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*

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 *Schrems*, 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 *amici 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 *Schrems* 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