



Date de réception : 23/01/2015



|                               |                |
|-------------------------------|----------------|
| Published ID                  | : C-362/14     |
| Document number               | : 13           |
| Register number               | : 976996       |
| Date of lodgment              | : 03/11/2014   |
| Date of entry in the register | : 03/11/2014   |
| Type of document              | : Observations |

|                         |                           |
|-------------------------|---------------------------|
| Lodgment reference      | : Document                |
| File number             | : DC33346                 |
| Person lodging document | : 1                       |
|                         | : Julie Vondung (R249125) |
|                         | : Commission              |



EUROPEAN COMMISSION

LEGAL SERVICE

Brussels, 3 November 2014

sj.f(2014)4003332

*Court procedural documents*

**TO THE PRESIDENT AND THE MEMBERS OF  
THE COURT OF JUSTICE OF THE EUROPEAN UNION**

**WRITTEN OBSERVATIONS**

**submitted by**

**THE EUROPEAN COMMISSION**

represented by Mr Ben Smulders, Principal Legal Adviser, Mr Bernd Martenczuk and Ms Julie Vondung, members of its Legal Service, acting as agents, with an address for service at the office of Ms Merete Clausen, also a member of its Legal Service, Bâtiment Bech, 5 rue A. Weicker, L-2721 Luxembourg, and which consents to service by e-Curia,

**in Case C-362/14,**

Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

**Maximilian Schrems**

v

**Data Protection Officer,**

amicus curiae:

**Digital Rights Ireland Ltd.**

on the interpretation of Commission Decision 2000/520/EC 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.

## TABLE OF CONTENTS

|   |    |
|---|----|
| 1. INTRODUCTION AND SUMMARY .....   | 3  |
| 2. LEGAL FRAMEWORK .....  | 4  |
| 2.1. The Charter of Fundamental Rights .....  | 4  |
| 2.2. Directive 95/46/EC .....   | 5  |
| 2.3. Decision 2000/520/EC (Safe Harbour Decision) .....   | 6  |
| 3. THE COMPLAINT IN THE MAIN PROCEEDINGS AND THE QUESTIONS<br>REFERRED FOR A PRELIMINARY RULING .....   | 8  |
| 4. THE REACTION OF THE EUROPEAN COMMISSION TO THE SNOWDEN<br>ALLEGATIONS .....  | 10 |
| 5. LEGAL ANALYSIS .....   | 13 |
| 5.1. General Observations .....   | 13 |
| 5.2. The conditions of Article 3 (1) (b) of the Safe Harbour Decision are only<br>partly met .....  | 13 |
| 5.2.1. First condition: There is a substantial likelihood that the Principles<br>are being violated .....   | 13 |
| 5.2.2. Second condition: There is a reasonable basis for believing that the<br>enforcement mechanism concerned is not taking or will not take<br>adequate and timely steps to settle the case at issue .....  | 18 |
| 5.2.3. Third condition: The continuing transfer would create an imminent<br>risk of grave harm to data subjects .....   | 18 |
| 5.2.4. Fourth condition: The competent authorities in the Member State<br>have made reasonable efforts under the circumstances to provide<br>the organization with notice and an opportunity to respond ..... | 20 |
| 5.3. No power of the data protection authority to investigate .....   | 20 |
| 6. CONCLUSION .....   | 21 |

The European Commission has the honour to present the following written observations:

## **1. INTRODUCTION AND SUMMARY**

1. The questions referred concern the powers and duties of national data protection authorities under the Safe Harbour Decision<sup>1</sup> following the Snowden revelations on large-scale surveillance programmes of US national security agencies. In the Safe Harbour Decision, the European Commission found in 2000 that US companies subscribing to the privacy principles set out therein ensure an adequate level of protection of personal data and, consequently, personal data can be transferred to these companies according to Directive 95/46/EC on the protection of personal data. The surveillance programmes, the existence of which were revealed in 2013 by whistle-blower Edward Snowden, allow US national security agencies to access personal data transferred to US companies – among which Facebook Inc. - on a mass and indiscriminate basis. Following these revelations the Commission has started to review the Safe Harbour Decision, a process which is still ongoing.
2. The Applicant in the main proceedings, Maximilian Schrems, challenges the refusal of the respondent Irish data protection authority, the Data Protection Commissioner, to investigate further his complaint on the transfer of his personal data by Facebook Ireland Ltd to Facebook Inc. in the US, which has self-certified under Safe Harbour. He is arguing that due to the surveillance programmes (under which PRISM) an adequate level of protection is not ensured anymore and thus such transfer is unlawful. The Respondent contends that he is bound by the finding of the Commission to the contrary in the Safe Harbour Decision. The High Court, in essence, asks whether, in the light of the Charter of Fundamental Rights, the Data Protection Commissioner is indeed absolutely bound by this finding or, alternatively, whether he may and/or must conduct his own investigations in the light of the Snowden revelations.

---

<sup>1</sup> Commission Decision 2000/520/EC 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 (OJ L 215, 25.08.2000, p. 7 – 47).

3. The Commission considers that the Snowden revelations indeed raise serious concerns with a view to the application of the Safe Harbour Decision. For this reason, it has taken action and started the review of the Safe Harbour Decision, as will be presented more in detail later. However, in the Commission's view, a national data protection authority is bound by the Commission's adequacy finding as long as the Safe Harbour Decision itself does not allow the contrary according to its Article 3 (1). Under Article 3 (1) (b), national data protection authorities may in particular suspend data flows to a self-certified organisation *"where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond."* Under circumstances such as in the case before the national court, these conditions are only partially met. Whereas, in the light of the Snowden revelations, *"a substantial likelihood that the Safe Harbour Principles are being violated"* and *"a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue"* do exist, there are no indications that the continuing transfer of personal data of the Applicant by Facebook Ireland Limited to Facebook Inc would create *"an imminent risk of grave harm"* to the Applicant.

## 2. LEGAL FRAMEWORK

4. The legal framework set out by the law of the European Union relevant to the present case is composed of Articles 7, 8 and 47 of the Charter of Fundamental Rights, Art. 25 of Directive 95/46/EC and the Safe Harbour Decision.

### 2.1. The Charter of Fundamental Rights

5. Article 7 of the Charter is drafted as follows:

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

6. Article 8 of the Charter is drafted as follows:

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

7. Article 47 of the Charter is drafted as follows:

Right to an effective remedy and to a fair trial

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

## 2.2. Directive 95/46/EC

8. 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, p. 31 – 50) governs the transfer of personal data to third countries. According to Article 25 of Directive 95/46/EC, in principle, such transfer is only admissible if the third country ensures an adequate level of protection. The Commission may find under Article 25 (6) that a third country ensures such an adequate level of protection; transfers of personal data to this third country are consequently admissible without the necessity of providing additional guarantees. Member States are obliged to comply with the Commission's decision as regards the recognition of the level of protection offered in that country (Article 25 (6), last sub-paragraph).

9. Article 25 of Directive 95/46/EC is drafted as follows:

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other

provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

### **2.3. Decision 2000/520/EC (Safe Harbour Decision)**

10. The Safe Harbour Decision is based on Article 25 (6) of Directive 95/46/EC.

11. According to Article 1, the Safe Harbour Decision governs the transfer of personal data from the EU to organisations established in the US that have self-certified to the Safe Harbour Privacy Principles as set out in Annex I to the Decision and implemented in accordance with the guidance provided by the Frequently Asked Questions (FAQs) issued by the US Department of Commerce as set out in Annex II of the Decision. The Commission's Decision recognises according to Article 1(1) the Privacy Principles and the accompanying FAQs as ensuring an adequate level of protection for personal data transfer to US companies in the US.

12. The fourth paragraph in the preamble to the Privacy Principles issued by the US Department of Commerce and contained in Annex I of the Safe Harbour Decision states:

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; ...



13. Annex III of the Decision sets out an overview of the Safe Harbour enforcement. According to Annex VII, the US Federal Trade Commission and the Department of Transportation are empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.
14. Furthermore, the Safe Harbour Decision outlines and distinguishes respective powers of, on the one hand, the European Commission, and on the other, national data protection authorities of the Member States.
15. The powers of the Commission are referred to in recital 9 and set out in Article 4 of the Safe Harbour Decision.
16. Recital 9 reads as follows:

The "safe harbor" created by the Principles and the FAQs, may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved.

17. Article 4 states in relevant part:

1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.

The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.

2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.

18. The powers of data protection authorities in the Member States are referred to in recital 8 and set out in Article 3 (1) of the Safe Harbour Decision.

19. Recital 8 reads as follows:

In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.

20. Article 3 (1) states in relevant part:

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) ...; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

21. Additionally, Article 3 (2) specifically requires that Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

### **3. THE COMPLAINT IN THE MAIN PROCEEDINGS AND THE QUESTIONS REFERRED FOR A PRELIMINARY RULING**

22. The Applicant, an Austrian national, challenges a decision of the Respondent, the Irish Data Protection Commissioner, not to investigate further the merits of his complaint brought in the wake of the revelations in June 2013 of the mass surveillance of internet and telecommunications data by the US national security agencies ("the Snowden revelations"). The Applicant has been a customer of the social networking service "Facebook" operated by Facebook Ireland Ltd since 2008. Facebook Ireland Ltd transfers some or all data of its customers to its parent company in the United States of America, Facebook Inc. Facebook Inc. is self-certified under the Safe Harbour Regime. The essence of Mr Schrems' complaint to the Respondent was that, in light of the Snowden revelations,

there was no meaningful protection in US law and practice in respect of data transferred by the company Facebook Ireland to its US parent company so far as State surveillance was concerned. He did not raise any special implications of the mass surveillance for his own situation.

23. In assessing the complaint, the Commissioner did not find evidence that Mr Schrems' own personal data had been disclosed to the US (*locus standi* objection). The Commissioner further took the view that the question of observance of data protection standards by the US was foreclosed by the Safe Harbour Decision of the European Commission.
24. The High Court, having rejected the *locus standi* objection, found that the Commissioner has "*demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision*" and stressed that neither the validity of Directive 95/46/EC nor the Safe Harbour Decision have been challenged. According to the referring court, Article 3 (1) (b) of the Safe Harbour Decision was not applicable to the case as the complaint was not directed to the *conduct* of Facebook itself.<sup>2</sup> The referring court's questions and doubts about the approach taken by the Commissioner stem from developments that have taken place in the 14 years since the adoption of the Safe Harbour Decision, namely technological advancements, the Snowden revelations and, since 2009, the binding nature of the Charter of Fundamental Rights of the European Union, in particular Articles 7, 8 and 47.
25. Furthermore, the referring court stated that "if the matter were to be judged solely by reference to Irish constitutional law standards, the Commissioner could not properly have exercised his s. 10(1)(a) powers to conclude in a summary fashion that there was nothing further to investigate".<sup>3</sup> As noted by the referring court, under Irish national law, "the accessing of private communications by the State authorities through interception or surveillance engages the constitutional right to privacy. Further, accessing by State authorities of private communications generated within the home [...] is also a clear interference with the inviolability of the dwelling as guaranteed by Article 40.5 of the

---

<sup>2</sup> See paragraph 19 of the request for a preliminary ruling.

<sup>3</sup> See paragraph 15 of the request for a preliminary ruling.

Constitution".<sup>4</sup> However, as the matter concerned was covered by EU legislation and Irish law thus precluded, the referring court decided to submit a request for a preliminary ruling to the CJEU.

26. The High Court consequently stayed its proceedings and referred the following questions for a preliminary ruling:

"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 subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may and/or must the once holder conduct his or her own investigation of the matter in the light of actual developments in the meantime since that Commission Decision was first published?"

#### **4. THE REACTION OF THE EUROPEAN COMMISSION TO THE SNOWDEN ALLEGATIONS**

27. Since June 2013, the existence of a number of US surveillance programmes involving the large-scale collection and processing of personal data has been revealed. The programmes concern in particular the collection of personal data from US internet and telecommunication service providers and the monitoring of data flows inside and outside the US. Given the central position of these US companies in the EU market, the transatlantic routing of a large part of electronic data flows and communications, and the volume of electronic data flows across the Atlantic, a very significant number of

---

<sup>4</sup> Paragraph 9 of the request for a preliminary ruling.

individuals in the EU, and most likely all users of the internet in Europe, may be affected by these programmes.

28. Following these revelations, the Commission immediately expressed serious concerns and requested clarifications from the US both orally and in writing regarding the impact of these programmes on the fundamental rights of individuals in the EU, specifically their right to privacy and to the protection of personal data. In particular, an ad hoc EU-US working group on data protection<sup>5</sup> was set up in July 2013 to establish the facts surrounding the revelations. A report of the Working Group was published on 27 November 2013 (ANNEX 1).<sup>6</sup> The US confirmed that it is under Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) that the National Security Agency (NSA) maintains a database known as PRISM which allows collection of electronically stored data.<sup>7</sup> The US also confirmed that Section 702 provides the legal basis for the so-called "upstream collection"; this is understood to be the interception of Internet communications by the NSA as they transit to or through the US (e.g. through cables, at transmission points). The US further confirmed that Executive Order 12333 is another legal basis for other surveillance programmes for the broad mass collection of data from the internet and is the general framework on intelligence gathering inside and outside the US.<sup>8</sup>
29. On the same day, the Commission issued two communications which respectively assessed the functioning of the Safe Harbour (ANNEX 2)<sup>9</sup> and set out a series of action to

---

<sup>5</sup> The group was co-chaired by the Commission and the Presidency of the Council and with, inter alia, the participation of the EEAS, Member States' experts and representatives of the relevant US government authorities.

<sup>6</sup> Report of the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection: <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>

<sup>7</sup> See section 2.1.1 of the Report of the EU-US ad hoc High Level Working Group. PRISM allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube.

<sup>8</sup> See section 2.3 of the Report of the EU-US ad hoc High Level Working Group.

<sup>9</sup> 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, 27.11.2013.

be taken in order to restore trust in data flows between the EU and the US (ANNEX 3)<sup>10</sup>. The Communication on the Functioning of Safe Harbour identified 13 recommendations, addressed to the US, aimed at strengthening the Safe Harbour framework in light of developments that have taken place since its adoption. Recommendations 1-11 address basic obligations of the Safe Harbour framework and fall into three categories: transparency, redress and enforcement. Recommendations 12 and 13 relate to the need to address the question of access by US authorities to Safe Harbour data for national security purposes, in particular in the context of the national security exemption contained in the current Safe Harbour framework. Number 12 states: *"Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements."* Number 13 states: *"It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate"*.<sup>11</sup>

30. In its Communication on rebuilding trust in EU-US data flows, the Commission outlined three policy options vis-à-vis the Safe Harbour: maintaining the status quo, strengthening the Safe Harbour scheme and reviewing its functioning thoroughly and suspending or revoking the Safe Harbour decision. The Commission is currently actively engaged with the US government authorities to discuss the implementation by the US of the 13 recommendations set out in the Communication. Given the sensitivity and complexity of the issues at hand, discussions are ongoing.

---

<sup>10</sup> Communication from the Commission to the European Parliament and the Council, "Rebuilding Trust in EU-US Data Flows", COM(2013) 846, 27.11.2013. The main measures of the package are: (1) a swift adoption of the EU's data protection reform; (2) making Safe Harbour safe; (3) strengthening data protection safeguards in the law enforcement area (umbrella agreement); (4) using existing Mutual Legal Assistance and sectoral agreements to obtain data; (5) addressing European concerns in the on-going U.S. reform process on intelligence gathering activities; and (6) promoting privacy standards internationally.

<sup>11</sup> COM(2013) 847, p. 18.



## 5. LEGAL ANALYSIS

### 5.1. General Observations

31. In accordance with Article 25 (6), last subparagraph, of Directive 95/46/EC, adequacy decisions are in principle binding on all Member States. Article 3 (1) (b) of the Safe Harbour Decision allows national data protection authorities under certain conditions to suspend data flows to the US. This provision is an exception to the uniform application of the Commission's adequacy decision and therefore, in principle, must be interpreted restrictively. At the same time, it has to be interpreted in the light of the Charter, especially of Articles 7 and 8 thereof.
32. Moreover, in the interpretation of Article 3 (1) (b), it is important to take into account the relationship of the respective powers of the Commission and of the national data protection authorities. In particular, as will be explained in more detail below, the competences of the national data protection authorities are focused on the application of data protection law in individual cases whereas the general review of the application of the Safe Harbour Decision including any decisions as regards its suspension or termination fall under the competences of the Commission.

### 5.2. The conditions of Article 3 (1) (b) of the Safe Harbour Decision are only partly met

33. Pursuant to Article 3 (1) (b) of the Safe Harbour Decision, there are four cumulative conditions under which the DPAs can decide to suspend specific data flows:

5.2.1. *First condition:* There is a substantial likelihood that the Principles are being violated

34. In the Commission's view, a substantial likelihood that the Safe Harbour Principles have been violated does exist. The very large-scale and indiscriminate nature of the US mass-surveillance programmes is namely incompatible with the strictly tailored national security exemption in the Safe Harbour Principles as set out in the fourth paragraph of the preamble to the Privacy Principles.
35. This conclusion follows from an interpretation of the Safe Harbour Decision in the light of the Charter of Fundamental Rights and the relevant case law of the Court. According to Article 52(1) of the Charter, "*any limitation on the exercise of the rights and freedoms*

*recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."* Equally, under the European Convention on Human Rights *"there shall be no interference by a public authority with the exercise of the right"* to respect for private and family life, which includes the right to data protection, *"except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"* (Article 8 (2) thereof). According to the case law of the Court on the right to respect for private life:

*"(...) the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".<sup>12</sup>*

36. Consequently, the Safe Harbour Decision which specifies that such limitations are allowed only *"to the extent necessary"* to meet national security, public interest, or law enforcement requirements, must be interpreted *strictly*.

37. As the Court has repeatedly held, the exception foreseen in Article 4 (2) TEU, according to which national security remains the sole responsibility of each Member States, cannot lead to setting aside EU law (cf. Case C-300/11, *ZZ v. Secretary of State for the Home Department*, para. 38<sup>13</sup>). Furthermore, the Court also held that the limits of Article 52 (1) of the Charter of Fundamental Rights apply also in this area of law; see, for instance paragraphs 49 and 51 in Case C-300/11, *ZZ v. Secretary of State for the Home Department*:

*"It is only by way of derogation that Article 30(2) of Directive 2004/38 permits the Member States to limit the information sent to the person concerned in the interests of*

---

<sup>12</sup> See Case C-293/12, *Digital Rights Ireland*, EU:C:2014:238, paragraph 52.

<sup>13</sup> EU:C:2013:363.



*State security. As a derogation from the rule set out in the preceding paragraph of the present judgment, this provision must be interpreted strictly, but without depriving it of its effectiveness. [...] In particular, it should be taken into account that, whilst Article 52(1) of the Charter admittedly allows limitations on the exercise of the rights enshrined by the Charter, it nevertheless lays down that any limitation must in particular respect the essence of the fundamental right in question and requires, in addition, that, subject to the principle of proportionality, the limitation must be necessary and genuinely meet objectives of general interest recognised by the European Union".*

38. This reasoning holds all the more true, as the present case concerns the use of a national security exemption for the benefit of a *third country*, here the U.S., which is contained in a decision of the European Commission. The present case therefore does not concern the responsibilities of Member States in the maintenance of their national security.
39. Of relevance in this context is moreover the Court's judgment in Case C-293/12, *Digital Rights Ireland*, where it held in paragraph 37:

*"It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance. "*

40. Furthermore, by way of analogy in the specific context of criminal law enforcement the CJEU held in the same judgment, para. 51, that the:

*"fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight."*

41. Against this background the Court considered that there was a manifest violation of the principle of proportionality and consequently an unlawful interference with the right to personal data protection insofar as:

a) the retention of personal data affected, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions (para. 58);

b) Directive 2006/24 did not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it was not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences (para. 59).

c) Not only there was a general absence of limits in Directive 2006/24 but also of any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference (para. 60).

42. The Snowden revelations on mass surveillance (the veracity and seriousness of which the referring Court has acknowledged), the publication in the press of a series of official documents, including classified documents, a number of which were subsequently declassified and made public by the US government, as well as the findings of the EU-US Ad Hoc High Level Working Group point to a scale of mass surveillance that, in the words of the referring court itself *"demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens [whose] data protection rights have been seriously compromised by*

*mass and largely unsupervised surveillance programmes*".<sup>14</sup> The surveillance programmes do not contain any limitations either with regard to the persons concerned or the type of personal data collected. The large-scale nature of the surveillance programmes may thus indeed result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbour Decision.

43. Furthermore, Facebook is self-certified under Safe Harbour and implicated in the PRISM programme.<sup>15</sup> In this context, contrary to the views of the referring court,<sup>16</sup> it is irrelevant whether Facebook Inc. itself has (directly or knowingly) violated the Principles. From the point of view of the protection of EU data subjects' rights it is only relevant whether the level of protection that an adequacy finding is meant to guarantee has been undermined regardless of the fact of whether this is the result of an action by a company or by a public authority.
44. In light of these facts, it must be established that there is a substantial likelihood that adherence to the Safe Harbour Privacy Principles have been limited in a way that fails to comply with the strictly tailored national security exemption. The revelations in question point to a level of surveillance of a massive and indiscriminate scale incompatible with the standard of necessity laid down in that exemption as well as, more generally, with the right to personal data protection as enshrined in Article 8 of the Charter.
45. Accordingly, in light of the above and the nature and extent of the surveillance programmes at issue, there is a substantial likelihood that the Principles laid down in the Safe Harbour Decision have been violated under circumstances such as in the main proceedings.

---

<sup>14</sup> Judgment of the High Court of 18<sup>th</sup> June, 2014, *Schrems v. Data Protection Commissioner* [2014] IECCA 68, point 8.

<sup>15</sup> See section 2.1.1 of the Report of the EU-US ad hoc High Level Working Group. PRISM allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube: <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

5.2.2. *Second condition:* There is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue

46. According to the second condition of Article 3 (1) (b) of the Safe Harbour Decision, there must be a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue.

47. The enforcement of the Safe Harbour framework rests primarily with the US Federal Trade Commission. However, the enforcement mechanism of the Safe Harbour has no authority to intervene as regards surveillance programmes in general and in particular on the question whether the necessity condition of the exemption is complied with. The scope of the surveillance programmes and the conditions under which they operate are fixed by the US national security agencies under the control of the Director of National Intelligence and only some programmes are subject to the judicial oversight of the US Foreign Intelligence Surveillance Court (FISC). It is worth recalling that the FISC proceedings are non-adversarial and there is no representation before the Court of the interests of the data subject during the consideration of an application for an order.<sup>17</sup> It follows from the above that the enforcement mechanism is not able to take adequate and timely steps to settle the possible surveillance under the surveillance programmes by US national security agencies of the complainant's personal data in Facebook.

48. Accordingly, there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue under circumstances such as in the main proceedings.

5.2.3. *Third condition:* The continuing transfer would create an imminent risk of grave harm to data subjects

49. According to the third condition of Article 3 (1) (b) of the Safe Harbour Decision, the continuing transfer of personal data has to create an imminent risk of grave harm to data subjects.

---

<sup>16</sup> Cf. above para. 23.

<sup>17</sup> See the Report of the EU-US Ad hoc Working Group on Data Protection (section 4.3).

50. When interpreting this condition, the general observations on the interpretation of Article 3 (1) (b) as set out above have to be kept in mind. Being an exception to the uniform application of the Commission's adequacy decision, this provision, in principle, has to be interpreted restrictively. Moreover, as already noted, in the interpretation of Article 3 (1) (b), it is important to take into account the relationship of the respective powers of the Commission and of the national data protection authorities. In particular, the competences of the national data protection authorities are focused on the application of data protection law in individual cases whereas the general review of the application of the Safe Harbour Decision including any decisions as regards its suspension or termination fall under the competences of the Commission. This means in particular that the conditions set out in Article 3 (1) (b) have to be fulfilled in the specific circumstances at hand, as recital 8 of the Safe Harbour Decision ("*suspension of specific data flows*").
51. In this regard, it must be underlined that "grave harm" indicates a higher level of damage or prejudice than the mere violation of the right to the protection of personal data. The language rather points to a qualified prejudice. Also, a systematic reading with the first condition shows that a mere violation of the right to the protection of personal data would not suffice since otherwise the third condition would become largely redundant.
52. Moreover, whether an imminent risk of such grave harm exists has to be assessed on the basis of the concrete situation of the complainant(s). As set out above, the conditions of Article 3 (1) (b) have to be met in the specific case at hand. However, the complainant has not brought forward any specific arguments which would indicate that there is an imminent risk of grave harm. Rather, due to their generality and abstractness, Mr Schrems' concerns about the surveillance programmes of the US national security agencies are exactly the same as those which have led the Commission to start the review the Safe Harbour Decision. National data protection authorities would encroach upon the Commission's competence to renegotiate the terms of the Safe Harbour Decision with the US or, if necessary, suspend the Decision if they took action based on complaints raising only structural and abstract concerns.

This having been said, the Commission does not exclude that in other specific cases, where an imminent risk of grave harm to complainants is demonstrated, national data protection authorities could take action.

5.2.4. *Fourth condition:* The competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organization with notice and an opportunity to respond

53. As the third condition of Article 3 (1) (b) is not met, there is in principle no need to examine the fourth condition. However, should the Court come to a different result regarding the third condition, the Commission notes that it appears that the Commissioner did discuss the PRISM allegations with Facebook Ireland even before he had received Schrems' complaint and was satisfied with the responses provided including that the company "*had appropriate procedures in place for the handling of access requests received from security agencies generally*" (Appendix 1, submission on behalf of the respondent (Commissioner), point 66). From this, it could be concluded that the fourth condition was fulfilled. However, the Commission notes also that such discussions with the organization involved may not be sufficient to address problems created by the access to personal data by US national security agencies. This also supports the Commission's view that such issues are better addressed through review of the Safe Harbour Decision by the Commission.

### **5.3. No power of the data protection authority to investigate**

54. If, as under circumstances such as in the main proceedings, not all of the cumulative conditions of Article 3 (1) (b) are met, the data protection authority has no power to investigate further a complaint. It is rather bound by the finding of adequacy by the Commission in the Safe Harbour Decision. This having been said, the Commission does not exclude that in other specific cases, where an imminent risk of grave harm to complainants is demonstrated national data protection authorities could take action.

## 6. CONCLUSION


55. In the light of the above observations, the Commission respectfully suggests that the Court should answer the questions referred for a preliminary ruling by the High Court of Ireland as follows:

Under circumstances such as in the main proceedings, the data protection authority is bound by the finding of adequacy by the European Commission in Decision 2000/520/EC (Safe Harbour Decision).

Ben Smulders

Bernd Martenczuk

*Agents for the Commission*

  
Julie Vondung



## **Schedule of Annexes**

### Annex 1:

Report of the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 27.11.2013, referred to in paragraph 28 of the observations.

### Annex 2:

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, 27.11.2013, referred to in paragraph 29 of the observations.

### Annex 3:

Communication from the Commission to the European Parliament and the Council, "Rebuilding Trust in EU-US Data Flows", COM(2013) 846, 27.11.2013, referred to in paragraphs 29 and 30 of the observations.