THE HIGH COURT
COMMERCIAL

[2016 No. 4809 P.]

BETWEEN

THE DATA PROTECTION COMMISSIONER

PLAINTIFF

AND

FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

DEFENDANTS

JUDGMENT of Ms. Justice Costello delivered on the 3rd day of October, 2017

Introduction

1. This is an unusual case. The proceedings have been brought in this court for the purposes of obtaining a ruling from the Court of Justice of the European Union ("the CJEU") on the validity of three decisions of the Commission of the European Union ("the Commission") insofar as they apply to data transfers from the European Economic Area ("the EEA") to the United States of America. The decisions are:

(1) *Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19;*

(2) *Commission Decision 2004/915/EC of 27 December 2004 amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004)5271) [2004] OJ L385/74; and*

(3) *Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C (2010) 593) (Text with EEA relevance) [2010] OJ L39/5* (together the "SCC decisions")

2. The plaintiff is the Data Protection Commissioner in Ireland ("the DPC"). She is the person charged with the enforcement and monitoring of compliance with the Data Protection Acts 1988 to 2003. She is also the person designated as the national supervisory authority for the purposes of monitoring the application in Ireland of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Directive").

3. The DPC is investigating a complaint made by the second named defendant (Mr. Schrems), a student with an address at Schadegasse 2/13, 1060 Vienna, Austria who operates a Facebook account. She has formed the view that the complaint raises issues as to the validity of the SCC decisions having regard to the provisions of Article 7 and/or Article 8 and/or Article 47 of the Charter of Fundamental Rights of the European Union ("the Charter"). In light of the Ruling of the CJEU in Case C-362/14 *Schrems v. Data Protection Commissioner*, EU:C:2015:650 *"Schrems")* 6th October, 2015, and in particular para. 65 of the Ruling she instituted these proceedings in order that the validity of the SCC decisions may be determined, either by this court declining to make a reference pursuant to Article 267 of the Treaty on the Functioning of the European Union ("TFEU") on the basis that no issue as to the validity of the SCC

decisions arises, or on the basis that this court makes a reference to the CJEU and the CJEU makes a ruling on the validity of the SCC decisions.

The Parties

4. The DPC joined Mr. Schrems as a defendant to the proceedings as he is the complainant whose complaint she is investigating and which gives rise to these proceedings. Facebook Ireland Ltd ("Facebook") is a limited liability company which operates an online social networking service, with a registered address at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2. It is part of the Facebook group of companies. Facebook Inc. is a US corporation, established under the laws of the State of Delaware and having its principal place of business at Menlo Park, California. It is the ultimate parent of the Facebook group of companies. Facebook is joined as a defendant to these proceedings as Mr. Schrems' complaint relates to the transfer of his data by Facebook to Facebook Inc. in the United States for processing. The DPC seeks no relief against either party. She joined them as defendants as they were the parties most concerned with the issues in order that they might engage fully in the proceedings. They have each done so.

5. The case raises issues of very major, indeed fundamental, concern to millions of people within the European Union and beyond. Firstly, it is relevant to the data protection rights of millions of residents of the European Union. Secondly, it has implications for billions of euros worth of trade between the EU and the US and, potentially, the EU and other non-EU countries. It also has potentially extremely significant implications for the safety and security of residents within the European Union. There is considerable interest in the outcome of these proceedings by any parties having a very real interest in the issues at stake.

6. Applications were made by a number of parties to be joined or heard in the proceedings. In the event four parties were joined as *amici curiae* to the proceedings. These were the United States of America, the Business Software Alliance (BSA), Digital Europe and the Electronic Privacy Information Centre (EPIC). Each of these parties made submissions at the hearing but were not permitted to adduce evidence before the court.

Legal Framework

The Charter of Fundamental Rights of the European Union ("the Charter")

Article 7

Respect for private and family life

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

Article 8

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.

Article 47

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.

Article 51

Field of application

1. *The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.*

2. *This Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties*

Article 52

Scope and interpretation of rights and principles

1. 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....

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

The Treaty on the functioning of the European Union (2012/C326/47) ("the TFEU")

Article 16

(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Article 267

(ex Article 234 TEC)

The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning:

(a) the interpretation of the Treaties;

(b) the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union;

Where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the Court to give a ruling thereon…..

Treaty on the European Union (2012/C326/13) ("TEU")

Article 4

1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.

2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

3. Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties….

Article 5

(ex Article 5 TEC)

1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality.

2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.

3. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level….

The Directive

Recitals

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any

lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-

mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation

by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

Articles

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic

means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

Article 25

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.

Article 26

Derogations

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.

2. Without prejudice to paragraph 1, a Member State may authorize 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), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

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

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim….

The European Convention on Human Rights ("the Convention")

Article 8

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right 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.

The Data Protection Act 1988-2003

10.(1) (a) The Commissioner may investigate, or cause to be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of opinion that there may be such a contravention.

(b) Where a complaint is made to the Commissioner under paragraph (a) of this subsection, the Commissioner shall—

(i) investigate the complaint or cause it to be investigated, unless he is of opinion that it is frivolous or vexatious, and

(ii) if he or she is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.

(1A) The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof.

(2) If the Commissioner is of opinion that a person has contravened or is contravening a provision of this Act (other than a provision the contravention of which is an offence), the Commissioner may, by notice in writing (referred to in this Act as an enforcement notice) served on the person, require him to take such steps as are specified in the notice within such time as may be so specified to comply with the provision concerned.

(3) Without prejudice to the generality of subsection (2) of this section, if the Commissioner is of opinion that a data controller has contravened section 2 (1) of this Act, the relevant enforcement notice may require him—

(a) to block, rectify, erase or destroy any of the data concerned, or

(b) to supplement the data with such statement relating to the matters dealt with by them as the Commissioner may approve of; and as respects data that are inaccurate or not kept up to date, if he supplements them as aforesaid, he shall be deemed not to be in contravention of paragraph (b) of the said section 2 (1).

(4) An enforcement notice shall—

(a) specify any provision of this Act that, in the opinion of the Commissioner, has been or is being contravened and the reasons for his having formed that opinion, and

(b) subject to subsection (6) of this section, state that the person concerned may appeal to the Court under section 26 of this Act against the requirement specified in the notice within 21 days from the service of the notice on him.

(5) Subject to subsection (6) of this section, the time specified in an enforcement notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of 21 days specified in subsection (4) (b) of this section and, if an appeal is brought against the requirement, the requirement need not be

complied with and subsection (9) of this section shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(6) If the Commissioner—

(a) by reason of special circumstances, is of opinion that a requirement specified in an enforcement notice should be complied with urgently, and

(b) includes a statement to that effect in the notice,

subsections (4) (b) and (5) of this section shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of section 26 (other than subsection (3)) of this Act and shall not require compliance with the requirement before the end of the period of 7 days beginning on the date on which the notice is served.

(7) On compliance by a data controller with a requirement under subsection (3) of this section, he shall, as soon as may be and in any event not more than 40 days after such compliance, notify—

(a) the data subject concerned, and

(b) if such compliance materially modifies the data concerned, any person to whom the data were disclosed during the period beginning 12 months before the date of the service of the enforcement notice concerned and ending immediately before such compliance unless such notification proves impossible or involves a disproportionate effort, of the blocking, rectification, erasure, destruction or statement concerned.

(8) The Commissioner may cancel an enforcement notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(9) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence.

Annotations

11.—(1) The transfer of personal data to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer and, in particular, but without prejudice to the generality of the foregoing, to—

(a) the nature of the data,

(b) the purposes for which and the period during which the data are intended to be processed,

(c) the country or territory of origin of the information contained in the data,

(d) the country or territory of final destination of that information,

(e) the law in force in the country or territory referred to in paragraph (d),

(f) any relevant codes of conduct or other rules which are enforceable in that country or territory,

(g) any security measures taken in respect of the data in that country or territory, and

(h) the international obligations of that country or territory.

(2) (a) Where in any proceedings under this Act a question arises—

(i) whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred, and

(ii) a Community finding has been made in relation to transfers of the kind in question,

the question shall be determined in accordance with that finding.

(b) In paragraph (a) of this subsection 'Community finding' means a finding of

the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area.

(3) The Commissioner shall inform the Commission and the supervisory authorities of the other Member States of any case where he or she considers that a country or territory outside the European Economic Area does not ensure the adequate level of protection referred to in subsection (1) of this section.

(4) (a) This section shall not apply to a transfer of data if—

(i) the transfer of the data or the information constituting the data is required or authorised by or under—

(I) any enactment, or

(II) any convention or other instrument imposing an international obligation on the State,

(ii) the data subject has given his or her consent to the transfer,

(iii) the transfer is necessary—

(I) for the performance of a contract between the data subject and the data controller, or

(II) for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller,

(iv) the transfer is necessary—

(I) for the conclusion of a contract between the data controller and a person other than the data subject that—

(A) is entered into at the request of the data subject, and

(B) is in the interests of the data subject, or

(II) for the performance of such a contract,

(v) the transfer is necessary for reasons of substantial public interest,

(vi) the transfer is necessary for the purpose of obtaining legal advice or for the purpose of or in connection with legal proceedings or prospective legal proceedings or is otherwise necessary for the purposes of establishing or defending legal rights,

(vii) the transfer is necessary in order to prevent injury or other damage to the health of the data subject or serious loss of or damage to property of the data subject or otherwise to protect his or her vital interests, and informing the data subject of, or seeking his or her consent to, the transfer is likely to damage his or her vital interests,

(viii) the transfer is of part only of the personal data on a register established by or under an enactment, being—

(I) a register intended for consultation by the public, or

(II) a register intended for consultation by persons having a legitimate interest in its subject matter,

and, in the case of a register referred to in clause (II) of this subparagraph, the transfer is made, at the request of, or to, a person referred to in that clause and any conditions to which such consultation is subject are complied with by any person to whom the data are or are to be transferred,

or

(ix) the transfer has been authorised by the Commissioner where the data controller adduces adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals and for the exercise by individuals of their relevant rights

under this Act or the transfer is made on terms of a kind approved by the Commissioner as ensuring such safeguards.

(b) The Commissioner shall inform the European Commission and the supervisory authorities of the other states in the European Economic Area of any authorisation or approval under paragraph (a)(ix) of this subsection.

(c) The Commissioner shall comply with any decision of the European Commission under the procedure laid down in Article 31.2 of the Directive made for the purposes of paragraph 3 or 4 of Article 26 of the Directive.

(5) The Minister may, after consultation with the Commissioner, by regulations specify—

(a) the circumstances in which a transfer of data is to be taken for the purposes of subsection (4)(a)(v) of this section to be necessary for reasons of substantial public interest, and

(b) the circumstances in which such a transfer which is not required by or under an enactment is not to be so taken.

(6) Where, in relation to a transfer of data to a country or territory outside the European Economic Area, a data controller adduces the safeguards for the data subject concerned referred to in subsection (4)(a)(ix) of this section by means of a contract embodying the contractual clauses referred to in paragraph 2 or 4 of Article 26 of the Directive, the data subject shall have the same right—

(a) to enforce a clause of the contract conferring rights on him or her or relating to such rights, and

(b) to compensation or damages for breach of such a clause,

that he or she would have if he or she were a party to the contract.

(7) The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from the State to a place outside the State unless such transfer is required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on the State.

(8) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data.

(9) A prohibition under subsection (7) of this section shall be effected by the service of a notice (referred to in this Act as a prohibition notice) on the person proposing to transfer the data concerned.

(10) A prohibition notice shall—

(a) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned,

(b) specify the time when it is to take effect,

(c) specify the grounds for the prohibition, and

(d) subject to subsection (12) of this section, state that the person concerned may appeal to the Court under section 26 of this Act against the prohibition specified in the notice within 21 days from the service of the notice on him or her…..

Overview of the legislation

7. Article 7 of the Charter provides that everyone has the right to respect for his or her private life, home and communication. This largely reflects Article 8 of the Convention. Article 8 of the Charter confers the right of protection of personal data. This is also protected by Article 16 of TFEU. Article 8 (1) of the Charter provides that

everyone has the right to protection of personal data concerning him or her. Article 8 (2) provides that 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. It provides that everyone has a right of access to data which has been collected concerning him or her and the right to have it rectified. Article 8 (3) provides that compliance with the rules of Article 8 shall be subject to control by an independent authority.

8. Article 47 of the Charter provides that 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 by Article 47. These include a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law.

9. Article 52 recognises that the rights and freedoms recognised by the Charter may be limited but any such limitation must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, the 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.

10. Article 1 of the Directive requires Member States to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data. The Directive is primarily directed towards the processing of personal data and the free movement of such data within the EEA. Chapter IV of the Directive deals with the transfer of personal data outside of the EEA to third countries.

11. Article 25 (1) of the Directive establishes a general rule prohibiting the transfer of personal data outside the EEA unless the country to which the data is transferred "ensures an adequate level of protection" for the data protection rights of those data subjects to whom the transferred data relates. The adequacy of the level of protection available within a third country is to be assessed by reference to criteria set out in Article 25 (2) of the Directive.

12. The Commission is authorised to make a finding to the effect that a specified third country does not ensure an adequate level of protection for the data protection rights of data subjects. Article 25 (6) confers a power on the Commission to make a finding that a particular third country ensures an adequate level of protection so that in principle personal data may be transferred from any EEA member state to that third country. Where the Commission makes a finding pursuant to Article 25 (6) then the Member States are required to take the measures necessary to comply with the Commission's decision.

13. Article 26 permits the transfer of data to third countries which do not ensure an adequate level of protection as they do not satisfy the criteria set out in Article 25. It thus permits transfers to be undertaken even if it is accepted that the third country to which the data is to be transferred does not ensure an adequate level of protection. Article 26 (1) sets out six specific circumstances in which data transfers to a third country may be permissible even though the third country in question does not ensure an adequate level of protection, such as for example whether data subject gives consent to the transfer pursuant to Article 26 (1) (a).

14. Article 26 (2) provides that, without prejudice to Article 26 (1), a Member State may authorise 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)

where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regard the exercise of the corresponding rights. Article 26 (2) specifically states that such safeguards may in particular result from "appropriate contractual clauses".

15. Article 26 (4) of the Directive provides that, in accordance with the procedure referred to in Article 31 (2) of the Directive, the Commission may decide that certain contractual clauses offer sufficient safeguards as required by Article 26 (2). Where the Commission makes a decision in such terms the member states are obliged to take the necessary measures to comply with the Commission's decision.

16. Where the Commission decides that certain contractual clauses provide sufficient safeguards for the protection of individuals' data protection rights pursuant to decisions made under Article 26 (4) and those particular contractual clauses are incorporated into contracts regulating the terms of transfer of personal data to data controllers or data processers established in a third country, such transfers are, in principle, permissible, even if the third country in question does not ensure an adequate level of protection.

17. The Directive was transposed into national law by means of the Data Protection Act 1988 and the Data Protection Amendment Act 2003 (collectively the Data Protection Acts 1988-2003). The DPC is the national supervisory authority in the State for the purposes of the Directive. Section 11 (2) of the Acts provides that where a finding has been made by the Commission to the effect that a third country ensures adequate protection for the data privacy rights of data subjects, that finding is binding in any proceedings under the Acts. Section 11 (4) (c) of the Acts provides that where the Commission has adopted a decision approving particular standard contractual

clauses as fulfilling the requirements of Article 26 (4) of the Directive, the DPC shall comply with that decision.

The Factual Background

18. On the 26th of July, 2000, the Commission adopted Decision 2000/520/EC of 26th July, 2000, pursuant to the Directive on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the United States Department of Commerce ("the Safe Harbour Decision") establishing the so called "Safe Harbour" arrangements for data transfers from the EU to the U.S. The Safe Harbour Decision did not identify the U.S. as a third country recognised as ensuring "an adequate level of protection" for the purposes of Article 25 (6) of the Directive. It provided that EU-US transfers were permissible under the terms of the Safe Harbour Decision provided the entity to whom the data was being transferred self certified that it complied with (1) the Safe Harbour privacy principles; and (2) a set of "frequently asked questions", both published by the U.S. Department of Commerce and incorporated into the Safe Harbour Decision at Annexes 1 and 2.

19. Since the adoption of the Safe Harbour Decision, the importance of transfers of data from the EU to the US increased substantially reflecting exponential growth in the volume of EU-US data transfers generated by business undertakings of all sizes and all industry sectors and by the general explosion in the volume of data created by modern technology and the increasing importance of data transfers globally. The Safe Harbour Decision became an important mechanism by which certain data controllers established in the EU sought to transfer data to the US for processing. Due to the history of the evolution of the Internet, much of the processing of data occurs in companies established in the US.

20. In June, 2013 Mr. Edward Snowden, a contractor engaged through a private company working for the United States National Security Agency ("NSA") disclosed documents said to reveal the existence of one or more programmes operated by the NSA under which internet and telecommunications systems operated by some of the world's largest technology companies including, by way of example, Microsoft, Apple, Facebook and others, were the subject of surveillance programmes.

21. On the 25th of June, 2013, Mr. Schrems filed a complaint with the DPC in relation to the processing of his personal data by Facebook. He contended that in the light of Mr. Snowden's disclosures, the transfer of his personal data by Facebook to its US parent, Facebook Inc. for processing was unlawful both under national and EU law.

22. The DPC took the view that as the Commission had adopted the Safe Harbour Decision establishing and/or endorsing the Safe Harbour arrangements, the DPC was bound to accept the Safe Harbour Decision as binding upon him in light of Article 25 (6) of the Directive and s. 11 (2) of the Acts. On that basis, the DPC declined to investigate Mr. Schrems' complaint, deeming it unsustainable in law.[1]

23. Mr. Schrems instituted judicial review proceedings on the 21st of October, 2013, seeking orders to quash the DPC's refusal to investigate his complaint and directing the DPC to investigate and decide his complaint on its merits.

24. On the 18th of June, 2014, the High Court (Hogan J.) held that it would be appropriate to refer a number of questions to the CJEU so that the CJEU could in turn determine, in particular, whether the DPC was bound absolutely by the Safe Harbour Decision having regard to Articles 7, 8 and 47 of the Charter notwithstanding the provisions of Article 25 (6) of the Directive. The court considered that a reference was

[1] The plaintiff's predecessor

necessary in circumstances where the essence of the complaint concerned the terms of the Safe Harbour Decision rather than the manner in which the DPC had applied it.

25. The CJEU delivered its ruling on the reference on the 6th of October, 2015. The court held that: -

> (1) While noting that the CJEU alone has jurisdiction to declare an EU act invalid, and that, until such time as the Safe Harbour Decision was declared invalid by the CJEU, the [DPC] was not at liberty to adopt any measure contrary to its terms, the CJEU nonetheless found that, as a matter of EU law, the Safe Harbour Decision did not preclude the conduct of an investigation into the EU-US data transfers by the [DPC] so that the [DPC] ought properly to have investigated Mr Schrems' complaint with all due diligence.
>
> (2)Where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25 (6) of the Directive lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.
>
> (3) In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second sub paragraph of Article 28 (3) of the Directive read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such decision adversely affecting him before the

national courts. The national courts must stay proceedings and make a reference to the CJEU for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion, are well founded.

(4) In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first paragraph of Article 28 (3) of the Directive read in the light in particular of Article 8 (3) of the Charter, be able to engage in legal proceedings.

(5) It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

(6) The Safe Harbour Decision of the Commission was invalid.

Thus, data could no longer lawfully be transferred from the EU to the US pursuant to the Safe Harbour Decision.

26. After the ruling of the CJEU the judicial review proceedings came back before the High Court. On the 20th of October, 2015, the High Court made an Order quashing the decision of the DPC to refuse to investigate Mr. Schrems' complaint and remitted the complaint back to the DPC for investigation.

27. Following the ruling in *Schrems* and the determination of the judicial review proceedings, the DPC commenced an investigation into Mr. Schrems' complaint. Mr. Schrems was invited to reformulate his complaint as it was no longer appropriate to focus upon the Safe Harbour Decision which had been declared invalid. The DPC informed Facebook that it had commenced an investigation into Mr. Schrems' complaint regarding the transfer of his personal data by Facebook to Facebook Inc.

Mr. Schrems' Reformulated Complaint

28. Mr. Schrems states that Facebook forwards his personal data to Facebook Inc. in the United States of America where his data is processed. Facebook Inc. is subject to a number of known and secret laws, rules, court decisions and executive orders that oblige it to make his personal data available and/or oblige it to disclose it to US authorities, such as, for example, the National Security Agency (NSA) and the Federal Bureau of Investigations (FBI). He alleges that U.S. law targets data rather than people and that there is no judicial remedy that would allow the data subject to take appropriate action. He complains that non-US persons are not covered by constitutional protections in the United States. He says that Facebook Inc. is subject to "gag orders" that order it to deny and/or not to disclose any facts about government surveillance systems to which it is subject. He says that the United States authorities have access to data held by Facebook Inc., among other U.S. based companies. He states that there is clear evidence that leads him to believe that his personal data controlled by Facebook and processed by Facebook Inc. is at the very least "made available" to US government authorities under various known and unknown legal provisions and spy programmes such as the "PRISM" programme (which I explain more fully below). He also believes that there is a likelihood that his personal data has, in addition, been accessed under these provisions as he was prevented from boarding a

transatlantic flight on the 16th of March, 2012, to the United States for reasons of "national security".

29. He states that under Article 2 (b) of the Directive making data available is a form of processing so that even if his personal data is never accessed by any US government agency, the mere fact that Facebook Inc. is obliged to make this data available to various government agencies in accordance with US law engages the provisions not only of the Directive but also of Article 8 of the Charter.

30. His complaint relates to two operations: firstly, the transfer and/or disclosure of his personal data from Facebook to Facebook Inc and secondly the subsequent processing. He says that "the operation of the "mass surveillance" systems in the United States is therefore only a secondary matter that has to be taken into account when assessing the legality of the relevant processing operation – which is the transfer from "Facebook Ireland Ltd" to "Facebook Inc.". He makes no complaint about the manner in which Facebook Inc. processes his data if it is in compliance with the SCCs.

31. In order to reformulate his complaint Mr. Schrems' solicitors wrote to Facebook on 12th October, 2015, requesting that it identify all legal bases upon which it relies to transfer Mr. Schrems' data to the US. In reply on the 27th of November, 2015, Facebook did not identify all such legal bases. It referred to a data transfer and processing agreement between Facebook and Facebook Inc. effective as of 20th November, 2015, (7 days earlier) and relies upon the standard contractual clauses decision of the Commission 2010/87/EU (one of the three SCC decisions). The agreement of the 20th of November, 2015, refers to other intragroup agreements in the Facebook group of companies and to the Data Hosting Services Agreement between Facebook and Facebook Inc. dated September 15, 2010. These agreements have not been disclosed. Mr. Schrems therefore argues that *if* these agreements alter the annex

to the agreement of November, 2015 (which incorporates the standard contractual clauses) in any way then Facebook is not entitled to transfer data pursuant to Commission decision 2010/87/EU. In addition he points out that the agreement of November 2015 does not cover all processing operations by Facebook Inc. and it does not include the necessary arrangements with subprocessers.

32. As a result, he says that the DPC is not bound by Decision 2010/87/EU pursuant to the provisions of Article 26 (4) of the Directive or s. 11 (2) of the Data Protection Acts as Facebook in fact is not transferring his data to Facebook Inc. pursuant to that decision.

33. He then says: -

> "*Even if the current and all previous agreements between 'Facebook Ireland Ltd' and 'Facebook Inc.' would not suffer from the countless formal insuffiencies above and would be binding on the DPC (which it is not), 'Facebook Ireland Ltd' could still not rely on them in the given situation of factual 'mass surveillance' and applicable US law that violate Article 7, 8 and 47 of the [Charter] (as CJEU has held) and the Irish Constitution (as the Irish High Court has held).*
>
> *Article 4 (1) of Decision 2010/87/EU (as all other relevant Decisions) takes account of a situation where national laws of a third country override these clauses and allows [data protection authorities] to suspend data flows in the situation."*

He argues that the PRISM programme violates the essence of Article 7 and 47 of the Charter and that this was established by the CJEU in the decision in *Schrems* and is binding on the DPC. He therefore requests the DPC to issue a prohibition notice under s. 11 (7) to (15) of the Data Protection Acts, an enforcement notice under s. 10 (2) to

(9) and to take any other appropriate steps to suspend all data flows from Facebook to Facebook Inc.

The DPC's Investigation

34. The DPC examined Mr. Schrems' reformulated complaint as it related to interferences on national security grounds with his data privacy rights by governmental agencies in the United States. She examined whether, by reference to the adequacy criteria identified in Article 25 (2) of the Directive, the US ensures adequate protection for the data protection rights of EU citizens and if and to the extent that the US does not ensure adequate protection, whether it is open to Facebook to rely on one or more of the derogations provided for in Article 26 of the Directive to legitimise the transfer of subscribers' personal data to the US, if indeed, such transfers continued to take place.

35. Her investigation proceeded on two distinct strands. Strand 1 comprised a factual investigation focused on establishing whether Facebook continued to transfer personal data to the US subsequent to the decision of the CJEU of 6th October, 2015, in *Schrems*. Facebook acknowledged that it continues to transfer personal data relating to Facebook's subscribers resident in the European Union to its US established parent and that it does so, in large part, on the basis that it has adopted the standard contractual clauses set out in the annexes to the SCC decision 2010/87/EU. It therefore argues that it ensures adequate safeguards for the purposes of Article 26 (2) of the Directive with respect to the protection of the privacy and fundamental rights and freedoms of EU resident subscribers to the Facebook platform and as regards the exercise by such subscribers of their corresponding rights.

36. In Strand 2 of her investigation DPC has sought to examine whether, by reference to the adequacy criteria identified in Article 25 (2) of the Directive, the US

ensures adequate protection for the data protection rights of EU citizens. If it does not, she enquired whether the SCC decisions in fact offer adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of their corresponding rights.

37. The DPC engaged in a review of the remedies available for breach of data protection rights in US federal law. She says there appears to be well-founded objections that there are both specific and general deficiencies in the remedial mechanisms available under US law for those EU citizens whose data is transferred to the US. From a specific perspective, the remedies provided by US law are fragmented and subject to limitations that impact on their effectiveness to a material extent.

38. She says that further, the available remedies arise only in particular factual circumstances, and are not sufficiently broad and scoped to guarantee a remedy in every situation in which there has been an interference with the personal data of an EU data subject contrary to Articles 7 and 8 of the Charter. To that extent, the remedies are not complete.

39. From a more general perspective, the requirements of US law in relation to standing in respect of US federal courts operate as a constraint on all forms of relief available.

40. She therefore has formed the view that there appears to be a well-founded objection that there is an absence of an effective remedy in US law compatible with the requirements of Article 47 of the Charter for an EU citizen whose data is transferred to the US where it may be at risk of being accessed and processed by US State agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter. The safeguards purportedly constituted by the standard contractual clauses set in the annexes to the SCC decisions do not appear to address this well-founded

objection that there is an absence of a remedy compatible with Article 47 of the Charter. She is of the opinion that the standard contractual clauses approved by the SCC decisions do no more than establish a right in contract, in favour of data subjects, to a remedy against either or both of the data exporter and importer.[2]

41. She notes that the SCC decisions are not binding on any US government agency or other US public body and they do not so purport. The SCC decisions make no provision whatsoever for a right in favour of data subjects to access an effective remedy in the event that their data is (or may be) the subject of interference by a US public authority, whether acting on national security grounds or otherwise. Thus, in her opinion, the SCC decisions do not address her well-founded concerns that she has identified.

42. In the circumstances, the DPC formed the view that she could not conclude her investigation without obtaining a ruling from the CJEU on the validity of the SCC decisions. In light of the ruling in *Schrems*, she believed that it was appropriate that she would commence these proceedings forthwith so that the substance of the reformulated complaint, and the view reached by the DPC in relation to that portion of the complaint could be examined and determined by a court of competent jurisdiction at the earliest possible opportunity.

What the Case is not About

43. Before considering the arguments of the parties in relation to the central issue whether the court should or should not refer the question of the validity of the SCC decisions to the CJEU for a ruling, it is important to say what this case is **not** about.

44. The case raises issues fundamental to democratic societies and the balance to be achieved in respect of sometimes competing rights, values and duties. It concerns

[2] and subprocessor

the right to data privacy which is recognised as a fundamental right and freedom by the Charter and the TFEU. It also concerns the right, indeed the duty, of the State to protect itself and its citizens from threats to national security, terrorism and serious crime. A degree of surveillance for the purposes of national security, counter-terrorism and combating serious crime is vital for the safeguarding of the freedoms of all citizens of the union. This necessarily involves interference with the right to privacy, including data privacy.

45. A central purpose of the European Union is the promotion of the peace and prosperity of citizens of the European Union through economic and trading activity within the single market and globally. The free transfer of data around the world is now central to economic and social life in the union and elsewhere.

46. The recent history of our continent has shown how crucially important each of these objectives is to the wellbeing of the people of Europe. Damage to the global economy has resulted in very real detriment and hardship to millions of Europeans. International terrorist atrocities have been and continue to be perpetrated in many Member States of the European Union. There are many who experienced the corrosive effects of widespread state surveillance upon their private lives and society in general who regard preservation of the right to privacy, include data protection, as fundamental to a democratic society.

47. In a democratic society, a balance must be struck between these competing concerns, interests and values. Not every State will strike the same balance. One will place a greater emphasis on the right to privacy and one will place a greater emphasis on the requirements of national security. It is important to state that it is not the function of this court to assess, still less resolve, the relative merits of these positions.

48. The Directive with which this judgment is primarily concerned uses the word "adequate" and so this judgment will, of necessity, refer to the adequacy or inadequacy of certain laws or provisions of third countries and in particular of the United States. This does not involve a decision on the respective merits of the choices of the European Union (or its Member States) and the United States. The references to the adequacy or inadequacy of the provisions discussed in this judgment are references to the requirements laid down by the Directive. They do not constitute or reflect value judgments on the regime in the United States relating to data protection and surveillance by government agencies. It is not the function of this court to criticise the laws of a sovereign state, in this case, the United States, or to pronounce on the relative merits of the laws of the United States and the European Union. I do not purport to do so in this judgment.

49. Secondly, this case is not a judicial review of the draft decision of the DPC which she prepared prior to instituting these proceedings and which explains the history of the investigation into Mr. Schrems' complaint and her concerns about the validity of the SCC decisions in light of certain aspects of the law of the United States. The court is concerned with the merits of the arguments advanced by the DPC and the parties to the proceedings. It is not concerned with the process leading to the presentation of the arguments to court. It follows that criticisms levelled at the DPC that she failed to consider certain relevant matters do not invalidate the proceedings. The matters she may not have addressed have been brought before the court by other parties and all of the issues have been extensively argued, including submissions by the United States, with a view to determining whether or not there is merit in the contention that the SCC's decisions may be invalid having regard to the provisions of the Directive and the Charter.

Are EU law and the Charter Engaged?

Facebook's Submissions

50. Facebook argues that this case is concerned with national security. National security issues fall outside the scope of EU law entirely because the treaties reserve competence over national security issues to Member States. It refers to Article 4 (2) of TEU which provides that: -

> *"The Union shall respect [Member States'] … essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."*

51. Facebook submits that EU law does not apply to the processing of personal data for national security purposes regardless of whether the processing takes place in the EU or in third countries such as the United States.

52. It submits that the Directive does not apply to processing for national security purposes. Article 3 (2) of the Directive provides: -

> *"This Directive shall not apply to the processing of personal data:*
>
> *in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law…"*

53. It refers to Recital 13 of the Directive which states: -

> *"... whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters."*

In addition, it refers to Recital 16 which notes that data processing for "*national security*" purposes or "*in the course of state activities relating to the area of criminal law", "does not come within the scope of the Directive."*

54. Facebook points out that a similar exemption in respect of national security applies under national laws. The Directive has been transposed into Irish law by the Data Protection Acts. Section 1 (4) of the Acts provides:

> *"This Act does not apply to-*
>
> *(a) personal data that in the opinion of the Minister or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State…"*

55. Facebook refers to Article 51 (2) of the Charter which provides that the Charter does not extend the field of the application of Union law beyond the powers of the Union. Facebook submits that if it is correct that EU law does not apply to processing for national security purposes, then the Charter is inapplicable by reason of the provisions of Article 51 (2). Facebook submits that as the Directive and the Charter do not apply to Ireland and other EU states when engaged in national security activities, as a corollary, there can be no requirement that the US, when engaging in similar activities, complies with EU data protection law.

56. It relied upon the judgment in jointed cases C-317/04 and C-318/04, *European Parliament v. Council and the Commision* EU:C:2006:356. In that case the European Parliament sought the annulment of a decision of the Council on the conclusion of an agreement between the European Community and the United States of America on the

processing and transfer of passenger name record ("PNR data") by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection ("the CBP") and the annulment of Commission decision on the adequate protection of personal data contained in PNR of air passengers transferred to the CBP. The Commission's decision was adopted pursuant to Article 25 (6) of the Directive. Parliament sought the annulment of the decision of the Commission on the basis that the Directive did not apply to the processing of personal data in the course of an activity outside Union law, in this case, processing operations concerning public security and the activities of the United States in areas of criminal law by reason of the provisions of Article 3 (2) first indent of the Directive.

57. The CJEU noted that the initial processing of data by airlines in handing over the PNR was within the scope of Union law but the decision of the Commission related to the processing by third countries, in this case the United States, and constituted processing regarded as necessary for safeguarding public security and for law enforcement purposes. The court held that the decision of the Commission concerned processing of personal data as referred to in the first indent of Article 3 (2) of the Directive. This meant that the Commission's decision did not fall within the scope of the Directive. Thus, the decision was *ultra vires* the Commission and the court annulled the decision accordingly. The CJEU held that activities within the scope of Article 3 (2) of the Directive are activities of State or State authorities and unrelated to the fields of activity of individuals. The fact that the PNR data was collected by private operators (the airlines) for commercial purposes and it was they who arrange for the transfer of the data to the third country, does not mean that the transfer by the airlines to the United States CBP is thereby outside the scope of Article 3 (2).

58. Facebook's argument is that *Parliament v. The Council and Commission* clearly covers the processing of data with which this case is concerned. Private data is collected by Facebook and transferred by Facebook to Facebook Inc. in the United States. It may then be subject to further processing by the United States intelligence agencies for the purposes of national security. Facebook submits that this brings the transfer within the scope of Article 3 (2) of the Directive and therefore outside the scope of the competence of Union law and, in particular, the scope of the Directive.

The DPC's Submissions

59. The DPC distinguishes *Parliament v. The Council and Commission* from the facts in this case. In that case the private operators (the airlines) transferred all PNR data to the CBP before processing for reasons of public security and the activities of the State in areas of criminal law. There was no other, independent commercial reason for the transfer of the data. This is a crucial distinction. In this case, the transfers are pursuant to the SCC decisions. They are for commercial purposes by definition. In any country, not just the United States, the data could be subject to processing by the national intelligence agencies of the third countries. It cannot be known in advance of the transfer from the EU to the private operator in the third country which, if any, of the data will be subsequently processed for national security purposes by the third country's intelligence agencies. If the argument advanced by Facebook is correct and subsequent processing in a third country by its intelligence agencies for national security purposes takes the processing outside of the scope of the Directive by reasons of the provisions of Article 3 (2) then, logically, all data transferred to third countries potentially falls within the scope of Article 3 (2) of the Directive. In view of the fact that the data cannot be identified in advance, it is impossible to say which data

exported from the EU is entitled to the protections of Articles 25 and 26 and which data falls outside those protections by virtue of the provisions of Article 3 (2).

Discussion

60. If Facebook is correct in its submission that the entire subject matter of the case falls outside the scope of the law of the Union and the Charter, then this disposes of this case, and no reference for a ruling to CJEU should be made, as it would lack competence to rule on the validity of SCC decisions on the grounds advanced as the basis for such alleged invalidity.

61. I do not believe that the submission is correct for the following reasons:

(1) Article 4 (2) of TEU is concerned with the relationship between the European Union and its member states. It is not concerned with the national security of the United States. Therefore this does not assist Facebook in its submission.

(2) The submission is inconsistent with the ruling of the High Court in *Schrems v. The Data Protection Commissioner* [2014] 3 I.R. 75 and the CJEU in *Schrems* where the court proceeded on the basis that it had jurisdiction to rule on the reference. If Facebook's submission in this case is correct, it did not have jurisdiction so to proceed. Eight Member States, the European Parliament, the European Commission and the European Data Protection Supervisor intervened in those proceedings. If Facebook's point was well made, it is remarkable that none of these participants raised this fundamental matter of jurisdiction.

This is particularly so as the issue of the role of national security in the case was considered by Advocate General Bot who observed that *"... there is nothing to suggest that arrangements for the transfer of personal*

data to third countries are excluded from the substantive scope of Article 8 (3) of the Charter...." (Section 72). He considered the fact that the US was processing the data of EU citizens for national security purposes was within the scope of the Charter. At s. 170 he stated that: -

"... any form of processing of personal data is covered by Article 8 of the Charter and constitutes an interference with the right to protection of such data. The access enjoyed by the United States intelligence services to the transferred data therefore also constitutes an interference with the fundamental right to protection of personal data guaranteed in Article 8 of the Charter, since such access constitutes a processing of that data."

(3) The argument is inconsistent with the views of the Article 29 working party. It observed that the fact that national security activities of Member States are excluded from the scope of application of EU law does not mean that EU law ceases to apply. This means that data subject to EU data protection law remains subject to such law when it is accessed by third countries in the name of the national security of such third countries. (Working document on surveillance of electronic communications for intelligence and national security purposes, 5th December, 2014, s. 4.1.2).

(4) This case is concerned with processing consisting in the transfer of data by a private company from a Member State to a private company in a third country. Thereafter, the data may be processed in the third country, the United States, for the purposes of national security, counter-terrorism and the prevention and detection of serious crime. The processing that arises for consideration is not solely the processing of data by the United States in its surveillance activities. Furthermore, the processing concerns

commercial activities. This is not processing concerning public security, defence or state security. The parties to the transfers effected under the SCC decisions are private persons and companies, not State actors. The processing of the data by the United States subsequent to the transfer is unknown and uncertain. At the point of transfer it will not be known which data (if any) will be subject to surveillance. It follows that it cannot be said that the transfers concern public security or are for the purposes of national security. The argument is inconsistent with the case *Tele 2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson & Ors* (joined cases C-203/15 and C-698/15) (hereinafter "*Watson*"). The case concerned the interpretation of Article 15 (1) of the Directive 2002/58/EC (the e-Directive). The legislation under review included measures adopted in Sweden and the United Kingdom for reasons of national security. The CJEU held that the national legislation fell within the scope of the e-Directive, notwithstanding Article 1 (3) of that Directive which excluded from its scope "activities of the state" in specified fields, including activities of the State in areas of criminal law and in the areas of public security, defence and State security, including the economic well being of the State, when the activities relate to state security matters by analogy with the first indent of Article 3 (2) of Directive 95/46. (see paras. 69 and 81)

(5) The argument is also inconsistent with the views of the Commission (and apparently the United States). On the 12th of July, 2016, the Commission adopted Commission Implementing Decision (EU) 2016/1250 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the

adequacy of the protection provided by the EU-US PRIVACY SHIELD ("the Privacy Shield Decision"). The Privacy Shield Decision was adopted pursuant to the Directive and is directly concerned with data transfers to the United States and the potential subsequent processing of the transferred data pursuant to US national security surveillance operations. If the objection of Facebook in relation to national security is correct then it is difficult to understand why both the Commission and the United States engaged in extensive negotiations with the Commission and concluded the Privacy Shield Agreement or why the government of the United States gave the undertakings included in that agreement (as is more fully discussed below). Further, if Facebook is correct, the Privacy Shield Decision must be outside the competence of the Commission and accordingly be invalid. Far from arguing that the Privacy Shield Decision was invalid, Facebook argues, as is more fully set out below, that the decision is valid and binding.

(6) The argument of Facebook would entirely hollow out EU data protection law. If potential unknown, uncertain and ill defined processing of data to achieve the national security objects of a third country can remove a data transfer from the scope of Union law, the entire system of monitoring data transfers falls away and is completely hollowed out. At the point of transfer of data from the member state to the third country, it will not be known which data may be processed by the third country for national security purposes. There can be no way of segregating the data that may ultimately subsequently be processed for national security purposes from the data which will not be scrutinised. On the argument advanced by

Facebook, the transfer of the former data is outside the scope of the Directive, where the latter is not. If the argument were valid, the possibility that data may subsequently be processed for national security purposes by a third country would then suffice to remove all transfers of data outside the EEA from the protection of Union law. It would follow that all of the provisions relating to data transfers to third countries in the Directive would be rendered purposeless if such data transfers fell outside the scope of the Directive based upon the national security surveillance activities of third countries.

Does the Privacy Shield Decision Preclude the Making of a Reference to the CJEU?

62. Member States of the Union are required to ensure that decisions of the institutions of the Union, including the Commission, are complied with within each member state. Article 25 (6) of the Directive provides that member states shall take the measures necessary to comply with an adequacy decision of the Commission adopted in accordance with Article 25. In Ireland this is achieved by s. 11 (2) of the Acts.

63. On the 12th of July, 2016, the Commission adopted the Privacy Shield Decision for the purposes of Article 25 (2) of the Directive.

Facebook's Submissions

64. Facebook submits that the Privacy Shield Decision is a decision of the Commission adopted under the procedure provided for in Article 31 (2) and that it was a finding made for the purposes of Article 25 (6) of the Directive. It argues therefore that the proceedings before this national court were required to be determined in

accordance with that finding on the basis of the provisions of s. 11 (2) of the Acts implementing Article 25 (6) of the Directive. It points out that neither Mr. Schrems nor the DPC challenge the Privacy Shield Decision and that the decision is binding upon the court. A reference to the CJEU in relation to the validity of the SCC decisions on the basis of concerns about the inadequacy of the protections afforded to EU data subjects in respect of interference with their personal data once it has been transferred to the United States, would amount to an impermissible collateral attack on the validity of the Privacy Shield Decision. As the decision is binding upon the national court, it precludes the making of the reference sought by the DPC.

Discussion

65. The submission is predicated upon the argument that the Privacy Shield Decision constitutes an adequacy decision in respect of the United States. The Privacy Shield Decision is a decision that:-

> *"For the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations established in the United States under the EU-U.S. Privacy Shield.*
>
> *The EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on 7 July 2016 as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I, III to VII."*

It is therefore confined to data transferred to organisations in the United States under the EU-US Privacy Shield. This involves companies signing up to detailed principles set out in the Privacy Shield Decision and processing data solely in accordance with those principles.

66. Facebook is not relying on the Privacy Shield Decision to transfer data the subject of this case to Facebook Inc. in the United States. This case is concerned with the transfers of data pursuant to the SCC decisions.

67. Facebook argues that the Privacy Shield Decision is a decision as to the adequacy of the laws and protections of the United States generally for the purposes of Article 25 (2) of the Directive. In my opinion, this characterisation of the decision is incorrect. Only data transferred and processed in accordance with the very detailed provision set out in the Privacy Shield Decision and its Annexes is deemed to be adequately protected. A data controller could not transfer data to the United States in a manner that did not comply with the requirements of the Privacy Shield Decision (including for example, self-certification that it adheres to the principles mandated by the Decision) and claim that such transfer was lawful based upon the provisions of Article 25 (2) of the Directive. In my opinion, it is not permissible to parse a decision of the Commission so as to isolate one element of the decision and then apply that element to a separate decision or decisions of the Commission on the basis that the former decision is binding upon *inter alia* national courts of Member States. It is not a decision that the United States of America affords adequate protection of personal data transferred from the Union to the United States in all circumstances.

68. The difference between the Privacy Shield Decision and a comprehensive Article 25 (2) adequacy decision is illustrated by contrasting it with the adequacy decision in respect of transfers of personal data to the State of Israel of 31 January, 2011 Com. Decision 2011/6//EU (C(2011) 332)

69. Article 1 of that decision provides:-

> *"1. For the purposes of Article 25(2) of Directive 95/46/EC, the State of Israel is considered as providing an adequate level of protection for personal*

data transferred from the European Union in relation to automated international transfers of personal data from the European Union or, where they are not automated, they are subject to further automated processing in the State of Israel.".

70. In 2013 the Commission had expressed concerns in relation to the adequacy of protections afforded to personal data of EU data subjects in the United States in a Communication from the Commission to the European Parliament and Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU COM (2013) 847 Final. In particular it identified concerns it had in relation to individual remedies available in the United States. It identified concerns that EU data subjects did not have avenues of redress in respect of some legal bases for surveillance by US intelligence agencies (for example Executive Order 12333 discussed below). It was also concerned that when causes of action do exist in the US they are limited in a manner inconsistent with the decision of the CJEU in *Schrems* (para. 89) and other cases and that claims are limited by what it described as restrictive rules in the United States on standing to bring proceedings.

71. The solution devised by the Commission and the government of the United States was to adopt the Privacy Shield Decision, not an unconditional adequacy decision.

72. For these reasons, I am of the opinion that the adoption of the Privacy Shield Decision by the Commission is not binding and determinative of the issue as to whether the transfer of personal data by Facebook to Facebook Inc. pursuant to one of the SCC decisions (that of 2010) is valid.

73. In any event, the court is obliged to consider whether a genuine or well-founded issue as to the validity of a decision of the Commission arises. It cannot

abdicate its responsibilities in this regard on the basis of the terms of Article 25 (6) of the Directive and s. 11 (2) of the Acts. This is clear from the ruling in *Schrems*.

74. The Safe Harbour Decision was likewise a community finding within the meaning of the s. 11 (2) of the Acts and Article 25 (6) of the Directive. It had been adopted by the Commission pursuant to the provisions of Article 31 (2) and Article 25 (6) of the Directive. The High Court in *Schrems v. The Data Protection Commissioner* held that the conclusion that Mr. Schrems' complaint was unsustainable in law because of the Commission's Safe Harbour Decision was central to the entire case. The court held that Mr. Schrems' objection in reality was to the terms of the Safe Harbour regime itself. The court interpreted the central question to be whether the DPC was as a matter of European Union law, absolutely bound to follow the decision of the Commission. It therefore referred the question to the CJEU for a preliminary ruling in the following terms:-

(1) 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 [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) 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?

75. Neither the High Court nor the CJEU suggested that the High Court was not competent to make a reference to the CJEU on the basis that the Safe Harbour Decision, as a decision of the Commission, was binding on the High Court as well as the DPC, notwithstanding the fact that neither of the parties, in terms, had challenged the validity of the Safe Harbour Decision.

76. In its ruling in *Schrems*, the CJEU held that a Commission decision adopted pursuant to Article 25 (6) of the Directive cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim within the meaning of Article 28 (4) of the Directive concerning the protection of their rights and freedoms in regard to the processing of that data (para. 53). The decision of Commission cannot eliminate or reduce powers expressly accorded to national supervisory authorities by Article 8 (3) of the Charter and Article 28 of the Directive. The court held that even if the Commission has adopted a decision pursuant to Article 25 (6) of the Directive, the national supervisory authorities when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the Directive.

77. The court observed that the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and of fundamental rights. Commission decisions adopted pursuant to Article 25 (6) of the Directive cannot therefore escape such a review.

78. The court noted that neither the national supervisory authorities nor a national court had jurisdiction to disapply a decision of the Commission or declare any such act invalid themselves. The CJEU alone enjoyed the jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25 (6) of the Directive, is invalid. At para. 64 and 65 of the ruling, the court held: -

> *"64. In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of [a claim contesting the compatibility of a Commission decision with the protection of the privacy and fundamental rights and freedom of individuals] are unfounded and therefore rejects it, the person who lodged the claim must… have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts…those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded.*
>
> *65. …where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28 (3) of Directive 95/46, read in the light in particular of Article 8 (3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before* ***the national courts in order for them, if they share its doubts as to the validity of the***

Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity."

79. I am satisfied therefore that this court has jurisdiction to make a reference for a preliminary ruling to the CJEU for the purpose of considering the validity of the SCC decisions. On the basis of *Schrems* I have a duty so to do if I share the "well- founded" concerns raised by the DPC before the court. I am not precluded from so acting by reason of the adoption by the Commission of the Privacy Shield Decision for the reasons analysed above.

The Scope of the Application For a Reference to the CJEU

80. The DPC instituted these proceedings as she formed the view that the reformulated complaint of Mr. Schrems raised issues concerning the validity of the SCC decisions and she followed the directions set out in the ruling of the CJEU in para. 65 of *Schrems*.

81. The rules of court did not mandate any particular procedure for her to bring the proceedings before the national court. She therefore decided to present her concerns in relation to the validity of the SCC decisions to the court by way of a draft decision. There was no requirement that she adopt this approach.

82. During the hearing before me it was argued that the court's jurisdiction was confined to deciding whether or not it shared the well-founded concerns identified by the DPC in her draft decision.

83. Facebook in particular adduced a very considerable amount of evidence which had not been available to the DPC when she drew up her draft decision and this was all opened to the court. In addition, subsequent to the date of the draft decision, there were significant legislative changes at European Union level. The Commission adopted the Privacy Shield Decision (though a draft of the decision had been available

to the DPC when she prepared her draft decision) and the SCC decisions were amended in December, 2016 by the replacement of Article 4 with a new Article 4.

84. The fact that the DPC chose to present her concerns to the court by way of a draft decision does not mean that (a) she must be confined to arguing those grounds and may not expand her arguments in the light of the evidence and arguments advanced during the course of the trial and (b) that the court must be confined to what is set out in her draft decision.

85. The court as a matter of principle not only is entitled, but is obliged, to consider all of the facts and law properly presented to the court and to decide on the basis of those facts and arguments whether or not a reference is required. This is no ordinary *lis inter partes*, as I have explained, where the rights of private parties, or private parties and the State or emanations of the State, require a ruling on Union law in order to resolve the existing dispute between them. Here, the validity of decisions of the Commission are the essence of the proceedings because, in the course of her inquiry into Mr Schrems' reformulated complaint, the DPC has concluded that she requires a ruling from the CJEU on the validity of the SCC decisions in order to complete her inquiry. In such circumstances, it would be wholly wrong, in my opinion, to limit the scope of the court's enquiry and consideration on a quasi procedural basis. The court is in any event obliged to take account of amendments to the law that may have occurred in the interval between the institution of the proceedings and the hearing of the action, so to that extent it is not confined to the issues raised in the draft opinion. The parties advanced no reason or authority why the court should so limit its enquiry.

86. In *Schrems* (para. 64) the CJEU recognised that if a national supervisory authority rejected the complaint of a data subject the complainant must have a right to appeal that rejection to a court. The court may then decide whether or not the

arguments raised by the complainant are well founded or it may **of its own motion** decided that there are well founded concerns as to the validity of a decision.

87. There is no reason in principle why the court should enjoy a jurisdiction to formulate its own concerns in relation to European legislation or acts where the complainant appeals the rejection of his complaint to the national court, but *per contra*, when a national supervisory authority upholds the complaint and wishes to bring its concerns to the only forum with jurisdiction to rule on the matter, the CJEU, the court does not and the court's jurisdiction should be confined solely to those concerns raised by the national supervisory authority.

88. In my opinion, the CJEU was not implicitly limiting the right of a national court to make a reference to the CJEU. This reading of para. 64 of the ruling is particularly unlikely as the CJEU was expressly setting out the means by which a decision of the Commission, for example, could be brought before the CJEU as the sole authority with jurisdiction to resolve this point in circumstances where there was a well-founded belief as to the validity of the decision or act in question.

89. If a data subject complains that his data is not protected when it is transferred to a third country and challenges a decision of the Commission which says that the third country provides adequate protection, a national supervisory authority must investigate his complaint. If the national supervisory authority rejects the claim, the data subject has a right of appeal to a court. The court must make its own assessment regarding (1) the decision of the Commission and (2) the rejection by the national supervisory authority of the complaint as to whether one or more of the grounds put forward are well founded. In addition, the court may of its own motion raise a ground of invalidity and make a reference to the CJEU on the basis of one or other of these grounds. This

jurisdiction cannot be restricted simply because a national supervisory authority accepts one or more of the complaints as well founded.

90. In my opinion, this court must consider all of the evidence, all of the law and all of the arguments advanced by any of the parties including the a*mici curiae in* deciding whether or not to make a reference to the CJEU. It is not confined to the arguments set out by the DPC in her draft decision dated 24th May, 2016.

Comparator

Facebook's Submissions

91. Facebook argues the fact that the interference with the personal data of EU data subjects which gives rise to the concerns of the DPC is interference by the United States intelligence agencies means that the court is concerned with data protection in the context of national security. The assessment whether a third country ensures adequate protection to the personal data of EU citizens must involve a comparison with another regime and like must be compared with like. In other words, there must be a comparator to processing of private data by the United States intelligence agencies for purposes of national security against which the assessment whether the protections or safeguards afforded in the United States to data subjects in respect of their personal data are adequate may be made.

92. The comparator for processing in a third country which is not concerned with national security is to be found in the Directive read in the light of the Charter. However, according to Facebook, the Directive and the Charter do not apply to processing by Member States for national security purposes. It follows therefore that there is no European Union comparator for processing by a third country for national security purposes. The Facebook argues that the comparator therefore can only be

found in the domestic laws of each of the Member States. As the Directive confers no remedy in each of the Member States in respect of EU data subjects where there is inference with personal data on the grounds of national security, it follows that there is no requirement that there be a remedy in the United States.

The DPC's Submissions

93. The DPC argues that as a matter of principle the adequacy of the laws of the third country must be assessed by reference to Union law and not by reference to the laws of individual Member States or even an amalgam of the laws of the Member States. In *Watson* the CJEU applied Union law to national legislation. It would be inconsistent with both principle and case law to apply anything other than Union law as a comparator to the legal regimes of third countries.

94. As a practical matter, the test suggested by Facebook is unworkable and leads to the logical conclusion that there is no possible comparator. It follows that if there is no comparator it can never be assessed and therefore the laws of a third country can never be found to be inadequate, regardless of the level of protection afforded to the data to be transferred or the degree of interference to which it is subject in the name of national security by the third country. This applies to all non-EEA countries no matter what legal regime exists in the third countries.

95. The DPC referred to a report of the European Union Agency for Fundamental Rights dated 2015 entitled Surveillance by Intelligence Services Code on Fundamental Rights Safeguards and Remedies in the EU. The report notes that at the EU level the rights to privacy and data protection are enshrined in Articles 7 and 8 of the Charter and the right to data protection is provided for in Article 16 TFEU and Article 39 TEU. It refers to the Directive and other directives. It refers to the national security exemption in Article 4(2) TEU and Article 3(2) of the Directive. It then states: -

"The limits of the national security exemption are subject to debate, including in relation to the activities of intelligence services. Although international guidelines exist, there is no uniform understanding of 'national security' across the EU. The concept is not further defined in EU legislation or in CJEU case law, although the CJEU has stated that exceptions to fundamental rights must be interpreted narrowly and justified. The CJEU has also stated that the mere fact that a decision concerns State security does not render EU law inapplicable. (See ZZ v. Secretary of State Home Department, 4th June 2013, para. 38)." Page 10.

96. The Report continues at p. 11 as follows:-

"This unclear delineation of 'national security' also has repercussions for the applicability of EU law, which depends both on the interpretation of the national security exemption's scope and on the specific characteristics of the various surveillance programmes carried out by intelligence services. Although the existence of such programs remains largely unknown, even in light of the Snowdon revelations, some contain elements that can justify the full applicability of EU law. ***For instance, when EU companies transfer data to intelligence services, including those of third countries, they are considered under the Data Protection Directive as data controllers who collect and process data for their own commercial purposes. Any subsequent data processing activities, such as the transfer of personal data to intelligence services for the purpose of the protection of national security, will therefore fall within the scope of EU law [Schrems]****. Any limitations of the rights to privacy and personal data protection should be examined according to Article 13 of the Data Protection Directive and Article 15 of the e-Privacy Directive,*

as well as Article 52(1) of the Charter. Such limitations are to be treated as exceptions to the protection of personal data, and thus subject to narrow interpretation and requiring proper justification. ***The essence of the right to privacy and protection of personal data shall at any rate be respected. The 'national security' exception thus cannot be seen as entirely excluding the applicability of EU law. As the UK Independent Reviewer of Terrorism Legislation recently put it,***

> ***"National security remains the sole responsibility of each Member State: but subject to that, any UK legislation governing interception of communications data is likely to have to comply with the EU Charter because it would constitute a derogation from the EU directives in the field."***

Discussion

97. I found the submissions of the DPC more compelling than those of Facebook. They are consistent with the recent decisions of the CJEU in *Schrems* and *Watson* and with the views of the European Union Agency for Fundamental Rights. However, that is not the end of the matter. My decision on this point is not binding across the other Member States of the European Union but it is clearly a decision which requires uniformity across the European Union. As it is not competent for a national court to make such a decision, it is a matter on which the CJEU is required to give a ruling in order properly to give effect to Union law. For the purposes of this judgment I am not persuaded that the application of the DPC for a reference to CJEU should be refused on the basis of this argument urged by Facebook. On the contrary, it throws up a point upon which a ruling from CJEU is required in order to determine these proceedings.

Protection of Personal Data Required by the Directive

98. The principle objective of the Directive is as set out in Article 1 quoted above. It is the protection of the fundamental rights and freedoms of natural persons and in particular the right to privacy with respect to the processing of personal data. Recital 10 of the Directive makes clear that the aim is to ensure a high level of protection in the Union. This was confirmed by the CJEU in its ruling in *Schrems* at para. 39 where it stated: -

> *"It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that the directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data,* ***but also a high level of protection of those fundamental rights and freedoms****. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to protection of personal data, guaranteed by Article 8 of thereof, is, moreover, emphasised in the case law of the court."*

99. The processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. (Article 2(b)).

100. Chapter II of the Directive establishes general rules on the lawfulness of the processing of personal data. Member States are required to provide that personal data is processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; is

adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and are accurate. Where necessary, personal data must be kept up to date and every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they were further processed, are erased or rectified. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes which the data were collected or for which they are further processed. Member States are required to lay down appropriate safeguards for personal data stored for longer periods or historical, statistical or scientific use. (see Article 6)

101. Article 22 requires member states to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question. This is in addition to the data subject's right to an administrative remedy before the national supervisory authority (as required by Article 28). Article 23 requires Member States to provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation from the controller for the damage suffered. The controller may be exempt from this liability, in whole or in part, if the controller proves that it is not responsible for the event giving rise to the damage. In addition, the member states are required to adopt suitable measures to ensure the full implementation of the provisions of the Directive and to lay down sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive (see Article 24).

102. The starting point therefore is that data processed within the European Union is entitled to a high degree of protection and the Member States are required to provide

for the right of every person to a judicial remedy for any breach of the rights guaranteed to him. *Prima facie* any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions is entitled to receive compensation for that damage.

103. These rules apply to processing of data within the EU. I turn now to consider the question of the transfer of personal data to third countries pursuant to Article 25 and 26 of the Directive.

104. Personal data which either are undergoing processing or are intended for processing after transfer may only be transferred to a country outside the EEA ("a third country") if the third country ensures an adequate level of protection. Transfers of personal data to third countries which do not ensure an adequate level of protection are therefore prohibited. (See Recital 57 and Article 25 (1)).

105. The adequacy of the level of protection afforded by the third country is to be assessed by reference to the criteria set out in Article 25(2). It is in light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration is to be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the 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. In *Schrems* the CJEU held that the adequate level of protection to be afforded to personal data transferred to third countries is to be the same as the high level of protection guaranteed by the Directive to processing of personal data within the EU.

106. Article 25 (6) authorises the Commission to make a decision that a particular third country ensures an adequate level of protection as required by Article 25 (2) of

the Directive. In *Schrems* (paras. 39 and 46) it was held that transfers pursuant to an adequacy decision under Article 25 are entitled to a high level of protection and that an adequacy decision by the Commission under Article 25 (6) must satisfy the test set out in Article 25 (2).

107. The CJEU held that the third country is not required to ensure a level of protection that is identical to that guaranteed by Union law. It is required to ensure by reason of its domestic law or its international commitments a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the Directive read in the light of the Charter. (*Schrems* para. 73). It is thus necessary to ensure that the requirement that the personal data transferred to the third country continues to enjoy a high level of protection is not disregarded.

Transfers of Data Pursuant to Article 26

108. Recitals 58 and 59 of the Directive recognise that provisions need to be made for exemptions from the prohibition on transferring personal data to a third country which does not ensure an adequate level of protection for personal data. Article 26 governs these derogations from the requirements of Article 25.

109. All transfers of personal data to third countries pursuant to Article 26 are predicated upon the fact that the third country does not ensure an adequate level of protection within the meaning of Article 25 (2). Notwithstanding this fact, Article 26 provides that transfers may take place on certain specified conditions.

110. Transfers made pursuant to Article 26 (1) correspond to the transfers referred to in Recital 58. These transfers are based upon the principle of waiver or transfers which are in the interests of the data subjects. They are not based upon the level of protection afforded to the data once it is transferred to the third country. These data transfers are

legitimised not on the basis of the protection afforded to the personal data but upon the six individual grounds specified in sub article 1.

111. Article 26 (2) states that without prejudice to para. 1, Member States may authorise 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), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. This underscores the fact that transfers of data under Article 26 are not premised on the protections available in a third country. In the case of para. (2) the transfer is permitted if the controller of the data adduces adequate safeguards in respect of that data and as regards the exercise of the corresponding rights. The protection does not derive from the law of the third country but the practices of the controller of the data. Paragraph 2 expressly states that the safeguards may result from appropriate contractual clauses.

112. Article 26 (4) provides as follows: -

> *"Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision."*

113. The SCC decisions were decisions taken by the Commission pursuant to Article 26 (4) in accordance with the procedure established by Article 31 (2).

114. Thus there are a variety of mechanisms whereby personal data may lawfully be transferred from the EEA to a third country. It may be pursuant to a Commission adequacy decision (Article 25 (6)), pursuant to one of the six derogations identified in Article 26 (1), pursuant to an authorisation by a member state adopted pursuant to

Article 26 (2) or pursuant to a Commission decision adopted pursuant to Article 26 (4) that certain standard contractual clauses offer sufficient safeguards as required by para. 2 of Article 26.

SCC Decision 2010/87

115. Recitals 11, 12, 19, 20 and 22 provide: -

(11) Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.

(12) Standard contractual clauses should provide for the technical and organisational security measures to be applied by data processors established in a third country not providing adequate protection, in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against

accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

(19) Standard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular where the data subjects suffer damage as a consequence of a breach of the contract.

(20) The data subject should be entitled to take action and, where appropriate, receive compensation from the data exporter who is the data controller of the personal data transferred. Exceptionally, the data subject should also be entitled to take action, and, where appropriate, receive compensation from the data importer in those cases, arising out of a breach by the data importer or any sub-processor under it of any of its obligations referred to in the paragraph 2 of Clause 3, where the data exporter has factually disappeared or has ceased to exist in law or has become insolvent. Exceptionally, the data subject should be also entitled to take action, and, where appropriate, receive compensation from a sub-processor in those situations where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent. Such third-party liability of the sub-processor should be limited to its own processing operations under the contractual clauses.

(22) The contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law. The same law should also govern the provisions on data protection of any contract with a sub-processor for the sub-processing of the processing activities of the personal data transferred by the data exporter to the data importer under the contractual clauses.

116. Article 1 of the Decision provides that the standard contractual clauses set out in the Annex to the Decision are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26 (2) of the Directive. Article 3 (f) defines *"applicable data protection law"* for the purposes of the Decision as *"the legislation protecting the fundamental rights and freedoms of individuals and, in particular, the right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data controller is established."*

117. The data exporter is the controller who transfers the personal data. The data importer means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this SCC decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of the Directive. (Article 3 of the Decision).

118. As originally adopted, Article 4 (1) provided: -

Article 4

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data

protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;

(b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

119. Following the decision of the CJEU in *Schrems* Article 4 was replaced by a new Article 4 by Commission Implementing Decision (EU) 2016/2297. It now reads: -

"Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive 95/46/EC leading to the suspension or definitive ban of data flows to third countries in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States."

120. Clause 3 of the standard contractual clauses is a third-party beneficiary clause. 3.1 provides:

"*The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6 (1) and (2), Clause 7, Clause 8 (2), and Clauses 9 to 12 as third- party beneficiary."*

Omitted from the third-party beneficiary clause are Clause 4 (a) and (j) and Clause 5 (f).

121. Clause 4 sets out that the data exporter agrees and warrants the matters listed at (a) to (j). Sub Clause 4 (a) provides that the data exporter agrees and warrants:-

> *"that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;"*

This is an agreement between the data exporter and the data importer. The sub-clause is excluded from the third party beneficiary clause so that the data subject cannot enforce this warranty as against the data exporter pursuant to the standard contractual clauses.

122. Sub clauses (b), (c), (d), (e), (i) and (j) provide as follows:

> *(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;*
>
> *(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;*
>
> *(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where*

the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(*i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and*

(j) that it will ensure compliance with Clause 4(a) to (i).

123. On the facts of this case, the applicable data protection law referred to is Irish law. As noted above, a data subject cannot enforce sub clause (j) against the data exporter as it is omitted from the third party beneficiary clause. Thus, the data subject may not ensure compliance with Clause 4 (a) by directly suing the data exporter pursuant to these clauses. It will be noted that a significant number of these warranties relate to the security measures relating to the processing of the data once it has been transferred to the third country and not to the legal protections applicable to the data.

124. By Clause 5 (a) (b) and (c) the data importer agrees and warrants as follows:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

125. A footnote to Clause 5 provides as follows: -

"Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements."

129. At Clause 6 the parties agreed that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from data exporter for the damage suffered. This entitles the data subject to sue the data exporter in the relevant member state where the data exporter is situated. He is not obliged to sue a data importer in a third country outside the European Union. The proceedings will be governed by the national law of the Member State, and not the law of the third country.

130. By Clause 6.2 the data importer agrees that if the data subject is not able to bring a claim for compensation in accordance with Clause 6.1 against the data exporter because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, then the data importer agrees that the data subject may issue a claim against it as if it were the data exporter unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law. Thus, the data subject may sue the data importer if necessary in the Member State where the data exporter was situate. That case likewise will be subject to the law of the member state.

131. There is a similar provision which allows a data subject to sue a data sub-processor at Clause 6.3. The liability of the sub-processor is limited to its own processing operations under the Clauses.

132. The other two SCC decisions the subject of these proceedings were not analysed in the hearing before me which focused exclusively upon the decision of 2010. This was the decision which Facebook said it employed to transfer Mr. Schrems' personal data to Facebook Inc.

The SCC Decisions and the laws of Third Countries

133. What is the level of protection required to be afforded to personal data transferred to third countries pursuant to standard contractual clauses adopted in accordance with a decision of the Commission under Article 26 (4) in light of the provisions of the Directive and in particular Articles 25 and 26 read in the light of the Charter?

Submissions of the DPC

134. The DPC says that whether the Directive refers to adequate protection (Article 25), adequate safeguards (Article 26 (2)) or sufficient safeguards (Article 26 (4)), data processing is entitled to the same high level of protection whether or not the processing occurs within the EU or is transferred for processing to a third country and regardless of the method employed to effect a lawful transfer of personal data to a third country. This submission is based upon Recital 10, in particular, of the Directive. She also relies upon the opinion of Advocate General Bot in Schrems. At paras. 139 and 140 he states:-

> *"Article 25 of Directive 95/46 is based entirely on the principle of the transfer of personal data to a third country cannot take place unless that third country guarantees an adequate level of protection of such data.* ***The objective of that article is thus to ensure the continuity of the protection afforded by that directive where personal data is transferred to a third country****. It is appropriate, in that regard, to bear in mind that that Directive affords a high level of protection of citizens of the Union with regard to the processing of their personal data.*
>
> *In view of the important role played by the protection of personal data with regard to the fundamental right to privacy, this kind of high level of protection*

must, therefore, be guaranteed, including where personal data is transferred to a third country."(emphasis added)

135. She also refers to the fact that Advocate General Bot noted that there might be an apparent difference between the English word adequate and the French word "adéquat". The only criterion that must guide the interpretation of that word is the objective of attaining a high level of protection of fundamental rights, as required by the Directive.

136. The DPC says that the standard contractual clauses must ensure that personal data transferred pursuant to those clauses to a third country continue to enjoy that high level of protection. She submits that when the particular provisions of the law of the United States are considered, there are well-founded concerns that the laws of the United States do not ensure this continuity of a high level of protection and that the standard contractual clauses do not ensure that data transferred to the United States enjoys a high level of protection to which data subjects in the European Union are entitled by virtue of the provisions of the Directive as read in the light of the Charter.

Submissions of Digital Europe

137. Facebook, Digital Europe and the Business Software Alliance disagreed with the analysis of the DPC. They say Article 26 is a derogation from Article 25. By definition, transfers of data to third countries pursuant to Article 26 are on the basis that the third country does not afford the data an "adequate level of protection". The six circumstances in Article 26 (1) are not related to the level of protection to be afforded to the data transfers.

138. Digital Europe submitted that it was part of the scheme of the Directive that it is permissible to transfer data to a third country whose laws either have not been assessed or whose laws have been found to be inadequate in their protection of

personal data with contractual clauses providing a substitute for the protections that are not available in the third country.

139. It submitted that under Article 26 (2) it is for the controller to adduce adequate safeguards. These are provided by standard contractual clauses which the Commission has found to provide sufficient safeguards pursuant to Article 26 (4). The key innovation of the standard contractual clauses is to impose the responsibility for ensuring that the Charter rights of EU data subjects are respected within a third country upon the data exporting and importing entities. The SCCs protect the data protection rights of EU citizens guaranteed by the Charter including the availability of remedies through a combination of the contractual protections enshrined in the standard contractual clauses and the powers granted to the data protection authorities pursuant to Article 4.1 of the SCC decisions i.e. the power to suspend or ban data flows to a particular third country. EU citizens are enabled to obtain relief before the relevant national data protection authority (DPA) or national court where the data exporter is located and if necessary to have transfers of their data to the third country suspended. The SCCs therefore provide "adequate safeguards" within the meaning of Article 26 (2) of the Directive.

140. Digital Europe submitted that the argument of the DPC in effect required that wherever EU data subjects' personal data was transferred they were entitled to the protections guaranteed by Article 47 of the Charter. It was submitted that this would utterly defeat the purpose of the Directive to facilitate transfers of data to third countries, many of which would not satisfy the requirements of a remedy essentially equivalent to that guaranteed by Article 47 of the Charter.

141. Digital Europe pointed out that the DPC's argument was that the SCCs only established rights in contract which by definition could not be binding upon the United

States government or any agency of the United States government. Therefore, the SCCs could not provide an effective remedy in the event that the personal data of EU citizens is unlawfully interfered with whether on national security grounds or otherwise. This argument renders Article 26 (2) inoperable. It submitted that if it is the case that contractual clauses can never be adequate to protect personal data when such data has been transferred to a third country which does not provide an adequate level of protection within the meaning of Article 25 (2) then the utility of Article 26 (2) is entirely undermined. It results in applying the criteria of Article 25 (2) to every transfer of data thereby rendering the derogations permitted in Article 26 inoperable and redundant. If the adequacy of the protections in the destination country were a requirement for data exporters to rely on SCCs then the very notion of SCCs would become meaningless because data exporters would simply rely on the adequacy of protection under Article 25.

Submissions of Business Software Alliance

142. The Business Software Alliance (BSA) submitted that there was a clear distinction between transfers under Article 25 on the one hand and transfers under Article 26. By definition transfers of data pursuant to Article 26 were to a country which did not ensure an adequate level of protection within the meaning of the Directive. It was argued that Article 26 (2) implies that appropriate contractual provisions could provide a sufficiently robust level of protection for data subjects specifically in scenarios where their data were being transferred to third countries which do not offer an adequate level of protection. The fundamentals premise of Article 26 as far as the SCCs is concerned, is that the contract pursuant to which the data are transferred itself provides sufficient protection to data subjects, both in terms of substantive protection and availability of remedies. Under the SCCs data subjects

have a judicial remedy in the EU. Article 26 generally, and the SCCs in particular, are not premised on an effective remedy, whether judicial or otherwise, being available in the third country to which the data are transferred. The SCCs provide the remedies in the transferring EU member state according to its law. This is intended to comply with the requirements of the Charter and in particular Article 47.

143. The BSA submitted that the power of a DPA to prohibit or suspend data flows to a particular third country pursuant to Article 4.1 of the SCCs decision was crucial to assessing the validity of the SCC decisions. While a data subject may have no direct remedy against agencies in the third countries, the data subject could call upon a DPA to suspend or prohibit flows of data to that third country and it was open to the DPA to protect data subjects by making such an order.

144. Under Article 4 (1) (a) of the SCC Decision (as originally drafted) any analysis of the mandatory requirements imposed by a third country in relation to accessing the data for the purposes of national security must be assessed in relation to the "*restrictions necessary in a democratic society*". EU law itself allows significant limitations and exclusions in respect of EU data protection law in the realm of national security, defence, public security and criminal investigations. This must be taken into account when considering whether "adequate remedies" are available in third countries and whether the restrictions are necessary in a democratic society. Furthermore, in assessing whether the protection in a third country is "essentially equivalent" to the level of protection available within the EU, it is necessary to have regard to the degree to which EU data protection laws do not apply to Member States in the realm of national security, defence, public security or criminal investigations.

145. It was argued that if it was necessary to apply the Article 25 standard of adequacy of protection to transfers effected under Article 26, this effectively revokes

Article 26 and makes it impossible to comply with. If it was necessary to have the same protection as that provided by Article 25, this can never be achieved by means of standard contractual clauses under Article 26. Standard contractual clauses by definition operate in the private sphere and do not bind the national authorities in third countries. It was submitted that this means that there must be a different structure of protection and that the rights of data subjects are protected differently under Article 26 compared to Article 25.

146. It was argued that it was important to differentiate between the level of protection that was required (a high level) and how that protection was achieved. It was submitted that data subjects whose data are transferred pursuant to SCCs have a legal remedy in the Member State of the exporter but not in the third country importer State. The SCCs were not and are not intended and could not have been intended to remedy the inadequacy in relation to the third country legal protections. If effective judicial remedies in third countries are a prerequisite for lawful transfer under Article 26 (2), it can never be satisfied.

Response of the DPC

147. In response, the DPC asks what remedy does an EU citizen have where his data are transferred to a third country pursuant to the SCC decisions and in that third country his data are interfered with unlawfully for the purposes of national security? The ability to sue either the data exporter or the data importer or the sub-processer pursuant to the SCCs is of no benefit. In this case, no wrong has been alleged against either Facebook or Facebook Inc. or any of the sub-processers in relation to the processing of his data (assuming it is being processed pursuant to the SCCs). Mr. Schrems could not look to the SCCs for a remedy in respect of his complaints.

Discussion

148. The submissions of Digital Europe and BSA are based on the argument that the adequate safeguards of an EU data subject in relation to his data privacy rights is to be found in the SCCs rather than in the laws of the importer country. The clauses compensate for the inadequacy of those laws. But, the SCC decisions themselves refer to the content of the laws of the third country. Under Article 4.1 (a) of SCC Decision 2010/87/EU (as originally drafted), a DPA had power to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data where is it is established that: -

> *"... the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which goes beyond the restrictions necessary in a democratic society as provided for in Article 13 of [the Directive] where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses."*

149. This Article shows that as originally drafted, DPAs had a role in assessing the law of the country of the data importer or sub-processer. The DPAs were to assess the extent to which the data importer or sub-processer was required to derogate from the data protection law of the Member State where the data exporter was established. The DPAs were required to determine whether the requirements of the third country laws go beyond the restrictions necessary in a democratic society and whether those requirements were likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the SCCs.

150. While this Article has been repealed and a new Article 4 substituted, the implications of this Article are relevant to the construction of the SCC decisions and show that the SCCs alone cannot ensure an adequate level of protection in the third country for data protection rights and freedoms. Despite the provisions of the SCCs, nonetheless data transferred pursuant to the SCCs to third countries may not enjoy the adequate level of protection mandated by reason of the laws of the individual third country.

151. It seems to me that the provisions of the law in a particular third country may be the basis for suspending or prohibiting a data transfer or transfers pursuant to an SCC decision. It follows therefore that the provisions of the law of that third country may provide the basis for concluding that data transfers effected pursuant to SCCs under Article 26 (2) do not provide adequate safeguards for the personal data of data subjects.

152. As referred to above, following the decision of CJEU in *Schrem*s, this Article was replaced by a new Article 4 so that the power of the DPAs under the SCC decisions is the general power conferred on the DPAs by Article 28 of the Directive. This applies to all forms of processing whether within the EU or to transfers of data to third countries. It is not specific to the transfer of data outside the EU to third countries. It is not constrained as was formerly the case under Article 4.1 (a) as originally drafted. The laws of the third country may be such as to require the suspension or prohibition of data transfers to the third country under the provisions of SCCs notwithstanding protections afforded by the SCCs themselves, though whether this is always the appropriate response is a matter to which I shall return.[3]

[3] This analysis is reinforced by footnote 12 to clause 5 of the SCCs. It provides that mandatory requirements of the national legislation applicable to the data importer which go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13 (1) of Directive 95/46/EC…are not in contradiction with the standard contractual clauses. It gives as examples

153. It seems to me that this leads to the following conclusion. Article 26 is a derogation from Article 25. Data transfers pursuant to Article 26 are not premised upon the existence of an adequate level of protection in the third country. Nonetheless the data is still entitled to a high level of protection, as was stated by Advocate General Bot in *Schrems*. It follows therefore that transfers of personal data to a third country cannot simply step outside the protections guaranteed by the Directive entirely. It is clear that data exporters cannot rely solely upon the SCCs as complying with the requirements of the Directive regardless of the legal regime in the third country to which the data is exported. DPAs have an obligation to ensure that the data still receives a high level of protection and they are expressly granted powers to suspend or prohibit data transfers if the laws of the third country undermine that mandatory high level of protection.

154. If there are inadequacies in the laws of the United States within the meaning of Union law, the SCCs cannot and do not remedy or compensate for these inadequacies. The private contractual clauses cannot bind the sovereign authority of the United States and its agencies. This was not contended. This conclusion means that the terms of the SCCs themselves does not provide an answer to the concerns raised by the DPC in relation to the existence of effective remedies for individual EU citizens in respect of possible infringement of their data privacy protection rights if their data are subject to unlawful interference. Whether Article 4 of the SCC decisions provides the answer, I consider later in this judgment.

The Relevant Laws of the United States of America.

155. Five experts gave evidence in relation to the provisions of US law relevant to the issues in these proceedings. The primary source of law is the Constitution of the

---

internationally recognised sanctions, tax reporting requirements or anti money-laundering reporting requirements. The footnote would be superfluous if the arguments of the a*mici curiae* were correct.

United States. There are then federal statutes, state statutes (which are not relevant to the issues in these proceedings) and case law. The judgments of the United States Supreme Court are binding throughout the United States. The US Courts of Appeal decisions are binding in their particular circuits and persuasive in other circuits. The decisions of District Courts are of less precedential value.

156. The United States is a common law jurisdiction. The state of the law at any particular moment on a given point may be in flux and there may be divergent, even inconsistent, authorities from the circuits. It is not always possible to give a clear unqualified statement of the current state of the law. Therefore, of necessity, the opinions of the experts reflect their best endeavours to explain the laws of the United States as of date of the hearing before me in February, 2017. There could not be a clear-cut consensus on all points. That said, there was in fact a significant degree of agreement and often the areas of disagreement were at the margins.

157. The experts gave very detailed evidence in relation to many aspects of US law. Of necessity, this judgment cannot record or assess the entirety of this evidence. I have summarised the evidence I believed was necessary for the purposes of reaching my decision on the issues in this case. It is focused on the transfer of personal data from Facebook to Facebook Inc. for private purposes and on the possibility that the data may as a result be made available to or actually accessed, processed and retained by authorities in the United States for reasons of national security.

158. After the conclusion of the trial and before judgment was delivered there were significant developments relevant to the evidence adduced on the laws and practices of the United States. As an exceptional measure, I permitted the parties to adduces this additional evidence and for the expert witnesses to give further testimony in relation to it. I heard brief submissions from all parties in light of the developments.

What is the correct basis upon which the court should assess the adequacy of the protections afforded by the laws of the United States to the data privacy rights of EU citizens?

159. There was fundamental disagreement between the DPC on the one hand and Facebook and the United States on the other hand in the approach to be taken in assessing the adequacy of US law for the purposes of investigating Mr. Schrems' reformulated complaint and these proceedings.

Submissions of the DPC

160. The DPC started from the adequacy criteria set out in Article 25 (2) of the Directive. This states that particular consideration is to be given to, *inter alia*, the rules of law, both general and sectoral, in force in the third country to which the data is to be transferred. Article 47 of the Charter guarantees everyone the right to an effective remedy before a tribunal in compliance with the conditions laid down in the Article. Article 52 of the Charter requires that the essence of the right must be respected. She analysed the remedial regime in the United States and conducted what might be described as an inadequacy assessment rather than an adequacy assessment.

161. She did not engage in an investigation to see whether US laws provided adequate protection such as would be conducted by the Commission for the purposes of making a decision pursuant to Article 25 (6). She reasoned that an essential requirement of Union law is that there be a remedy compatible with Article 47 so that EU data subjects' fundamental rights and freedoms in relation to data protection may be vindicated. If US law does not guarantee the availability of a remedy compatible with Article 47, then, regardless of any other provisions of US law, it cannot provide adequate protection for the personal data of EU data subjects as guaranteed by the Directive read in the light of Article 47 of the Charter.

162. She therefore investigated the remedies available to EU citizens in the United States for interference in their personal data by US intelligence agencies. The evidence adduced by her experts focused on the availability of and limitations on remedies available to EU citizens and the obstacles to obtaining relief in the United States for breach of their data protection rights and freedoms.

163. The DPC and Mr. Schrems strongly argued that the court should be concerned with the laws of the Unites States and not the practice. They argued that the adequacy of the level of protection of the third country is to be assessed by reference to the content of the applicable rules and the practice designed to ensure compliance with those rules. This is based upon the analysis of CJEU in *Schrem*s at para. 75 and the Advocat General at para. 143. Thus, evidence as to practices in the United States were not relevant to the consideration of the court.

Submissions of Facebook and the government of the United States

164. Facebook and the United States government said that this approach was wrong in principle. An adequacy assessment of the entire relevant regime in the United States was required. The DPC – and the court – should make an holistic assessment of the laws and protections afforded to data subjects. Neither the DPC nor the court should confine its consideration to the legal remedies available to EU citizens in the United States. It must look at the practices, oversight mechanisms and other forms of indirect protection employed to ensure compliance with the requirements of legal authorisations, administrative protections, congressional oversights and wider protections against unlawful surveillance by United States intelligence agencies before making any decision.

165. They submit that a person only enjoys a right to a remedy under Article 47 where there is at least an arguable violation of that person's rights and freedoms. The

DPC did not conduct such an analysis so the issue does not even arise. Even if it did, the court must consider the overall context of the right or entitlement and then assess what remedy is required in the circumstances. They say that the ruling of CJEU in *Schrems* (para.95) establishes that the correct test is whether or not the laws of the third country fail to provide "any possibility for an individual to pursue legal remedies" in relation to breaches of his data protections rights.

166. They submit that the regime in the United States respects the essence of the rights of EU citizens guaranteed by Articles 7, 8 and 47 of the Charter. The limitations on the fundamental rights and freedoms respect the essence of those rights. The limitations are proportionate, necessary and comply with the requirements of Article 52 as they genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. They say that a proportionality test must be conducted and the DPC never purported to carry out such a test. Therefore, her analysis is fundamentally incorrect.

The legal basis for electronic surveillance by the United States

167. Before considering these arguments and whether it is always necessary to conduct a proportionality analysis, it is necessary to put them in context and to consider the legal basis upon which surveillance is conducted by the agencies of the United States, the practice of the intelligence agencies, the oversight mechanisms (on the assumption that this is relevant to the assessment to be conducted) and the remedies available to parties claiming to have suffered legal wrong as a result of surveillance by the intelligence agencies of the United States.

168. The principal statute to which all parties referred was the Foreign Intelligence Surveillance Act ("FISA") (as amended). FISA authorises two types of surveillance. There are "traditional" FISA orders and surveillance pursuant to s. 702 of FISA.

169. Pursuant to the provisions of traditional FISA orders, government authorities must obtain individual orders from the FISA court (FISC) on an individualised basis to conduct electronic surveillance or physical searches as defined in the law. In order to obtain an order authorising electronic surveillance or physical search the government must demonstrate to the FISC "probable cause" that, among other things, the target is a "foreign power or an agent of a foreign power". These are principally foreign governments, international terrorist groups or proliferation networks and their agents. A "significant purpose" of the collection must be to gather "foreign intelligence information" which FISA defines as five specific categories of information that relate to the government's ability to protect against foreign attack, terrorism, proliferation of weapons of mass destruction and other threats **or to the conduct of the foreign affairs of the United States** (50 U.S.C. 1801 (e)). The breadth of the definition of foreign intelligence information was emphasised by both the DPC and Mr. Schrems.

170. Surveillance pursuant to s. 702 is fundamentally different. Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorise surveillance conducted within the United States by targeting non-US persons reasonably believed to be located outside the United States with the compelled assistance of electronic communication service providers in order to acquire foreign intelligence information. Persons who may be targeted under s. 702 cannot intentionally include US persons or anyone located in the United States. The targeting must be conducted to acquire foreign intelligence information as defined in the Act.

171. The joint authorisations of the Attorney General and the Director of National Intelligence must be approved by the FISC along with procedures governing targeting and the handling of information acquired (minimisation). Under s. 702 the Attorney General and the Director of National Intelligence make annual certifications

authorising this targeting to acquire foreign intelligence information without specifying to the FISC the particular non-US persons who will be targeted. There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power as generally required in the "traditional" FISA process. The certifications identify categories of information to be collected which must meet the statutory definition of foreign intelligence information. The FISC determines that the procedures are consistent with the statute and the Fourth Amendment of the Constitution. The privacy rights of non-US persons located outside of the United States are not protected by the Fourth Amendment.

172. The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-US person located outside the United States and that targeting this person will lead to the acquisition of foreign intelligence information. Minimisation procedures cover the acquisition, retention, use and dissemination of any non publicly available US personal information acquired through the s. 702 programme. They do not apply to non-US persons located outside the United States. Data may only be legally collected in compliance with the orders of the FISC authorising particular targeting and minimisation procedures for each individual agency engaged in collecting or receiving and sharing signals intelligence.

173. Once foreign intelligence acquisition has been authorised under s. 702 the practice is that the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government identifies or "tasks" certain "selectors", such as telephone numbers or email addresses. A named individual may not be tasked. The selectors are associated with the targeted persons. The government sends these selectors to the electronic

communications service providers who then provide the data to the relevant government agency.

174. An electronic communication service provider receiving a directive may file a petition to modify or set aside the directive with the FISC. The government or an electronic communication service provider may appeal a decision of the FISC to the Foreign Intelligent Surveillance Court of Review (FISCR).

175. Section 215 of the USA-PATRIOT Act, 2001 (50 USC s. 1861) is the second legal authority for surveillance programmes. It permits the Federal Bureau of Investigation (FBI) to make an application to the FISC for an order requiring a business or other entity to produce "tangible things", such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution (i.e. freedom of religion, freedom of speech, freedom of assembly). The application must include a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorised investigation to obtain foreign intelligence information. As with applications under s. 702, the application and court order will specify minimisation procedures to be followed upon receipt of the tangible things required to be produced pursuant to the court order.

176. Section 215 allowed for bulk collection of telephony metadata maintained by telephone companies to whom orders under s. 215 were addressed. The USA FREEDOM Act which was enacted on the 2nd June, 2015, prohibits the collection in bulk of records pursuant to *inter alia* s. 215 of the US-PATRIOT Act.

177. The FISC is staffed by federal judges with lifetime tenure appointed by the chief justice. Applications for authorisations are *ex parte* and are secret. The parties served with the directives issued under the authorisations are likewise bound to secrecy. Unless expressly declassified, all procedures under FISA are secret.

178. FISA governs the acquisition of signals intelligence within the United States in relation to non-US persons reasonably believed to be located outside of the United States. However, the primary authority under which the NSA acquires foreign intelligence is EO 12333. This applies to intelligence collections made outside of the United States. It is an executive order of the President of the United States. It is not law and may be revoked or amended at any time by the President. The activities of the NSA authorised by EO 12333 are not governed by statute, are not subject to judicial oversight, are not justiciable and there was no evidence in relation to any programmes conducted pursuant to EO 12333. The collection of intelligence must be for the purposes of foreign intelligence as defined in EO 12333. This is an extremely broad definition, wider than the definition in FISA: -

> *"**Information relating** to the capabilities, **intentions and activities of foreign** powers, organisations or **persons**, but not including counterintelligence except for information on international terrorist activity."* (emphasis added)

The order establishes limits in relation to the collection, retention or dissemination of information concerning US persons (as defined) acquired pursuant to the order. It has no such limits in respect of information concerning non-US persons, though this may be qualified by PPD-28, as discussed below.

179. While EO 12333 is not relied upon for intelligence collection within the United States, it does authorise the collection of data in transit to the United States and data transiting through the United States but never intended to arrive for processing within

the United States. This is referred to as transit authority. This means that the NSA may be authorised under EO 12333 to collect data from the deep underwater cables on the floor of the Atlantic by means of which data are transferred from the EU to the US for processing within the US before the data arrives within the US (and thus would be subject to the provisions of FISA). This means that the data of EU citizens in transit to the US may be accessed, acquired or retained pursuant to EO 12333. There was no evidence adduced in relation to any programme actually operated pursuant to EO 12333. There is no legal remedy for any actions of NSA pursuant to EO 12333.

180. The manner in which surveillance is actually conducted and data processed following acquisition is governed by Presidential Policy Directive – 28 (*"*PPD-28*"*). PPD - 28 applies certain principles to signal intelligence activities for the benefit of all persons whether United States persons or otherwise. Privacy and civil liberties are stated to be integral considerations in the planning of US signals intelligence activities. Signals intelligence is to be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes. Signals intelligence activities are required to be *"as tailored as feasible"*. PPD – 28 does not authorise any surveillance activities but establishes principles how authorised activities are to be conducted.

PRISM and Upstream

181. In order to appreciate how these laws may operate and may affect EU citizens it is useful to consider the evidence adduced based on declassified information in relation to two programmes operated by United States intelligence agencies pursuant to s. 702 of FISA.

182. In PRISM collection, the government sends a selector, such as an email address, to a United States based electronic communications service provider and the

provider is compelled to give the communications sent to or from that selector to the government. The NSA receives all data collected through PRISM. In addition, the CIA and the FBI each receive a select portion of the data collected through PRISM. A selector must be a specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number. People are targeted and selectors are tasked. Only selectors used by non-US persons reasonably believed to be located abroad may be tasked. The government estimates that 89,138 persons were targeted under s. 702 during 2013. In 2015 there were 94,368 persons targeted under s. 702. A decision of the FISC from 2011 reveals that the government acquired more than 250,000,000 communications under this programme.

183. Upstream differs from PRISM in several respects. The acquisition occurs with the compelled assistance of service providers that control the telecommunications backbone – the network of cables, switches and routers - over which telephone and internet communications transit, rather than with the compelled assistance of internet service providers or similar companies. Upstream collection includes telephone calls as well as internet communications. Through Upstream collection the experts said that the NSA copies and searches streams of internet traffic as data flows across the internet backbone.

184. Prior to April, 2017 the situation with regard to Upstream was as follows. NSA Upstream collection acquired internet transactions that were *"to"*, *"from"*, or *"about"* a tasked selector. With respect to *"to"* and *"from"* communications, the sender or a recipient is a user of a s. 702 tasked selector. This is not necessarily true for an *"about"* communications. An about communication is one in which the tasked selector is referenced within the acquired internet transaction, but the target is not necessarily a participant in the communication. Collection of *"about"*

communications involves searching the **content** of internet communications traversing the internet backbone which are subjected to Upstream surveillance. The internet transactions are first filtered to eliminate potential domestic transactions and then screened to capture only transactions containing a tasked selector. Transactions which pass both screening operations are acquired by the NSA. As of 2011, the NSA acquired approximately 26.5m internet transactions a year as a result of Upstream collection. Necessarily, this is a small portion of the amount of Internet transactions subjected to the filtering process and of the number of worldwide Internet communications.

185. Upstream also captures Multiple Communications Transactions (MCTs). MCTs are Internet transactions that contain more than one discrete communication within it. If a single discrete communication within an MCT is to, from or about a s. 702 tasked selector and, at least, one end of the transaction is foreign, the NSA will acquire the entire MCT. This may include communications between persons who have no connection whatsoever with the s. 702 target and are not themselves targets for surveillance for national security purposes or otherwise.

186. On 26th April,2017, the FISC released an opinion addressing the United States government's submissions seeking reauthorization to conduct surveillance under s.702 of FISA. The experts said that the opinion states that the government will not "acquire" or "collect" communications that are merely about a target but it does not indicate that the NSA has stopped copying and searching communications as they pass through its surveillance equipment prior to "acquisition" or "collection". The opinion left unchanged the government's long standing ability to query s. 702 data using non-US person identifiers. The opinion authorises the conduct of surveillance for a year and is

a binding decision of the FISC. The government will have to reapply for authorization next year.

Mass surveillance?

187. There was a dispute between Mr. Schrems on the one hand and Facebook and the United States on the other hand as to how surveillance by the United States intelligence agencies should be characterised. Facebook and the United States said that in practice the surveillance was very targeted; it was not indiscriminate and it was not mass surveillance. Mr. Schrems on the other hand pointed to the vast number of communications acquired pursuant to the PRISM programme and to the method by which UPSTREAM operated. Ms. Gorski, who gave evidence on his behalf, was of the opinion that UPSTREAM involved searching billions of Internet transactions crossing the internet backbone and this must be regarded as mass surveillance. She referred to the generalised access by the government of the United States to the content of communications under s. 702 Upstream surveillance.

188. The United States government acknowledges that in certain circumstances it collects signals intelligence in bulk and that it may result in the collection of information about persons whose activities are not of foreign intelligence or counter intelligence value (PPD-28, s. 2). It maintains that it is not engaged in mass or indiscriminate surveillance.

189. Service providers are required by law to comply with directions served upon them by the relevant agencies and thus potentially the intelligence agencies have access to all of the data held by the service providers as a matter of law and practice. Collection of data from the service providers pursuant to PRISM is targeted. An individual is the target. An email address or mobile phone number that is associated with the target is the selector and it is tasked and the service provider is directed to

provide the communications responsive to the selector. As stated above, in 2015 there were 94,386 targets. However, this can multiply up to a very large number of communications. Targets communicate with non targets. Targets can have multiple selectors. In 2011, the government acquired more than 250,000,000 communications under s. 702 surveillance. PRISM accounts for approximately 90% of s. 702 surveillance so it can be seen that starting with less than 100,000 targets can result in the acquisition of an extremely large number of communications indeed. Of course, it is fair to say, as was pointed out on behalf of Facebook, that this in itself, though large, constitutes a very tiny proportion of the total number of internet communications.

190. UPSTREAM operates differently. It necessarily involves making huge numbers of non relevant communications available for surveillance by the NSA. The NSA then searches this vast number of communications. It retains the communications which it "acquires" or "collects" from the vast number of communications to which it has access. It has access to the content as well as the metadata of these communications.

191. It is of course inherent in targeted searching that a large body of data is searched. The true difference between Mr. Schrems on the one hand and Facebook on the other hand, was the focus by Mr. Schrems on the making available and initial searching of billions of communications passing through the internet backbone, while Facebook focused upon the fraction of these communications which was actually acquired or collected and therefore subsequently retained and made available for analysis.

192. There is a distinction between bulk searching and bulk acquisition, collection or retention. In my opinion, the evidence clearly establishes that under UPSTREAM there is mass surveillance in the sense that there is mass searching of communications.

The search is for targeted communications and is in that sense not indiscriminate. Even when targeted it involves the collection of non relevant data as explained above.

193. The Directive defines processing of personal data as including any operation or set of operations which is performed upon personal data such as collection… or otherwise making available the data. On the basis of this definition and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, it is clear that there is mass indiscriminate **processing** of data by the Unites States government agencies, whether this is described as mass or targeted surveillance.

Evidence on Relevant Data Protection Law in the United States

194. One of the experts described data protection law in the United States as an overlapping and labyrinthine array of statutory and non-statutory authorities. It is a complex web of constitutional law, sector specific federal statutes, state statutes and common law rules. This section of my judgment necessarily is a summary of the evidence adduced at trial and does not purport to be an exhaustive or comprehensive statement of the laws of the United States in this area.

195. The basic principle is that surveillance is legal unless forbidden and there is no requirement ever to give notice in relation to surveillance.

196. Data protection and data privacy rights, whether express or implied are to be found in the First and Fourth Amendments to the Constitution. The First Amendment, which relates to freedom of speech, did not feature in the evidence at trial.

The Fourth Amendment

197. The experts identified the Fourth Amendment to the Constitution as being the most important protection against unlawful government surveillance. The Fourth Amendment applies to searches and seizures that take place within the US (such as on

data transferred to the US). The prevailing assumption is that, as the law currently stands, non-EU citizens lacking substantial voluntary connection with the United States (such as the majority of EU citizens) may not bring a Fourth Amendment case. Thus, the foremost protection under US law against unlawful government surveillance is not available to most EU citizens. They may benefit indirectly from the protections guaranteed by the Fourth Amendment to those entitled to its protections.

Individual remedies available to EU citizens under US law

A. 18 U.S.C. Section 2712 (Stored Communications Act)

170. Section 2712 (a) permits a person who is aggrieved by a "willful" violation of certain specific statutory provisions to sue for damages. It applies to the Wiretap Act and the Stored Communications Act (together the Electronic Communications Privacy Act) and to three sections of FISA.

171. These are 50 USC sections 1806 (a), section 1825 and section 1845. Section 1845 is of no relevance to Mr. Schrems' reformulated complaint.

Section 1806 (a) prohibits the use or disclosure by Federal officers or employees except for lawful purposes of information acquired from an electronic surveillance within the United States for foreign intelligent purposes.

172. Section 1825 prohibits the use or disclosure by Federal officers or employees except for lawful purposes of information acquired from physical searches within the United States for foreign intelligent purposes.

173. The court may award as damages (1) actual damages, but not less than $10,000, whichever amount is greater and (2) litigation costs reasonably incurred. "Willful" in the context of a claim for damages under s. 2712 (a) has been held to mean both knowing and reckless violations of the statute.

174. Section 2712 amounts to an express waiver of sovereign immunity for the government. Damages may be recovered from the government. It is an exclusive remedy against the United States. Therefore, no relief other than damages may be obtained for breaches of these provisions.

175. Because s. 2712 provides an exclusive remedy for damages against the United States, it precludes action under the Administrative Procedures Act (as discussed below) for any of the causes of action listed in s. 2712. It does not apply to ss. 1810 or 1861 of FISA (s. 215 of PATRIOT Act).

176. There are minimisation procedures and other provisions in relation to ss. 1806, 1825 and 1845 which concern only United States persons – defined as US citizens and lawful residents or US corporations. Therefore, EU citizens who are not US citizens or residents would not be able to bring a claim under s. 2712 for non-compliance with the minimisation procedures or these other provisions.

B. 50 USC Section 1810

177. Under s. 1810 an affected person (other than a foreign power or an agent of a foreign power) who has been subjected to electronic surveillance, or about whom information obtained by electronic surveillance of such person has been disclosed or used, in violation of the provisions of s. 1809 can recover

(1) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of the violation, whichever is greater;

(2) punitive damages and

(3) reasonable attorneys' fees and other costs .

178. Section 1810 is not included within s. 2712. It does not operate as a waiver of sovereign immunity which means that the United States cannot be held liable under the section. Any case must be brought against the individual actors. Under s. 1810 the disclosure must be in breach of s. 1809 which means the plaintiff must prove willful/intentional violation of the section. There have been no prosecution of officers or employees under s. 1809 and the section was described by Professor Vladeck on behalf of Facebook as very narrow and difficult to prove.

179. Even if a plaintiff under s. 1810 could prove willful violation the plaintiff must still overcome possible issues of sovereign immunity and official immunity. Because there is no waiver of sovereign immunity with regard to the United States, it is arguable that sovereign immunity may extend to officers acting in their official capacity. If it does not, officers may still rely upon official immunity. The test is: the officer must have violated clearly established law of which a reasonable officer would have known. It is clear that the liability is personal and therefore the head of an agency may be entitled to claim official immunity in respect of proceedings brought under s. 1810 (even if he or she cannot assert sovereign immunity).

180. Professor Vladeck accepted that both of these possible immunities may prove substantial obstacles to relief. On the other hand, he was of the opinion that if the plaintiff could prove his or her case, it was likely that the government would indemnify the individual officer.

C. 50 USC Section 1806

181. Claims brought for willful violation of s. 1806 (a) are brought under s. 2712. Section1806 (e) provides an exclusionary remedy for a person against whom evidence gained by electronic surveillance is being introduced in criminal or administrative proceedings. The person against whom the evidence is being introduced has the right

to bring a motion to suppress the evidence gained by electronic surveillance if it is shown that the information was unlawfully obtained or that the surveillance was not made in conformity with an order of authorisation or approval. It does not of itself provide a remedy for unlawful processing of personal data.

182. To date, only eight criminal defendants have received notices of s. 702 surveillance. The only adversarial rulings by US courts on the legality of surveillance under FISA s. 702 to date have come through s. 1806 motions to suppress.

D. Electronic Communications Privacy Act (ECPA)

183. The Electronic Communications Privacy Act governs when electronic communications and wire communications can be intercepted or monitored. It is an exceptionally complex piece of legislation. It consists of the Wiretap Act and the Stored Communications Act (SCA). The Wiretap Act applies to the interception or accessing of information while in transmission. The SCA applies to the unauthorised access of stored communications. Remedies under the ECPA are generally available to both US citizens and foreign nationals and non citizens are entitled to protections of the ECPA. It is unclear whether suits can proceed against the agencies themselves in addition to the individual officers.

184. Section 2712 confers a cause of action for willful violation of the Wiretap Act or the SCA. Under the Wiretap Act it is a crime for persons to intentionally *intercept* or *procure* electronic communications, including email, unless certain exceptions apply. It is a violation of the Wiretap Act to *disclose* communications if the person making the disclosure knew or had reason to know that the communication was intercepted in violation of the ECPA.

185. Under the SCA it is illegal to obtain, alter or prevent authorised access to a wire or electronic communication while it is in electronic storage in such system if a person

"intentionally accesses without authorisation a facility through which an electronic communication service is provided" or "intentionally exceeds an authorisation to access that facility".

186. Claims for damages under the Wiretap Act or the SCA apply to wrongful collection and not just use and disclosure.

E. Privacy Act and Judicial Redress Act

187. The Privacy Act allows US citizens to access their records or information pertaining to those individuals held by governmental agencies and to review those records and have copies made. The head of any agency may promulgate rules to exempt certain systems of records from the Act. There is no blanket exemption for records collected by a particular agency. However, there are regulations prohibiting the disclosure of records pertaining to the functions and activities of the NSA. All systems of records maintained by the NSA are exempt from disclosure to the extent that the system contains information properly classified under an executive order and that is required by executive order to be kept secret in the interest of national defence or foreign policy. Thus, the NSA has exempted itself from the most significant protections afforded to individuals. As the NSA is the primary agency responsible for foreign intelligence signals gathering, this means that the Privacy Act for all practical purposes is likely to provide no remedy to an EU citizen.

188. In any event, it is necessary to establish that the disclosure was intentional or willful and that the disclosure had an adverse effect on the plaintiff. It is necessary to establish pecuniary loss and damage. Non economic harm is insufficient. *Federal Aviation Authority. v. Cooper* 137 S.Ct. 1441 (2012)

189. The experts stated that Privacy Act suits face numerous hurdles including subject matter exemptions, classified documents, the "routine use" exception, *F.A.A. v.*

Cooper limiting damages and most importantly the exemption of national security records from the coverage of the Privacy Act.

190. The Judicial Redress Act extended the protections of the Privacy Act to the covered records held by designated agencies in respect of covered countries. As of the 1st of February, 2017, all EU countries, with the exception of the United Kingdom and Denmark, are covered countries for the purposes of the Judicial Redress Act. However, the NSA is not a designated agency for the purposes of the Act therefore citizens of the EU may not bring a Privacy Act/JRA suit against the NSA.

191. There are also issues concerning the definition of covered records and covered countries which means that data initially transferred to a private company in the US and then acquired by a US government agency may not be a covered record. As the United States is not defined as a covered country, this may mean that sovereign immunity has not been waived with the result that any suit against any agency would be barred by a plea of sovereign immunity.

192. On the 25th of January, 2017, a new executive order on the topic of immigration was issued by President Trump. Section 14 states: -

> "*Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residence from the protection of the Privacy Act regarding personally identifiable information."*

The legal effect of the executive order is uncertain. The experts agree that the provision is a change in policy from the previous administration which had expanded the number of agencies that applied administrative Privacy Act protections to mixed systems of records (databases containing both US and non-US person information).

This order has been superseded as of the date of judgment but no evidence was given of the terms of the latest version of this executive order.

193. In practice it is extremely unlikely that the Privacy Act will afford a remedy for breaches of data protection to an EU citizen.

Administrative Procedure Act

5 U.S.C. Section 702

194. Only Professor Vladeck placed emphasis on the Administrative Procedure Act as a possible source of remedy. It was not referred to by Professor Swire who gave evidence on behalf of Facebook or Mr. Robert Litt in his letter to the Commission included as an annex to the Privacy Shield Decision. Professor Richards and Mr. Serwin who gave evidence on behalf of the DPC both discounted it as a meaningful avenue of redress for EU citizens.

195. The Administrative Procedure Act is precluded if a plaintiff has a remedy under an alternative statutory provision. By reason of the provisions of s. 2712 this means that the Act is precluded in relation to suits brought pursuant to the Wiretap Act, the SCA and ss. 1806, 1825 and 1845 of FISA. Claims under FISA 1810 and 1861 (s. 215 PATRIOT Act) are not precluded from the Administrative Procedures Act as discussed above.

196. The Act provides that *"any person suffering legal wrong because of agency action or adversely affected or aggrieved by agency action is entitled to seek judicial review."* Even where the Act applies the remedies available are subject to limitations. A plaintiff must establish that he or she falls within "the zone of interest" of the Act and that the action complained of is "a final agency action". It is not clear whether monitoring a particular individual's communications for the purposes of national security is "a final agency action" under the APA, but Professor Vladeck believes that

a directive to a service provider would qualify as a final agency action. He adduced no authority to support this opinion. A plaintiff may obtain injunctive or declaratory relief (provided the complained of action has not ceased) but not damages under the APA.

Standing

197. While there are a variety of possible judicial remedies open to EU citizens in respect of possible unlawful processing of their private data by United States agencies as I have set out, in all cases it is necessary for a plaintiff to establish that he or she has standing to bring the suit. This is a very complex matter in the context of secret government surveillance. All of the evidence show that it is an extraordinarily difficult hurdle for a plaintiff to overcome. It constitutes a substantial obstacle to maintaining any of the causes of action discussed.

198. Under Article III of the US Constitution, a plaintiff must have standing to bring suit before a federal court as a precondition to bring a claim. The party invoking federal jurisdiction bears the burden of establishing the following three elements:

(1) that it has suffered an injury in fact – an invasion of a legally protected interest which is (a) concrete and particularised and (b) actual or imminent, not conjectural or hypothetical;

(2) That there is a causal connection between the injury and the conduct complained of – the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court;

(3) That it is likely, as opposed to merely speculative, that the injury will be redressed by a favourable decision.

199. In *Clapper v. Amnesty International* US, 133 S.Ct. 1138 [2013] the Supreme Court considered the imminence test of "injury in fact" in the context of alleged

unlawful surveillance by the Director of National Intelligence of the communications of the plaintiffs. The court held that it meant "certainly impending". It rejected the formulation of the Second Circuit that "objectively reasonable likelihood" that communications will be interfered with was sufficient to meet the test of "injury-in-fact".

200. This decision makes it more difficult for plaintiffs to establish standing in the absence of express notice that they personally have been surveilled. This is particularly significant as there is no notification obligation. The experts agreed that in the absence of notice that a plaintiff has been the subject of surveillance (and thus his data processed), it would be very difficult to challenge that surveillance. In the vast majority of cases persons surveilled will never receive notice of the fact –and therefore they will not be in a position to challenge the surveillance both because of their ignorance of a possible claim and their inability to establish standing as required by *Clapper*.

201. The application of the test depends upon what is called the posture of the case. A plaintiff's standing to sue can be challenged on the basis of the pleaded case by a motion to dismiss, in which case the plaintiff is required to show that he has plausibly pleaded his case in order to survive the motion to dismiss. The facts are assumed in his favour but they must amount to a legal wrong, if proven. His standing may also be challenged by a motion for summary judgment. If that occurs, it is not sufficient for the plaintiff to plead plausible allegations; he must adduce evidence to support his claim and if he fails to do so his action will be dismissed.

202. *Clapper* was an application for summary judgment and the plaintiffs failed because they failed to prove facts that the injury alleged was imminent.

203. *Wikimedia Foundation v NSA* (4th Cir. 15-2560) was a decision of the Fourth Circuit of Appeals on a motion to dismiss the claims of the plaintiffs delivered on 23 May, 2017. Wikimedia engages in more than 1 trillion international communications a year in almost every country on the globe. It challenged the Upstream programme pursuant to s. 702 based on the manner in which Upstream operates as acknowledged by the PCLOB report, the vast number of its communications and the geographical diversity of the people with whom it communicates. It said its communications almost certainly travers every international backbone link connecting the United States with the rest of the world. If the NSA is monitoring a single internet backbone link then the NSA is intercepting, copying and reviewing at least some of its communications. Wikimedia. The court held that Wikimedia had plausibly alleged that its communications travelled all of the roads that a communication can take and that the NSA seizes all of the communications along at least one of those roads. It therefore had standing at a motion to dismiss stage to sue for a violation of the Fourth Amendment.

204. The court emphasised the importance of the distinction between motions to dismiss and summary judgments in determining whether the plaintiff had standing to sue. The court held that Wikimedia had standing as it had pleaded an actual and ongoing injury. Because it pleaded an actual injury, the analysis of an impending injury set out in *Clapper* did not apply. On the other hand the court held that none of the other plaintiffs had plausibly pleaded a case – their case was different to that of Wikimedia- and therefore dismissed their claims at the motion to dismiss stage of the proceedings.

205. In addition to proving that the complained of wrong had occurred (actual) or was imminent, a plaintiff must also satisfy the "concrete and particularised" limb of the test. "Particularised" means that it affects the plaintiff in a personal and individual way.

"Concrete" means that the harm may not be hypothetical. It must be real not abstract. It may be intangible and still concrete, but a bare procedural violation of a statutory right is not sufficient. (See *Spokeo v. Robbins*) 135 S. Ct. 1892 (2016) Therefore a simple violation of an individual's statutory right may not be sufficient of itself to establish standing.

206. Interference with data was accepted by the court as sufficient to establish standing for the purposes of a claim for a violation of the Fourth Amendment in *Wikimedia*. The experts disagreed whether *Spokeo* meant that a plaintiff suing for violation of a statutory right would be required to show more than interference with his data in order to satisfy the concrete limb of the test for standing ie whether he was required to show damage. In *FAA v Cooper* 1320S. Ct 1441 (2012) the Supreme Court held that for a claim under the Privacy Act the plaintiff was required to prove pecuniary loss.

207. The experts all agreed that standing is notoriously indeterminative and that it is possible to find cases across a range of possibilities. Many cases have been dismissed for want of standing and others have not. There is significant uncertainty in the federal district courts over exactly when *Clapper* does and does not foreclose standing. There was a dispute among the experts as to the degree of the uncertainty and thus the difficulty in establishing standing. The experts agree that the government failure to notify individuals subject to its secret surveillance programs makes it more difficult for plaintiffs to establish standing.

208. The difficulties with regard to standing can be illustrated by two recent decisions. In *ACLU v. Clapper*, 785F3d 787 (2nd Cir. 2015) the second circuit was concerned with a s. 215 programme which authorised the collection of all of the metadata of all of the customers of Verizon in the United States. The FISC had

authorised this metadata programme on 41 occasions pursuant to s. 215 of the PATRIOT Act. Edward Snowden leaked the actual FISC order and it was thus clear that it applied to all customers of Verizon. ACLU was a customer of Verizon. Thus, it was able to satisfy the test for injury in fact as set down in *Clapper v. Amnesty International* as it could show an actual injury and not an imminent injury.

209. But for the fact the particular programme collected the data of **all** of the customers of Verizon, ACLU might not have been able to satisfy the test for standing in light of the decision in *Clapper v. Amnesty International*.

210. The case highlights the significance of the absence of notice. ACLU had no notice of the metadata programme and therefore was unaware of the fact that it was subject to surveillance and could not sue in respect of the surveillance. It was only as a result of the illegal leaks of Mr. Snowden that it became aware of the surveillance and that it had a possible cause of action.

211. The case also illustrates the importance of judicial review. The second circuit struck down the metadata programme in its entirety on the basis that it exceeded the statutory authorisation for such surveillance (to obtain foreign intelligence). This was so even though the programme had received prior authorisation from the FISC on 41 occasions.

212. It underscores the importance of remedies to protect the rights of individuals, not just the particular plaintiff. If the case had not been brought, the programme would not have been declared unlawful and the surveillance of millions of persons could have continued unchallenged. Incidentally, it should be noted that the case was brought on the basis of the Administrative Procedure Act and the Fourth Amendment, and an EU citizen would have been confined to the action under the APA, with all the technical difficulties involved in bringing forward such a claim.

213. The second case is *Wikimedia.* Wikimedia was held to have standing at the motion to dismiss stage of the proceedings because it could plausibly allege that its communications were so vast that they must travel **all** the roads that a communication can take **and** that the NSA seizes **all** of the communications along at least one of those roads. There will be very few other plaintiffs able to advance such acclaim. On the other hand the other plaintiffs, who included Amnesty International, Human Rights Watch and the National Association of Criminal Defense Lawyers, were held not to have standing even at this stage of the proceedings. Their case was that the NSA is intercepting "*substantially all*" text-based communications entering and leaving the United States. However, they could not assert enough facts about Upstream's operational scope to plausibly allege a dragnet that must capture their communications and, following *Clapper*, an *"objectively reasonable likelihood"* that their communications would be intercepted was not sufficient.

Systemic Safeguards and Oversights

214. The FISC oversees the activities of the agencies who obtain orders for the collection of data under s. 215 or the annual certifications that provide the basis for collection of data under s. 702. As stated above, there is no judicial approval of individual selectors to query the data collected under s. 215 or tasked for collection under s. 702. The FISC operates *ex parte* and in secret. Its orders and opinions are classified, unless they are declassified. Increasingly, more material has been declassified. There is no judicial oversight of the collection of foreign intelligence outside the US, including pursuant to transit authority, under executive order 12333.

215. The FISC (and the FISCR) is supported by a standing panel of five individuals that have an expertise in national security matters as well as civil liberties. From this group the court may appoint an individual to serve as an a*micus curiae* to assist in the

consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law. This ensures that there can be a suitably qualified interlocutor to engage with the government on what would otherwise be *ex parte* applications.

216. Professor Swire on behalf of Facebook gave evidence of the fact that the FISC has in the past refused to authorise certain programmes, has rigorously scrutinised the targeting and minimisation procedures and issues of non-compliance with these procedures which have been reported to the court. Where data has been obtained without due authorisation, the FISC has directed the destruction of the data.

217. The opinion of the FISC of 26 April, 2017 illustrates very close scrutiny by the FISC of the applications for certificates pursuant to s. 702 of FISA. The court is required to ensure that the requirements of the statute are satisfied and that procedures are reasonable in light of the Fourth Amendment. The opinion also illustrates the court monitoring and supervising compliance with its orders. The opinion referred to "significant non-compliance with NSA minimization procedures" which it said were widespread. It detailed a number of violations of earlier orders by the FBI and the CIA. It said that the NSA had failed to give the court timely notice of the issue and revealed "an institutional lack of candour" and emphasised that this was a very serious Fourth Amendment issue. The government was forced to end "about" collection under Upstream in light of the non-compliance with the previous procedures which protected the privacy of US persons.

218. The US intelligence agencies are subject to various review and oversight mechanisms. According to PPD-28, s. 4 (a) (iv), the policies and procedures of the intelligence community elements *"… shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information…"*.

These measures include periodic auditing. Multiple oversight layers have been put in place including civil liberties or privacy officers, Inspectors General, the office of the Director of National Intelligence Civil Liberties and Privacy Office and the President's Intelligence Oversights Board**.**

219. The civil liberties or privacy officers supervise procedures to ensure that the relevant agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints. Each agency has its own Inspector General with responsibility to oversee foreign intelligence activities. They are authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority in connection with Office of the Director of National Intelligence (ODNI) or the programmes or activities of agencies. Inspectors General may issue non-binding recommendations for corrective action. Their reports are made public and sent to Congress. Civil liberties and privacy officers periodically report to Congress and the PCLOB.

220. The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency within the executive branch composed of five presidential appointees. It receives reports from the civil liberties and privacy officers of several departments and agencies and regularly reports to congressional committees and the President. Currently and for some months it has only one member and is inquorate.

221. In addition, the Department of Justice and the Department of Defence each provide extensive oversight of intelligence activities. In the NSA alone there are over 300 employees dedicated to compliance issues.

222. Agencies are required to report incidents of non compliance with the rules and procedures authorising the collection of signals intelligence. The reports are to the head of the particular intelligence community element, the Director of National

Intelligence and the Intelligence Oversight Board. This is to ensure that an issue will be addressed at the highest level. They are also reported to FISC.

223. In considering the weight to be attached to these extensive provisions it is worth bearing in mind the limitations which have been shown to exist notwithstanding the best efforts of those concerned in carrying out this very extensive oversight of the intelligence agencies. It is apparent from the opinion of the FISC of 26 April, 2017 that it is dependent upon the agencies acting promptly and with candour, something that may, at times, be lacking. In this regard, I should note that the FISC authorised the revised targeting and minimization procedures despite the reported instances of non-compliance with prior orders of the court based largely on "the extensive oversight conducted within the implementing agencies" and by the Department of Justice and ODNI. It held that "due to those efforts, it appears that compliance issues are generally identified and remedied in a timely and appropriate fashion". Further, it should be remembered that the programme that was struck down in *ACLU v Clapper* on the basis that it far exceeded what was authorised by the statute had been authorised by the FISC on 41 occasions.

224. In addition to executive oversight mechanisms, the US Congress, specifically the House and Senate Intelligence and Judiciary committees, have oversight responsibilities regarding all US foreign intelligence activities, including US signals intelligence. The President is obliged to keep the congressional intelligence committees fully and currently informed of the intelligence activities of the United States including any significant anticipated intelligence activity. The President is to ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees as well as any corrective action that may have been taken or is

planned in connection with such illegal activity. The oversight committees have subpoena power and access to classified information.

225. The USA FREEDOM Act 2015 requires the government to disclose to Congress and the public each year the number of FISA orders and directives sought and received as well as estimates of the number of US and non-US persons targeted by surveillance. There has been an increased emphasis on declassifying the opinions of the FISC and the targeting and minimisation procedures adopted by the respective agencies pursuant to the orders of the FISC.

Conclusions in Relation to the Evidence Regarding Remedies

226. There are a variety of very significant barriers to individual EU citizens obtaining any remedy for unlawful processing of their personal data by US intelligence agencies.

227. Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no judicial or administrative avenues for data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.

228. The necessity for a plaintiff to establish that he has standing to sue constitutes a very substantial obstacle to any legal remedy. *Clapper v. Amnesty International* has made it exceedingly difficult to challenge secret government surveillance programmes, according to Professor Swire, who gave evidence on behalf of Facebook. Establishing an objectively reasonable likelihood that one has been the subject of surveillance is insufficient to satisfy the standing requirement. (*Clapper v. Amnesty International*, *Wikimedia v. NSA*).

229. The absence of express notice makes it even more difficult to meet the threshold for standing set by the Supreme Court in *Clapper v. Amnesty International* (see *Wikimedia* in contrast to *ACLU v. Clapper*) even if the plaintiff believes that it is highly likely that their data have been or will be accessed and/or acquired by one or more of the US intelligence agencies.

230. Under FISA, the personal data of an EU citizen can be seized, accessed and retained by a US government agency without the agency proving probable cause prior to obtaining a warrant in respect of the individual EU citizen from the FISC. There is no need to obtain any authorisation for surveillance conducted under EO 12333.

231. By far the most significant avenue of redress for unlawful interference with personal data is a claim for violation of the provisions of the Fourth Amendment. Such a claim is not open to EU citizens lacking a substantial voluntary connection with the US.

232. There are a number of possible causes of action potentially open to EU citizens in respect of processing of their data by government intelligence agencies in the United States, but on closer analysis it becomes clear that there are substantial obstacles to recovery in respect of some causes of action such that in reality an EU citizen is most unlikely to obtain a remedy for unlawful acquisition or processing of his personal data (actions under the Privacy Act or s. 1810 of FISA). A motion to suppress evidenced to be adduced in a criminal trial pursuant to s. 1806 of FISA is not a general remedy for wrongful interference with personal data. This in effect leaves claims for damages under s. 2712 of ECPA or claims under the APA. Some causes of action require the plaintiff to establish that he or she has suffered damage, which has been held to mean pecuniary damage. This is a significant limitation on the right to seek a remedy that does not apply under EU law. In *Schrems* para. 89 the CJEU noted that it has

repeatedly stressed that to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the person concerned has suffered any adverse consequences on account of the interference.[4] For claims under s. 2712 a plaintiff is required to prove a willful violation of the statute by an individual actor. How difficult this may be will obviously depend upon the facts of the case.

233. A claim under the APA only lies if there is no other statutory claim available. This rules out many potential cases. Even where the claim is not precluded, there is uncertainty whether it extends to collecting, processing or retaining the data of a particular individual.

234. In my opinion, despite the number of possible causes of action, it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by its intelligence agencies. On the contrary, the individual remedies are few and far between and certainly not complete or comprehensive.

235. I accept the conclusion of Professor Vladeck that retrospective judicial remedies will likely be unavailing to victims of governmental overreaching in the conduct of surveillance for the purpose of national security.

227. Quite clearly there are extensive rules to ensure that data is obtained in accordance with law and data, once obtained, is not misused. This is not the same as of providing a remedy where the rules are broken and data is unlawfully collected or otherwise misused. Protections against excessive or inappropriate surveillance are essential to an acceptable system of State surveillance. It is vitally important to ensure that secret surveillance does not exceed what society deems to be the appropriate limitations for such surveillance. But no system can ever be perfect. This is clearly illustrated by the FISC opinion of 26 April, 2017. There is a fundamental difference

[4] See also *Digital Rights* and *Watson*

between protections and safeguards on the one hand and remedies on the other. A protection cannot be a remedy though obviously the better the protection the less likely it is that a recourse to a remedy will be required. A remedy is to be available when the protections have in a sense failed.

228. Professor Swire gave as his opinion that it is sometimes difficult to provide individual remedies in the intelligence setting because of the risk of revealing classified information to hostile actors. He stated *"the desirability of individual remedies, in intelligence systems must be weighed against the risks that come from disclosing classified information"*

229. Article 52 of the Charter requires that the essence of the right be respected. In this case, the essence of the right under Article 47 of the Charter is the right of an individual to an effective remedy before a tribunal. The question of the desirability of individual remedies as referred to by Professor Swire does not arise if the essence of this right is not protected.

Article 47 of the Charter

(I) Is it Engaged?

256. The DPC in considering Mr. Schrems' reformulated complaint did not conduct an adequacy assessment in respect of the laws of the United States in relation to data protection and privacy. She conducted an inquiry into the essence of Mr. Schrems' rights under Article 47 of the Charter and then considered whether the essence of the rights guaranteed by Article 47 of the Charter were protected when his personal data were transferred by Facebook to Facebook Inc. and thereby made available to be processed by the United States intelligence agencies.

257. This approach was heavily criticised by Facebook, the government of the United States and two of the other a*mici curiae.*

Submissions of Facebook

258. Facebook argued that the DPC had not analysed whether there was any infringement of Mr. Schrems' fundamental rights and freedoms guaranteed under Articles 7 and 8. It submitted that this was a precondition to any question of a right under Article 47 arising and that therefore her entire analysis was flawed and must be rejected.

259. It seems to me that this argument is inconsistent with the requirement that each right under consideration (in this case the right to an effective remedy in the event that there is a breach of the protection of the data privacy rights of EU citizens whose data are transferred to the United States) must be individually assessed and the requirements of each Article engaged must be satisfied. This was emphasised by both the Advocate General and the court in *Schrems* (opinion para. 170 and 173; ruling paras. 94-95) and the Advocate General in *Digital Rights* (paras 60 – 61). The case was predicated upon the question that, insofar as there are breaches of EU citizens' data protection rights in the US, do the EU citizens have the same type of effective remedy before an independent and impartial tribunal of the type envisaged by Article 47 in the United States? Therefore, it is this question which must be addressed.

260. Facebook argues that Article 47 applies to rights and freedoms guaranteed by the law of the Union. It submits that the national security of the individual member states remains the sole responsibility of each member state (Article 4 of TEU). It follows, according to Facebook, that Article 47 is not engaged at all.

261. In addition, Facebook argues that if the actions complained of in these proceedings occurred in a Member State there would be no question of an Article 47

right to an effective remedy as the Charter would not apply to the actions of a Member State in the area of national security. On that basis, it says, the laws and practices of the United States cannot fail the essential equivalence test enunciated by CJEU in *Schrems*.

Discussion

262. It seems to me that these submissions are incorrect. In *Schrems* it was accepted by the Advocate General and CJEU that Article 47 applied notwithstanding the fact that the interference with personal data of EU citizens in question resulted from surveillance by the United States intelligence services. At para. 173 of his opinion, Advocate General Bot noted that the referring court found that in the United States citizens of the Union have no effective right to be heard on the question of the surveillance and interception of their data. He considered that this amounted to an interference with the rights of citizens of the Union to an effective remedy, protected by Article 47 of the Charter. The CJEU likewise considered that Article 47 applied in the circumstances of that case (see para. 95). The Court, in those circumstances, had no difficulty in applying the essential equivalence test.

263. In *ZZ v. Secretary of State for the Home Department* [2004] EWCA Civ 1578 the CJEU considered a decision of the United Kingdom refusing a citizen of the European Union admission to the United Kingdom on public security grounds. The Directive engaged in that case was Directive 2004/38/EC which concerned the freedom of movement of persons and the question referred related to the interpretation of Article 30 (2) of the Directive read in the light in particular of Article 47 of the Charter. At para. 38 the court stated: -

> *"... although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision*

concerns State security cannot result in European Union law being inapplicable"

ZZ was concerned principally with the application of Article 47 of the Charter in the context of a decision by the relevant authorities not to disclose information to ZZ on the grounds of national security. Thus, it is clear that as a matter of principle Facebook's argument in this regard is incorrect.

264. Finally, it should not be lost sight of that the transfers of data to which Mr. Schrems objects are the transfers by Facebook to Facebook Inc. in the United States and clearly EU law is engaged in respect of these transfers. He thus has the benefit of the fundamental rights and freedoms guaranteed to him by the Charter including the rights guaranteed under Article 47. This applies even though the processing which may give rise to a claim is that which may arise from subsequent interference with his personal data by intelligence agencies of the United States.

265. For these reasons, I believe that Article 47 of the Charter is engaged in these proceedings.

(II) Do the laws of the United States respect the essence of Article 47?

Submissions of the DPC

266. The DPC submits that, pursuant to Article 47, everyone whose rights and freedoms guaranteed *inter alia* by Articles 7 and 8 of the Charter and of the Directive are violated, has the right to an effective remedy before an independent and impartial tribunal. It was accepted by all parties that, pursuant to Article 52 (1) of the Charter, this right could be limited. Any limitation on the exercise of the right must be provided for by law and respect the essence of the right and freedom.

267. The DPC says that US law does not respect the essence of the right guaranteed by Article 47 to an effective remedy before an independent tribunal and that therefore it is not necessary to conduct a proportionality assessment of US law.

268. The DPC submits that there is an absolute requirement on intelligence agencies who have, in one way or another, surveilled the data of EU citizens to notify the persons affected as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities: - (*Watson* para.121).

> *"Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed This is so as notification is in fact necessary to enable the persons, affected to exercise their right to a legal remedy*."

269. While *Watson* is a decision of CJEU on Article 47 of the Charter, the reasoning reflects the jurisprudence of ECHR. In *Zakharov v. Russia* (case 47143/06) [2015] ECHR 1065 the ECHR considered secret surveillance laws in Russia in a case brought by a journalist who believed, but could not prove, that he had been the target of surveillance by state authorities. At para. 287 the ECHR held as follows: -

> *"It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual*

affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. ***As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned****… In the cases of Association for European Integration and Human Rights and Ekimdzhiev and Dumitru Popescu (no. 2), the Court found that* ***the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective****… in the case of Kennedy the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications."* (emphasis added)

270. Article 52 (3) of the Charter provides that insofar as the Charter contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights shall be the same as those laid down by that Convention. The provision does not prevent Union law from providing more extensive protection. In this case Article 13 of the Convention provides the right to an effective remedy which corresponds to Article 47 in the Charter. It follows therefore that Article 47 cannot be interpreted as providing for a lesser remedy than Article 13 of the Convention as expounded in the jurisprudence of the ECHR.

271. The DPC submits that US law never requires that the subject of surveillance receive notification at any time of the surveillance. She argues that this is critical to the right to an effective remedy as guaranteed by Article 47 of the Charter. It was accepted by the experts on the law of the United States that most people never know that they have been the subject of surveillance and if they do not know that effectively they can never sue. Thus, the DPC agrees with the conclusion of Professor Brown in Brown et al. "Towards Multilateral Standards for Surveillance Reform", (2015) that US law does not satisfy the requirements of the ECHR in relation to Article 13 and thus does not satisfy the requirements of Article 47.

272. Secondly, the DPC submits that the essence of an Article 47 right is a right to the possibility of a judicial remedy or at the very least a remedy from an independent tribunal. She argues that the law in relation to standing in the United States makes it extremely difficult to establish standing for an EU citizen who alleges interference with his personal data. Professor Swire accepted that it would be exceedingly difficult to challenge secret surveillance by government agencies for EU citizens and Professor Vladeck stated that it was likely that retrospective judicial remedies will be unavailing.

273. This is to be contrasted with the situation under European Union law. In *Verholen v. Sociale Verzekeringsbank Amsterdam* (Cases C-87/90, C-88/90 and C-89/90) [1991] E.C.R. I-3757 para. 24 the ECJ held: -

> *"While it is, in principle, for national law to determine an individual's standing and legal interest in bringing proceedings, Community law nevertheless requires that the national legislation does not undermine the right to effective judicial protection and the* ***application of national legislation cannot render virtually impossible the exercise of the rights conferred by Community law****."* (emphasis added)

274. In *Unibet (London) Ltd and Unibet (International) Ltd v. Justitiekanslern* (Case C-432/05) [2007] E.C.R. I-2271 the ECJ noted at para. 43 that: -

> *"... the detailed procedural rules governing actions for safeguarding an individuals' rights under Community law...****must not render practically impossible or excessively difficult the exercise of rights conferred by Community law****..."*(emphasis added)

275. The DPC says the effect of the rules of standing in the United States is to make the bringing of cases practically impossible or excessively difficult and that this effectively undermines the right to effective judicial protection. She submits that this fails to respect the essence of the fundamental right to an effective remedy guaranteed by Article 47.

276. She also argued that the US rules with regard to standing were more stringent than those accepted by the ECHR and this had the effect of rendering the remedies available under US law theoretical and illusory rather than practical and effective. In *Zakharov* the court summarised the case law of the ECHR and at para. 171 concluded: -

"*The Court accepts that an* ***applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures****, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies…. **where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance**, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential*

users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law in abstracto, is justified. ***In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be***

> ***a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.****"* (emphasis added)

277. It is submitted by the DPC that this test is far more liberal than the test to be found in the United States in cases such as *Clapper v. Amnesty International* and *Wikimedia*. Thus, the United States rules on standing in the area of national security are far more stringent than those established by ECHR.

278. The DPC highlighted the fact that the most important cause of action available in the United States to challenge unlawful interference with personal data, claims for a breach of the Fourth Amendment, are not available to EU citizens who do not have substantial voluntary connections with the United States and therefore are not available to the vast majority of EU citizens.

279. She also points to the extremely limited nature of the statutory remedies available to EU citizens and concludes that for all of the above reasons, the essence of the right to an effective remedy before an independent and impartial tribunal is not respected by the laws of the United States in the context of interference with the personal data of EU citizens by intelligence agencies on the grounds of national security. [5]

Submissions of Facebook and the United States

280. Facebook and the government of the United States argued that it was not appropriate to focus solely on the question of individual redress in the United States. They each urged that it was essential to consider the totality of the regime in relation to the authorisation of surveillance, the practice of targeting selectors, the minimisation

[5] I shall consider the Ombudsperson mechanism in the Privacy Shield decision below.

procedures, the multiple levels of oversight to ensure compliance with procedures, the procedures governing the acquisition of data, the storage of data, access by individuals and agencies to the raw data, retention and dissemination of the data.

281. They submitted that the essence of the Article 47 right was respected as EU citizens had available individual causes of action for substantive remedies before the courts in the United States. They emphasised that the CJEU in *Schrems* at para. 95 had established that it was only if there was *no possibility* of a remedy before a national court that the essence of the Article 47 right to an effective remedy was not respected. This is not the case in the United States and therefore the essence of the Article 47 right was respected.

282. In addition, they submitted that the DPC had overstated the difficulties of establishing standing in the United States and that, in essence, if an EU citizen had notice that he or she had been surveilled that he or she would likely have standing to sue for relief under one or more of the statutory remedies on the basis of *ACLU* and *Clapper v. Amnesty International*.

283. That being so, Facebook and the United States urged that a proportionality assessment is required before it can be said that any limitation on the exercise of a right or freedom recognised by the Charter is impermissible.

284. Facebook argued that when looking at the processing of data for the purposes of national security one does not look at the rights enshrined in the Directive. The test is not whether there is a high level of protection or an adequate level of protection or sufficient safeguards. The question is whether the interference with the rights of the data subject for national security purposes exceeds that which is strictly necessary and proportionate. Are the measures strictly necessary to achieve the objective of preserving national security?

285. Facebook referred to ECHR jurisprudence which has jurisdiction in the field of national security. It submitted that the case law establishes that when considering remedies in the context of national security, the court will consider the entire regime in the particular jurisdiction. It recognises that the concept of an effective remedy cannot carry the same meaning in the context of secret intrusive measures because the efficacy of such measures depends upon their remaining secret. Therefore, an effective remedy within the meaning of Article 13 of ECHR must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance (see *Klass v. Germany* (App. No. 5029/71) [1978] 2 EHRR 214 para. 69.)

286. Facebook noted that in *Silver v. The United Kingdom* (1983) 5 EHRR 347 at para. 113 the court synthesised the principles on the interpretation of Article 13 of ECHR to include the following: -

> "*… (a) where an individual has an arguable claim to be the victim of a violation of the rights set forth in the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress,*
>
> *(b) the authority referred to in Article 13 may not necessarily be a judicial authority but, if it is not, its powers and the guarantees which it affords are relevant in determining whether the remedy before it is effective,*
>
> *(c) although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so."*

287. Facebook submitted that the aggregate of the protections and remedies available in the United States provides an effective remedy as required by Article 47 of

the Charter. It referred to the authorisation by the FISC of the annual certifications in respect of each of the intelligence agencies, the ongoing oversight exercised by the FISC in respect of the individual agencies, the multiple levels of oversight both within the agencies, the Department of Justice, the ODNI, the Directors General as well as Congressional oversight. It said that the scope of the individual remedies available in the US to EU citizens must be seen in this context of oversight before, during and after acquisition of personal data. When viewed in this way, it is clear that US law and practice provides greater protections to EU citizens in respect of their personal data than is in fact available to them in practice in individual Member States within the EU. The limitations on the data protection rights of EU citizens in the circumstances satisfy the strictly necessary threshold and genuinely meet objectives of general interest recognised by the Union and are needed to protect the rights and freedoms of others as required by Article 52 (1) of the Charter.

Response of the DPC

288. In response, the DPC argued that US law fails to satisfy the tests established by the ECHR. In *Sakharov,* the ECHR conducted precisely the type of proportionality test in respect of the law and practices of Russia which Facebook said ought to have been conducted by the DPC in relation to the regime in the United States. In two significant respects, (1) in relation to the obligation to give notice when notice would no longer jeopardise the surveillance actually conducted and (2) the rules in relation to standing, the laws of the United States failed to pass these tests. This is confirmed by Professor Brown where he states at p. 3 of his work that the Convention "… *sets a higher general standard than the US government's interpretation of its international human rights law obligations as applying only within its own territory."* He notes at para. 3.4 that despite the relatively weak standards on foreign intelligence collection by EU

member states, the Convention sets relatively high standards in terms of compliance of all surveillance regimes with the rule of law. He identifies a number of minimum standards. The last two of these points are: -

> "*Persons who have been subjected to surveillance should be informed of this as soon as this is possible without endangering national security or criminal investigations, so that they can exercise their right to an effective remedy at least ex post facto; and*
>
> *The bodies charged with supervising the use of surveillance powers should be independent and responsible to, and be appointed by, Parliament rather than the Executive."*

289. The DPC submitted that the legal regime in the United States fails the strictly necessary test laid down in Article 52 (1) of the Charter in relation to interference with personal data on the grounds of national security. She submitted that there was no explanation why it is necessary to have strict rules in relation to standing with no latitude afforded to potential litigants to reflect the inherent difficulties in litigation in this area. She submitted that there was no explanation why notification along the lines similar to those described in *Watson* and *Zakharov* applied in the United States or why it was necessary to maintain in all cases for all time a policy of "neither confirm nor deny" that surveillance has taken place. Inherent in the *Watson* formula is accommodation for the danger posed by the so called "hostile vector attack".

Conclusion

290. To my mind the arguments of the DPC that the laws -and indeed the practices- of the United States do not respect the essence of the right to an effective remedy before an independent tribunal as guaranteed by Article 47 of the Charter, which applies to the data of all EU data subjects transferred to the United States, are well

founded. Furthermore, even if the essence of that right is respected, there are, for the reasons advanced by the DPC, well founded concerns that the limitations on the exercise of that right faced by EU data subjects in the United States are not proportionate and are not strictly necessary within the meaning of Article 52 (1) of the Charter.

291. The remaining issue therefore is whether the introduction of the Ombudsperson mechanism changes this assessment.

The Ombudsperson Mechanism

291. The Privacy Shield Decision was adopted after the CJEU in *Schrems* declared that the Safe Harbour Decision was invalid. Analysis by the working group, and the Commission highlighted concerns about the limits on individual redress for EU citizens in relation to data subjected to processing by the United States for purposes of national security. Recital 115 of the Privacy Shield Decision provides: -

> *"While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show 'standing', which restricts access to ordinary courts."*

292. It is thus clear that as of the 12th of July, 2016, when the decision was adopted, the Commission had concerns about the adequacy of the avenues for individual redress in the United States. Recital 116 records that: -

"In order to provide for an additional redress avenue accessible for all EU data subjects, the U.S. government has decided to create a new Ombudsperson Mechanism…"

293. The Ombudsperson will be appointed by the Secretary of State and will be independent from the intelligence community but operate within the Department of State. He or she will be part of the executive branch of government. The Ombudsperson will deal with requests received from EU citizens. Each EU citizen will send their individual requests to the supervisory authorities in his or her Member State. There is no requirement to demonstrate that the requester's data has in fact been accessed by the US government through its signals intelligence activities and the requester can deal with the matter through his own language. The supervisory authorities ensure that the request is in order and it is not frivolous, vexatious or not *bona fide*. They then forward the request to the EU individual complaint handling body. The EU body then submits the complaint to the Ombudsperson in the State Department.

294. The Ombudsperson will work closely with the United States government officials including independent oversight bodies to ensure that the requests are processed on the basis of necessary information and resolved in accordance with the applicable laws and policies. The Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policy. The response will confirm (1) that the complaint has been properly investigated, and (2) that the US laws, statutes, executive orders, presidential directives and agency policies providing the limitations and safeguards described in the annex to the Privacy Shield Decision have been complied with or, in the event of non-

compliance, that such non-compliance has been remedied. Critically, the Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Ombudsperson confirm the specific remedy that was applied.

295. There was some uncertainty as to whether the Ombudsperson mechanism applied in respect of EU citizens whose data is transferred pursuant to the SCCs. The mechanism is described in Annex A to the Privacy Shield Decision. On page 72 of the decision it records the fact that the new mechanism is: -

> "*to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), Derogations, or Possible Future Derogations*".

Clause 3 (B) requires the EU individual complaint handling body to verify that the request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to "*the Privacy Shield, SCCs, BCRs, derogations, or possible future derogations.*" In the circumstances, I am satisfied that it is open to an EU citizen who reasonably believes that his or her data have been transferred from the EU to the United States pursuant to the SCCs to make a request to the Ombudsperson through the mechanism established as part of the Privacy Shield Decision. It is therefore relevant to the assessment of the issues before the court.

Submissions of Facebook

296. Facebook relied upon the Ombudsperson mechanism. It said the Commission was of the view that the mechanism addressed any concerns regarding the adequacy of the individual avenues for redress in the United States. Recitals 122, 123 and 124 the Decision state: -

"(122) Overall, this mechanism ensures that individual complaints will be thoroughly investigated and resolved, and that at least in the field of surveillance this will involve independent oversight bodies with the necessary expertise and investigatory powers and an Ombudsperson that will be able to carry out its functions free from improper, in particular political, influence. Moreover, individuals will be able to bring complaints without having to demonstrate, or just to provide indications, that they have been the object of surveillance. In the light of these features, the Commission is satisfied that there are adequate and effective guarantees against abuse.

(123) On the basis of all the above, the Commission concludes that the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield.

(124) In this respect, the Commission takes note of the Court of Justice's judgment in the Schrems case according to which "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification of erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter." The Commission's assessment has confirmed that such legal remedies are provided for in the United States, including through the introduction of the Ombudsperson mechanism. The Ombudsperson mechanism provides for independent oversight with investigatory powers. In the framework of the Commission's continuous monitoring of the Privacy Shield, including through

the annual joint review which shall also involve the Ombudsperson, the effectiveness of this mechanism will be reassessed."

297. Facebook argues that the legal regime analysed by the Commission is (essentially) the same as the legal regime which falls to be considered by this court and that the Ombudsperson mechanism applies to the SCCs as well as to data transferred pursuant to the Privacy Shield Decision. Therefore, there is no distinction between the adequacy assessment to be made pursuant to the Privacy Shield Decision and the adequacy assessment which this court is asked to consider. In those circumstances, it argues that the court is bound by the adequacy decision of the Commission. In the alternative, if the court is not bound by it, then it should defer to the greater expertise and research conducted by the Commission in comparison to the analysis and research conducted by the DPC and should prefer the conclusions of the Commission to those of the DPC.

298. As discussed above, the DPC argues that the Privacy Shield Decision is a decision that there is adequate protection afforded to data transferred to the United States pursuant to all of the safeguards set out in the Privacy Shield Decision. In essence, these are threefold: the protections based upon the privacy shield principles (which are essentially private law remedies), the provisions of US law and the Privacy Shield Ombudsperson mechanism. As I have already held, the Privacy Shield Decision is not an adequacy decision binding upon the DPC and the court. However, it is difficult to see how the privacy shield principles (as opposed to the provisions of the laws of the United States and the Ombudsperson mechanism) could be relevant to the issues raised in Mr. Schrems complaint (leaving aside the fact that the data is not transferred pursuant to the privacy shield principles). It is fair to conclude therefore that the decision of the Commission in regard to the adequacy of the protections

afforded to EU citizens against interference by the intelligence authorities in the United States with the fundamental rights of EU citizens whose data are transferred from the Union the United States, conflicts with the case made by the DPC to this court.

Submissions of the DPC

299. The DPC submits that the Ombudsperson mechanism does not remedy the inadequacies in US law which she has identified. She says that the Ombudsperson is not independent of the executive and therefore does not constitute an independent tribunal within the meaning of Article 47. It is not established by law, it is not permanent, it does not give decisions or reasons and it does not grant compensation. It is not subject to judicial review. Each of these elements are requirements of an independent tribunal within the meaning of Article 47. Therefore, it does not alter her conclusion that the laws of the United States do not respect the essence of the right guaranteed by Article 47 of the Charter or, in the alternative, are not proportionate and strictly necessary within the meaning of Article 52 (1) of the Charter.

Discussion

300. Just as the DPC was required by the CJEU in *Schrems* to make her own independent inquiry into Mr. Schrems' complaint notwithstanding the provisions of the Safe Harbour Decision, so too this court, in fulfilling its role in the legal order of the Union and, in particular, the role referred to by the CJEU in its ruling in *Schrems* at paras. 64 and 65, must make its own assessment of the issues notwithstanding the assessment of the Commission enshrined in the Privacy Shield Decision. It is of course clear that there is no requirement that the third country provide identical protections to those provided for by EU law so long as there is an essential equivalence between the protections provided under Union law and under those in the third country. Under Union law the requirement is to "… *respect the essence of the*

fundamental right to effective judicial protection as enshrined in Article 47 of the Charter…" (*Schrems* para. 95).

301. It seems to me that there is a well-founded argument that the Ombudsperson mechanism does not respect the essence of that fundamental right. It does not afford EU citizens judicial protection. The Ombudsperson is not a judge and she is not on the face of it independent of the executive. The office arguably does not meet the *indicia* of a tribunal established the ECJ in *Denuit* [2005] ECR I-923 at para 12 that the body is established by law, is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law and whether it is independent. Critically, her decisions are not subject to judicial review. It is also arguable that the remedy is not an effective remedy as required by Article 47. If the data of an EU citizen have been illegally seized, processed or shared, while the "non compliance" may have been remedied, there is obviously no question of the person so wronged recovering damages or an injunction to prevent future wrongdoing or even a declaration to that effect, as the Ombudsperson will neither confirm nor deny that the requester has been subjected to electronic surveillance.

302. This is not to say that the response of the Ombudsperson is an unreasonable one in the context of the exigencies of national security, nor is that a matter for a national court to pronounce upon. On the contrary, there are good reasons why authorities should neither confirm nor deny whether or not an individual has been subject to surveillance. But these good reasons do not necessarily alter the assessment I have made with respect to the requirements of Article 47 of the Charter or the fact that I share what I consider to be the well-founded concerns of the DPC that the Ombudsperson mechanism does not remedy the issues with regard to individual redress in the Unites States.

Article 4 of the SCC Decisions

302. The remaining issue to be considered is whether the existence and provisions of Article 4 of the SCC decisions preserves the validity of the SCC decisions notwithstanding the laws and practices of the third country to which the data is transferred. As discussed above, Article 4 of the SCC decisions as originally drafted was replaced on the 16th December, 2016. It is the effect and implications of this text which is relevant to this judgment.

303. It was argued by a number of parties that the solution to the concerns raised by the DPC regarding the regime in the United States and in particular as concerns the issues of redress lay in her own hands: she could suspend or prohibit transfers of data by Facebook to Facebook Inc. pursuant to Article 4 of the SCC decisions if she believed that this was necessary in order to protect individuals with regard to the processing of their personal data. Even if, on the facts of this case, it was not appropriate to suspend data transfers to the United States, nonetheless the existence of Article 4 saved the SCC decisions from invalidity.

304. In order to examine this argument, it is necessary to consider the scope of the SCC decisions. Article 1 provides that the standard contractual clauses set out in the annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26 (2) of the Directive. Article 2 sets out the scope of the decision and Article 3 sets out relevant definitions. Article 4 now provides: -

> *"Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive 95/46/EC leading to the suspension or definitive ban of data flows to third countries in order to protect*

individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.'

Articles 5 to 8 of the decision provide that there is to be a review of the decision after three years, the commencement date, the repeal of earlier decisions, transitional arrangements and the fact that the decision is addressed to the Member States.

305. Article 4 is directed towards ensuring that the Member States notify the Commission and the Commission in turn notifies other Member States of the exercise by a competent authority of their existing powers pursuant to Article 28 (3) to suspend or ban transfers of data to third countries in order to protect individuals with regard to the processing of their data. It does not *confer* a power on a supervisory authority. In effect, the previous version of Article 4 has been removed from the SCC decisions. If Article 4 had simply been repealed, the supervisory authorities would nonetheless still retain their powers pursuant to Article 28 (3) of the Directive. Article 4 no longer operates as a saver provision in the SCC decisions analogous to the comparable provision in the Safe Harbour decision (Article 3) which was declared invalid by the CJEU in *Schrems*. The provisions of Article 4.1 (a) as originally drafted were specifically directed towards the legal regime in force in third countries. This is no longer the case. The supervisory authorities, in this case the DPC, enjoy the powers set out in Article 28 (3) of the Directive, no more and no less, when considering the protection of individuals with regard to the processing of their data.

306. Article 28 (3) sets out the powers to be conferred on supervisory authorities by the Member States in order that they may carry out their functions and obligations under the Directive in the light of the Treaties and the Charter. They are investigative powers, effective powers of intervention and powers to engage in legal proceedings.

Examples of effective powers of intervention include imposing a temporary or definitive ban on processing. This is a general power of supervisory authorities applicable to any and all processing operations within the EU. It also applies to processing comprising of transfers to third countries but it is by no means specific or limited to the latter situation. The power is not primarily conferred with a view to suspending data transfers to a third country pursuant to the SCCs where the supervisory authority contends that this is necessary in order to protect individuals with regard to the processing of their data, though undoubtedly the power extends to that situation. Neither is the power expressly related to complaints by individuals or associations, which are governed by Article 28 (4) of the Directive.

307. Given that it is a general power applicable to all processing governed by the Directive, it is useful to see if there are any indicators as to how the power should be exercised in the context of the SCC decisions. Recital 11 of Commission Decision 2010/87/EU provides:-

> *"Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In* ***exceptional cases*** *where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses* ***in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the***

warranties and obligations providing adequate protection for the data subject." (emphasis added).

308. Recital 11 shows that the power to prohibit or suspend a data transfer or a set of transfers based on standard contractual clauses should apply in exceptional cases. It applies where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations of the data exporter, the data importer and any sub-processor which are intended to provide adequate protection for the data subject. There can be any number of bases upon which this could be so and the legal regime of the third country is only one possible example of this exceptional case. The fact that it is described as an exceptional case would indicate that particular rather than systemic circumstances prevailing are envisaged.

309. Secondly, in *Com* [2013] 846 Final, the Communication from the Commission to the European Parliament and Council concerning the Safe Harbour Decision, the Commission noted at p. 7:-

> "*The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies. German data protection commissioners have decided not to*
>
> *issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.* ***The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core***

mechanism for the transfer of personal data between the EU and the US." (emphasis added).

315. The Commission's concern that different data protection authorities were intending to take different decisions in relation to data transfers pursuant to the Safe Harbour Decision applies equally to any decision taken by either a data protection authority or a member state individually to suspend or prohibit transfers of data pursuant to the SCCs to the United States. The reason is clear. The perceived difficulty in permitting continued transfers of data to the United States pursuant to the SCCs decision is general and systemic rather than particular to the individual contractual arrangements concerning Facebook and Facebook Inc. and/or its sub-processers. The scope for what the Commission described as differences in coverage applies equally in this case. It is undesirable that identical data transfers could be permitted under the SCCs in one Member State but suspended or banned in another depending on whether or not the particular national authorities had investigated the issues surrounding the transfer of data to the United States or not, or had reached different conclusions regarding the likelihood of the data being subjected to a substantial adverse effect on the warranties and obligations provided by the SCCs or whether such a ban or suspension of data flows is required in order to protect individuals with regard to the processing of their personal data.

316. Thirdly, the power of the data protection authorities to suspend or ban the transfer of data to third countries is a discretionary power. Both the Directive and the CJEU in *Schrems* emphasised that the authorities shall act with complete independence in exercising the functions entrusted to them. If the SCC decisions are valid because the DPC has the *power* to suspend the transfers of data to the United States where this is necessary to protect the personal data of EU citizens, this can only be on the basis

that the DPC is *obliged* to suspend the transfer of data in circumstances where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject. In other words, if the argument is correct, she is obliged to make the order, and this in turn means that she does not have a discretion to refrain from acting.

317. Further, once the precondition to the exercise of the power is established, the likely substantial adverse effect on the warranties and obligation, she must then make an order suspending or banning the transfer of data. She cannot consider, for example, whether it is desirable that a common position across the EU should be established or weigh competing interests in the balance or take account of the wider implications of such an act before taking such an extremely significant step as to prohibit all transfers of data by Facebook to Facebook Inc. Such a construction is inconsistent with her independence in relation to her functions. It also seems to be inconsistent with the judgment of the CJEU in *Schrems* para 42 where the court said that the national supervisory authorities must ensure a fair balance between the observance of the fundamental right to privacy on the one hand and the interests requiring the free movement of personal data on the other hand.[6] But if the power is in fact discretionary, with the implication that she may refrain in certain circumstances from exercising it, notwithstanding the perceived inadequacies in the legal regime in the third country to which the data is transferred, then she may validly decide not to make an order suspending or banning the transfer of data to a third country. It therefore follows that the mere fact that the power to suspend data transfers exists does not save the SCC decisions from invalidity based upon the perceived inadequacies of the law of the third country.

[6] See also Case C-518/07 *European Commission v Federal Republic of Germany* (judgment of the CJEU delivered on the 9th March, 2010)

318. It seems to me that as the power is and remains discretionary, the validity of the SCC decisions cannot depend on the automatic exercise of a discretionary power. She is entitled to take the view that the suspension of data transfers is not appropriate in any given circumstances, even if the threat to the data privacy of EU data subjects is established. In this case, she has decided that this is so as the problem which she has identified is systemic and general rather than particular and related to the specific contracts in question. She has adopted an alternative means of dealing with the issue by bringing these proceedings and seeking to have her concerns considered by a national court and if necessary referred to the CJEU for a decision on the validity of the SCC decisions insofar as they apply to transfers of data to the United States.

319. It seems to me that not only is this a legitimate conclusion for her to reach but it is one that is clearly hers to make as an independent supervisory authority. It is reasonable to ask whether it is legitimate to use the power granted to a data protection authority pursuant to Article 28(3) of the Directive to resolve major international structural issues of the kind identified in these proceedings.

320. It is also to be borne in mind that she can only make orders pursuant to the provisions of national legislation. Section 11, subs. 7 and 8 of the Data Protection Acts states that the DPC may prohibit the transfer of personal data from the State to a place outside the State but that in determining whether to prohibit a transfer of personal data under s. 11 she must also consider whether the transfer "*would be likely to cause damage or distress to any person and [to] have regard to the desirability of facilitating international transfers of data.*"

321. It seems to me that there is certainly an issue to be resolved as to whether the fact that the DPC has power pursuant to Article 28(3) of the Directive to suspend or ban the transfer of data by Facebook to Facebook Inc. necessarily saves the SCC

decisions from invalidity. There is also an argument to be made as to whether, in the circumstances of this case, the DPC was obliged to exercise that power or whether, in the alternative, she was entitled to proceed as she did and to seek a ruling from the CJEU on the validity of the SCC decisions. For these reasons, I do not accept the submissions that Article 4 is the answer to all of the issues raised by the DPC and that accordingly a reference to the CJEU is neither appropriate nor necessary.

Mr. Schrems' Objections to a Reference

322. Mr. Schrems' objections to the reference sought by the DPC in these proceedings are different to those raised by Facebook and some of the *amici curiae.* Firstly, he says that he did not raise any objection to the validity of the SCC decisions whether in his reformulated complaint or otherwise. He says his primary complaint was that the relevant clauses in the agreement relied upon by Facebook to transfer data to Facebook Inc. did not conform to or comply with the provisions of the SCC decisions and that therefore Facebook could not rely on the decisions and was not entitled to the derogation from Article 25 of the Directive provided for by Article 26.

323. He said the DPC wholly failed to examine, investigate or determine his primary complaint and instead she accepted Facebook's contention that the agreement was in compliance with the SCC decisions. He submits that in the absence of such a determination by the DPC the proceedings are premature, misconceived, unnecessary and are based entirely on a hypothesis developed and maintained by the DPC that there is a challenge to the validity of the SCC decisions.

324. He also argued that even if it were the case that the SCC decisions applied, Mr. Schrems did not question the validity of the SCC decisions as Article 4 (1) permits the prohibition or suspension of data transfer where the law to which the data importer (Facebook Inc.) is subject does not provide adequate safeguards. On this basis, the

SCC decisions provide for circumstances where the third country's laws are inadequate and thus they do not interfere or conflict with the rights of individuals to privacy and data protection as ensured by and enshrined in Articles 7 and 8 of the Charter.

325. He submitted that on the facts established by the DPC the US does not provide adequate safeguards as required by EU law and therefore data transfers to the US between Facebook and Facebook Inc. ought to be suspended or prohibited, as he sought in his reformulated complaint.

326. He submitted that Article 267 of TFEU requires that a reference only be made when a question is properly raised and the answer to that question is necessary to enable the court to give judgment. He says that para. 65 of the judgment of CJEU in *Schrems* does not confer a free standing right on the DPC to make a reference to the CJEU. It clarifies that a reference must be necessary by reference to the underlying claim.

327. He also stated that the making of a reference is premature as the DPC has expressly stated that her investigations have not concluded and that her decision is in draft form only and explicitly subject to further submissions. It is only once the investigation is completed that it will be possible to determine whether Facebook in fact transfers data to Facebook Inc. pursuant to SCCs as it asserts and to determine whether there are other bases upon which Facebook transfers data to Facebook Inc. which may or may not be justified whether under the provisions of Article 25 or 26 of the Directive.

Response of the DPC

328. The DPC submitted that, as an independent authority, it was a matter for her how she conducts her investigations into Mr. Schrems' reformulated complaint. Facebook has acknowledged that it transfers data in large part pursuant to the SCC

decisions and particularly that of 2010. It has exhibited the agreement of November 2016 between Facebook and Facebook Inc. which governs the transfers. She is the statutory decision maker and the independent authority under the Directive and once a complaint is made to her it is a matter for her to determine the order and the manner in which she proceeds to decide upon the issues raised. She has reached the conclusion that she cannot now progress her investigation further in the absence of the ruling which she seeks in these proceedings. This is a matter within her jurisdiction and one in which the court ought not to interfere by, for example, as submitted by Mr. Schrems, directing that she complete her investigations into whether or not the terms of the agreement of November 2016 accord with the provisions of the SCC decisions or whether there are other legal bases upon which Facebook relies when transferring data for processing to Facebook Inc.

329. The DPC submitted that she believes Mr. Schrems is incorrect in his belief that Article 4 of the SCC decisions secures the validity of the decisions for the reasons discussed above. As Mr. Schrems' alternative position is that if he is wrong about Article 4, then he does challenge the validity of the SCC decisions, it follows that it is not correct to say that the issue does not arise from his reformulated complaint. She submits that she did not raise this issue based upon her own hypothesis, as was submitted by Mr. Schrems, but that it arises from point 2 of his reformulated complaint page 11 which states: -

> "*Even if the current and all previous agreements between "Facebook Ireland Ltd" and "Facebook Inc." would not suffer from the countless formal insufficiencies above and would be binding for the DPC (which it is not), "Facebook Ireland Ltd" could still not rely on them in the given situation of factual "mass surveillance" and applicable US laws that violate Art. 7, 8 and*

47 of the [Charter] (as the CJEU has held) and the Irish Constitution (as the Irish High Court has held).”

330. Finally, even if it were the case that Mr. Schrems did not, in terms, in his reformulated complaint challenge the validity of the SCC decisions, the DPC is entitled to determine what is the key question raised by the reformulated complaint. It is to be noted that in the proceedings as they originally unfolded, neither party challenged the validity of the Safe Harbour Decision, but the High Court (with whom the CJEU agreed) took the view that the proceedings involved a challenge to the validity of the Safe Harbour Decision. Therefore, even if Mr. Schrems did not in fact challenge the validity of the SCC decisions, this does not mean that reference to the CJEU is not necessary for the resolution of the proceedings and Mr. Schrems' reformulated complaint.

Discussion

331. It is clear from the decisions of the High Court and CJEU in *Schrems* that it is both legitimate and appropriate for both the DPC and the court to identify the true controversy raised by the complaint and the point which requires to be determined in order properly to conclude the investigation into Mr Schrems' complaint. I accept that the central issue for resolution is the validity of the SCC decisions and this can only be resolved by a decision of the CJEU. I believe that there is a strong argument that Article 4 of the SCC decisions does not provide the answer to the concerns raised by the DPC in relation to the remedial regime in the United States. That being so, Mr Schrems' reformulated complaint does raise the validity of the SCC decisions and therefore it is legitimate for the DPC to seek a reference to the CJEU to resolve this issue in order that she may complete her investigation in accordance with law.

332. This court lacks jurisdiction to pronounce upon the validity of the SCC decisions. The DPC says that she needs to know whether or not they are valid, given her concerns that they are not valid for the reasons set out in this judgment. There are two options open to the court: it can make the reference sought by the DPC to the CJEU or it can refuse to make the reference and dismiss the proceedings as no other relief is sought. In that event the court in effect will be endorsing the validity of the decisions and require the DPC to conclude her investigation into Mr Schrems' complaint on the basis that the SCC decisions are valid.

333. I have formed the view that I concur with the DPC that there are well founded grounds for believing that the SCC decisions are invalid and furthermore that it is extremely important that there be uniformity in the application of the Directive throughout the Union on this vitally important issue. This requires that there be consistency and clarity. On that basis, I believe that a reference is necessary and appropriate. It follows that the balance of the arguments raised by Mr Schrems against making a reference must be rejected. For these reasons and the reasons advanced by the DPC I do not accept that I should refuse to make a reference to the CJEU as requested by the DPC.

Conclusion

334. The court has jurisdiction to make a reference to the CJEU for a preliminary ruling on the validity of the SCC decisions under Article 267 of TFEU. The court may do so if it finds that the DPC has raised well-founded concerns as to the validity of the decisions of the Commission and the court shares those concerns. Union law and the Charter are engaged. The court is not obliged to reject the application based upon the Privacy Shield Decision. It is certainly arguable that neither the DPC nor the court is required to conduct a comprehensive adequacy analysis of the laws and practices of the

United states in relation to electronic surveillance on the grounds of national security, oversight systemic protections and individual remedies in order that they may reach a conclusion that the protection of the data privacy of EU citizens whose data is transferred to the United States for processing does not enjoy the high level of protection which it is guaranteed under Union law. It is arguably legitimate to analyse the remedial regime of a third country to whom the data is transferred for processing in isolation and on the basis of the evidence in relation to individual rights of redress for EU citizens whose data is wrongfully interfered with to concluded that there is a failure to satisfy the essence of the right guaranteed under Article 47 of the Charter as required by Article 52 (1) of the Charter. In the alternative, it is arguable that the limitations on the exercise of the right to an effective remedy before an independent tribunal, as required by Article 47, for EU citizens whose data privacy rights are infringed by the intelligence agencies are not proportionate or necessary or needed to protect the rights and freedoms of others. Neither the introduction of the Privacy Shield Ombudsperson mechanism nor the provisions of Article 4 of the SCC decisions eliminate the well-founded concerns raised by the DPC in relation to the adequacy of the protection afforded to EU data subjects whose personal date is wrongfully interfered with by the intelligence services of the United States once their personal data has been transferred for processing to the United States.

335. I therefore propose to refer the issue of the validity of the SCC decisions to the CJEU for a preliminary ruling. As every party to the proceedings indicated that if I decided to refer issues to the CJEU that they would like the opportunity to be heard as to the questions to be sent to the court, I will list the matter for submissions and then determine the exact questions I shall refer to the court for a preliminary ruling.