[36] See: 'Reform of the Data Protection Legal Framework in the EU' (*European Commission: Justice*), <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 1 December 2015.

casions, the Commission, however, preferred to work closely with the US institutions to improve the enforcement of the Agreement in the US rather than to review the content of the adequacy decision.

In addition, the *Schrems* case should be read in a wider context, in relation to Edward Snowden's allegation in 2013 of extensive, global, internet, and phone surveillance by US intelligence, which included European Union offices in the US and Europe, as well as high-ranking EU politicians and Member State heads of state and government.[37] Following these revelations, on 12 March 2014 the European Parliament adopted a Resolution[38] on the electronic mass surveillance of EU citizens. With its vote (285 votes to 281), the Parliament decided to call on EU Member States to 'drop any criminal charges against Edward Snowden, grant him protection and consequently prevent extradition or rendition by third parties, in recognition of his status as whistle-blower and international human rights defender'.

Taking all the above into consideration, the CJEU's ruling in the *Schrems* case should have been expected. Following the judgment, the European Parliament adopted a Resolution[39] on 29 October 2015 stating that the *Schrems* case had confirmed the long-standing position of Parliament regarding the lack of an adequate level of protection under the Safe Harbour instrument. Additionally, in the Resolution, the Parliament

> urges the Commission to assess the legal impact and implications of the Court of Justice ruling of 6 October 2015 in the Schrems case (C-362/14) vis-à-vis any agreements with third countries allowing for the transfer of personal data, such as the EU-US Terrorist Finance Tracking Programme (TFTP) Agreement, passenger name record (PNR) agreements, the EU-US umbrella agreement and other instruments under EU law which involve the collection and processing of personal data.

Taking into account the findings of the Court on the US mass-surveillance of EU citizens, it is proper and desirable to encourage the European Commission to review all other instruments for cross-border trans-

---

[37] See 'Attacks from America: NSA Spied on European Union Offices' (*Spiegel Online International*, 29 June 2013) <http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html> accessed 28 November 2015.

[38] European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

[39] European Parliament Resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP)).

fers of personal data to the US. However, this will most certainly have an impact on the cross-border economy, and US companies are struggling to find other applicable procedures for transferring EU personal data. And this is a challenge.

Following the ruling, the Article 29 Working Party – an independent advisory body that brings together representatives of all data protection authorities of the Member States as well as the European Data Protection Supervisor – issued a Statement[40] on the implementation of the *Schrems* judgment:

> urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights.

Additionally, the Statement says:

> In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. In any case, this will not prevent data protection authorities to investigate particular cases, for instance on the basis of complaints, and to exercise their powers in order to protect individuals.

And it goes on to conclude:

> If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions.

Accordingly, and in line with this Statement, the European Commission issued a guidance document[41] relating to transatlantic data transfers after the *Schrems* ruling. In the guidance, the Commission joins the Article 29 Working Party in the position that alternative tools authorising data flows can still be used by companies for lawful data transfers to third countries, including to the US. These alternative tools are standard

---

[40] 'Statement of the Article 29 Working Party' (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm> accessed 28 November 2015

[41] See Commission (n 1).

contractual clauses under Article 26(4) of the Directive[42] (which specify data protection obligations and are pre-approved by the Commission), binding corporate rules[43] (for transfers within a multinational corporate group, which are pre-approved by the national Data Protection Authorities), and derogations under Article 26(1)(a) of the Directive.[44]

Pursuant to the Commission guidance document, reliance on the defined alternative tools is subject to two conditions: (1) transfers to a third country can be lawfully made only if the data have originally been collected and further processed by a data controller established in the EU in accordance with the applicable national laws transposing Data Protection Directive; and, (2) where the Commission does not find adequacy, controllers are responsible for making sure that transfers take place with sufficient safeguards. Compliance with these requirements is ultimately assessed by national data protection authorities. This means that data protection authorities play a central role as they are the main enforcers of the fundamental rights of data subjects and are responsible for supervising data transfers from the EU to third countries, in full independence. In the guidance document, the Commission invites data controllers to cooperate with the data protection authorities, thereby helping them to effectively carry out their supervisory role.

---

[42] See 'Model Contracts for the Transfer of Personal Data to Third Countries (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 1 December 2015

[43] See 'Overview on Binding Corporate Rules' (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm> accessed 1 December 2015

[44] Article 26(1) of the Directive: '1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:
(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.'
Only one of the above named legal bases has the potential for massive data transfer. Data controllers may use clauses in consumer contracts as 'unambiguous consent' waiving EU protection under Article 26(1)(a) of the Data Protection Directive. But these boilerplate clauses may not be informed consent or withstand challenge under EU privacy or unfair contract terms law.

However, in the Commission's view, a renewed and sound framework for transfers of personal data to the US remains a key priority. The Commission states that it hopes to conclude the negotiations with the US government on a new arrangement for transatlantic data transfers within three months, coinciding with the end of the 'grace period' which the Article 29 Working Party has implicitly granted until the end of January 2016.

In the meantime, companies are forced to either violate the European data protection rules and share the personal information as ordered by US authorities, or they can refuse to share the information and be at risk of penalties for not responding to a request from the US government. In this regard, an important case is continuing in the US that deals with the question of surveillance and EU data protection rules: *US Department of Justice v Microsoft.* The issue of the case is that the US Department of Justice wants access to a customer's data relevant to a drug trafficking investigation, stored on a Microsoft server in Ireland. While Microsoft said it would not give the information without an Irish court consenting to it, the Department of Justice said that because Microsoft is an American company and can access the data, the warrant that it produced is valid.[45] This case is further proof of the need for agreement on common US/EU standards on privacy protection, and for the development of a new framework for facilitating legal, transparent law enforcement data requests across borders.

5 Conclusion

We are living in the information world, and information represents power. Rapid technological developments have brought new challenges for the protection of information. The EU and the US are each other's most important trading partners, and data transfers, increasingly, form an integral part of their commercial exchanges. Brutal terror attacks and technological innovations making large-scale communications data monitoring possible have further complicated the matter, triggering concerns about violations of the rights to privacy and data protection in the name of national security protection. A transatlantic dialogue is needed not only on guiding principles for intelligence collaboration, but more generally on the appropriate limits of surveillance in the age of big data.

[45] See a number of articles related to this at the following sources: <http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant>; <http://www.pcworld.com/article/2981641/legal/microsoft-headed-to-court-to-protect-irish-data-from-us-doj-search.html>; <http://www.infoworld.com/article/2859897/internet-privacy/microsoft-vs-doj-the-battle-for-privacy-in-the-cloud.html> accessed 28 November 2015.

According to the EU, building trust in the online environment is a key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risk is slowing down the development of innovative uses of new technologies. Therefore, personal data protection plays a central role in the Digital Agenda for Europe,[46] and more generally in the Europe 2020 Strategy.[47] Accordingly, in January 2015 the European Commission revealed a draft of its European Data Protection Regulation to replace the present Data Protection Directive.[48] The completion of this reform is a policy priority for 2015.[49]

In line with CJEU case law, the Regulation should confirm and even enhance the powers and independence of national data protection authorities, with the final aim of putting control of personal data back in the hands of European citizens. One can also expect that, in accordance with the case law, the focus of the Regulation will be on the protection of privacy and respect for data protection, while the free movement of data seems to come a poor second whatever the data industry and the legal basis for the Directive might have to say.[50]

On both sides of the Atlantic, the Court's decision in the *Schrems* case was received with great attention by politicians and businesses. The Commission immediately announced it would renegotiate the scheme[51] under which personal data would be transferred from the EU to the US. Even though the US and European regulators are negotiating an updated Safe Harbour framework, the timetable of its enactment is unclear.

The implications of *Schrems* go much wider than just the invalidity of EC Decision 2000/520. The judgment has brought into clear view the conflict of laws between Europe and the US. While the US has viewed the data privacy issue mainly as a matter of commerce and at the same time subject to use at the sole discretion of the state, the EU views it as a matter of fundamental human rights. As the US companies (Safe Harbour or not) cannot escape or opt out of the current US surveillance programmes, based on the views expressed in *Schrems* it is difficult to see how any form of transfer can be said to adequately protect personal data.

---

[46] Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe COM (2010) 245 final, not published in the Official Journal.

[47] Communication from the Commission of 3 March 2010 – Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth COM (2010) 2020 final.

[48] 'Reform of the Data Protection Legal Framework in the EU' (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 28 November 2015.

[49] 'Protection of Personal Data' (*European Commission: Justice*) <http://ec.europa.eu/justice/data-protection/index_en.htm> accessed 28 November 2015.

[50] See Woods (n 8).

[51] Commission (n 1).

The question underlying the *Schrems* case is the scope and extent of the lawful state surveillance of citizens. This ruling will be very useful for the fight against mass surveillance in Europe. EU Member States do not all have the same position in respect of the scope of state surveillance.[52] In 2013 the EU Parliament adopted on that issue a Resolution[53] where it

> …expresses serious concern at the revelations relating to the alleged surveillance programmes run by Member States, either with the help of the US National Security Agency or unilaterally; calls on all the Member States to examine the compatibility of such programmes with EU primary and secondary law, in particular Article 16 TFEU on data protection, and with the EU's fundamental rights obligations deriving from the ECHR and the constitutional traditions common to the Member States.

On the other hand, we should take into account the latest events following the recent terrorist attack in Paris, and warnings and announcements of other attacks in EU capitals which significantly endanger the safety of EU citizens. It is expected that the situation of emergency will certainly increase the activities of security agencies and state surveillance.

In the context of empowering national data protection authorities by the CJEU case law, Member States may differ in defining standards of the protection of personal data of its citizens. Therefore, even if the European Commission and the US agree on a new Safe Harbour scheme, in accordance with the powers defined in the *Schrems* case, national data protection authorities may still restrict data transfers in cases where they feel that the privacy rights of data subjects are violated. This is why it is necessary to reach a political agreement between EU Member States on state surveillance issues, in order to have a common position in negotiating with the US the new Safe Harbour 2.0, and to find a commonly agreed balance between state surveillance in the name of national security and the protection of private data as a human right.

---

[52] See European Union Agency for Fundamental Rights, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Mapping Member States' Legal Frameworks (FRA – European Union Agency for Fundamental Rights 2015).

[53] European Parliament Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)).