THE HIGH COURT

COMMERCIAL

[2016 No. 4809 P.]

BETWEEN

THE DATA PROTECTION COMMISSIONER

PLAINTIFF

AND

FACEBOOK IRELAND LIMITED AND MAXIMILIAN SCHREMS

DEFENDANTS

REQUEST FOR A PRELIMINARY RULING

ARTICLE 267 TFEU

To: The Registrar

Court Of Justice of the European Union

L2925 Luxembourg

1. The High Court of Ireland (Ms. Justice Costello) hereby refers the questions set out in the annex to this reference to the Court of Justice of the European Union ("the Court" or "CJEU") for preliminary ruling in accordance with Article 267 TFEU. The parties before the High Court were the Data Protection Commissioner of Ireland, the plaintiff, Facebook Ireland Ltd and Maximillian Schrems, defendants, and four *amicus curia*, the government of the United States of America, Digital Europe, the Business Software Alliance, and EPIC.

2. The sole issue in the case is the validity of Commission Decision 2001/497/EC; Commission Decision 2004/915/EC and Commission Decision 2010/87/EU amended by Commission Decision 2016/2297 (together "the SCC

Decision(s)"). The Court alone has jurisdiction to adjudicate on the validity of decisions of the Commission of the European Union ("the Commission"). The validity of the SCC Decisions depends upon the interpretation of EU law as more fully set out in this reference.

Background

3. The issues arise from a complaint made by Mr. Maximillian Schrems ("Mr. Schrems") to the Data Protection Commissioner ("DPC") in Ireland regarding the transfer of his personal data by Facebook Ireland Ltd ("Facebook") to Facebook Inc. for processing. Facebook Inc. is a US corporation and the ultimate parent of Facebook. Facebook says that in large part it transfers data to Facebook Inc. by means of standard contractual clauses set out in the Annex to the SCC Decision.

4. The DPC 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 proceedings in order that the validity of the SCC Decisions may be determined either by the High 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 the High Court makes a reference to the CJEU and the CJEU makes a ruling on the validity of the SCC Decisions.

5. The High Court heard the evidence adduced and arguments advanced by the DPC, Facebook, Mr. Schrems, the government of the United States, BSA, Digital Europe and EPIC and concluded that it shared the well founded concerns of the DPC

as to the validity of the SCC Decisions and accordingly the questions set out below should be referred to the CJEU for a preliminary ruling pursuant to Article 267 of TFEU.

Overview of the legislation

6. 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 European Convention on Human Rights ("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 his 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.

7. 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.

8. 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 with the need to protect the rights and freedoms of others.

9. Article 4(2) of TEU provides that national security remains the sole responsibility of each Member State. This is reflected in Article 3(2) of Directive 95/46/EC ("the Directive") which provides that it does not apply in the course of an activity which falls outside the scope of Union law and in any case to processing operations concerning pubic 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.

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. This reflects Recitals 56 and 57 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 as 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 or where there has been no assessment of the level of protection afforded in the third country. 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, where the 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 regards the exercise of the corresponding rights. Article 26(2) specifically states that such safeguards may in particular result from "appropriate contractual clauses". This reflects Recital 59 of the Directive which says that particular measures may be taken to compensate for the lack of protection in a third country where the controller offers appropriate safeguards.

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 processors 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.

Mr. Schrems' reformulated complaint.

17. In light of the decision of the Court in *Schrems*, Mr. Schrems reformulated his complaint to the DPC. He states that his personal data is forwarded by Facebook to Facebook Inc. in the United States of America where his data is processed. Facebook Inc. is obliged to make his personal data available and/or obliged to disclose it to the United States authorities such as, for example, the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). He alleges that there is no judicial remedy which would allow the data subject to take appropriate action to protect his personal data rights. He says that the United States authorities have access to data held by Facebook Inc. among other US based companies. He says 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 is explained more fully below).

18. He makes various complaints regarding the current and previous agreements between Facebook and Facebook Inc. which he says means that they do not comply with the SCC Decision and that therefore the DPC is not bound by the SCC Decision. Aside from the complaints directed towards the basis upon which Facebook transfers his data to Facebook Inc., he maintains that Facebook cannot rely upon the SCC Decision "in the given situation of factual 'mass surveillance' and applicable US law that violate Article 7, 8 and 47" of the Charter and the Irish Constitution. He argues that the PRISM programme violates the essence of Article 7 and 47 of the Charter. He says that this was established by the CJEU in the ruling in *Schrems* and is binding on the DPC. He says that Article 4(1) of the SCC Decision takes account of a situation where national laws of a third country override the contractual clauses and allows data protection authorities to suspend data flows in such a situation. He therefore requests the DPC to issue a prohibition notice or an enforcement notice under domestic legislation (s.11(7) to (15) and s.10(2) to (9) of the Data Protection Acts) and to take any other appropriate steps to suspend all data flows from Facebook to Facebook Inc.

19. Facebook acknowledges that it transfers personal data relating to Facebook's subscribers resident in the European Union including Mr. Schrems to Facebook Inc. 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 Decisions. The DPC 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. She engaged in a review of the remedies available for breach of data protection rights in US federal law. She did not conduct a complete adequacy analysis of the entire regime in the United States.

20. Her preliminary view is 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 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 out in the annexes to the SCC Decisions in her opinion do not address this well founded objection as the standard contractual clauses do no more than establish a right in contract in favour of data subjects, to a remedy against either or all of the data exporter or data importer or data subprocesser.

Issues raised in the proceedings

1. Scope of Union law

21. Facebook argued that the case was concerned with national security. National security falls outside the scope of EU law entirely because the treaties reserve competence over national security issues to member states. It referred to Article 4(2) TEU and Article 3(2) and Recital 13 of the Directive. It argued 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. It argued that if this is correct, then the Charter is inapplicable by reasons of the provisions of Article 51(2). Facebook relied upon the decision of the Court in joined cases C-317/04 and C-318/04 *European Parliament v. Council and the Commission* EU:C:2006:346. The High Court did not accept the submission but it is a matter which requires to be determined by the CJEU and therefore this issue is the first question referred to the Court in this reference.

2. Comparator

22. The second issue arises from Facebook's submission that the assessment whether a third country ensures adequate protection of the personal data of EU citizens must involve a comparison with another regime and like must be compared with like. It submitted there must be a comparator to processing of private data by the United States intelligence agencies for purposes of national security against which the assessment whether the protections or safeguards afforded in the United States to data subjects in respect of their personal data are adequate may be made.

23. Facebook argued that the comparator for processing in a third country which is not concerned with national security is to be found in the Directive read in the light of the Charter. However, according to Facebook, the Directive and the Charter do not apply to processing by member states for national security purposes. It submits that it follows that there is no EU comparator for processing by a third country for national security purposes and therefore the comparator can only be found in the domestic laws of each of the member states. Further, as the Directive confers no remedy in each of the member states in respect of EU data subjects where there is interference with personal data on the grounds of national security, it follows, according to Facebook, that there is no requirement that there be a remedy in the United States.

24. This submission raises the issue whether, in determining whether there is a violation of the rights of an individual through the transfer of data from the EU to a third country under the SCC Decisions, where it may be further processed for national security purposes, the comparator for the purposes of the Directive comprises of the Charter, TEU, TFEU, the Directive and the European Convention on Human Rights (or any other provision of EU law) or, is the comparator to be found in the national laws of one or more member states, or an amalgam of the laws of all or some of the member states. Further, if the comparator is to be found in the national laws of one or

more member states or a combination thereof it further needs to be considered whether the practices in the context of national security in one or more member states are also to be included in the comparator. This issue is the second question referred to the Court.

25. The High Court proceeded on the basis that the comparator was to be found by reference to Union law and not by reference to the laws of individual member states or even an amalgam of the laws of the member states. The High Court did not make findings of fact in relation to the evidence adduced by Facebook in relation to the laws and practices of some member states. This evidence was not contested by the DPC on the basis, on her case, that it was not relevant to the issues to be determined.

3. Basis for assessment of the protection afforded to data exported from EU

26. There was a fundamental disagreement in principle between, on the one hand the DPC and Mr. Schrems, and on the other hand, Facebook and the government of the United States, Digital Europe and BSA, regarding the correct assessment as to whether a third country to which data is exported ensures the level of protection required by EU law. The DPC and Mr. Schrems argued the level of protection in the third country was to be assessed by reference to the applicable rules in the third country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules to include the professional rules and security measures which are complied with in the third country. It was not appropriate, according to them, to look at the practices or administrative procedures or policies of the third country in conducting this assessment.

27. Facebook and the government of the United States said that it was important to look at the regime holistically and that it was vital to include in the assessment such administrative, regulatory and compliance practices and policy safeguards,

procedures, protocols, oversight mechanisms and non judicial remedies as are in place in the third country. There was extensive evidence adduced as to privacy policies applicable to the security agencies in the United States and to a variety of oversight mechanisms both within the agencies, in the Department of Justice, in the Foreign Intelligence Surveillance Court and by committees of Congress. Reference was also made to the role of advocacy groups and freedom of the press in protecting the privacy rights of individuals whether or not they were US citizens. The findings of the High Court in relation to systemic safeguards and oversights which were considered to be of relevance to the issues raised in the case are at paras. 239-250 of the judgment appended to this reference.

28. The resolution of the appropriate factors to be taken into account when making the assessment in relation to a third country is a matter solely within the competence of the Court and necessary in order to determine the matters at issue. This is covered by the third question referred to the Court.

Findings of fact in relation to US law

29. Foreign law, that is law which is not the domestic law of the state of the national court or EU law, is a matter of fact and must be established by evidence in the same way as any other fact must be established to a court. Thus the provisions of US law were proved as facts at the hearing before the High Court. Inherent in this process is a selection between one or more interpretations or hypotheses regarding the state of the law of the third country in the circumstances where law of the third country on a particular point of the law of the third country may be debatable or where there may be conflicting decisions of different courts resulting in uncertainty as to the law on a particular point in that country. The court does not pronounce a definitive, encyclopaedic statement of the law of the third country. Five experts

produced reports relevant to the issues identified in the case and they were each cross examined regarding their opinions and conclusions. The experts also prepared a joint document where they identified the matters in respect of which they were in agreement and those upon which they could not reach a consensus. If a point was not covered in the evidence of any of the experts, it could not form part of the court's findings on US law.

30. Based on the evidence adduced by the experts the High Court made findings of fact regarding the laws of the United States as of April 2017 authorising surveillance by government authorities and agencies, a description of how two of the disclosed programmes operate, the various remedies available to individuals whose personal data privacy rights have been interfered with, the limitations with regard to those remedies and systemic safeguards and oversight mechanisms. These are to be found in paras. 152 to 263 of the judgment appended to this reference. The judgment does not purport to be a comprehensive or definitive statement of the law and practice of the United States in relation to these matters.

Processing and Articles 7 and 8 of the Charter

31. The Directive defines the processing of personal data as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (Article 2 (b)). At paras. 164 to 190 of the judgment the findings of fact in relation to the legal basis for electronic surveillance by the United States agencies are set out together with a description how two acknowledged programmes, PRISM and Upstream, operate. In 2015 under the PRISM programme there were 94,386 targets. In 2011,

the United States government acquired more than 250 million communications under surveillance authorised pursuant to s. 702 of the Foreign Intelligence Surveillance Act, ("FISA"). PRISM accounts for approximately 90% of s. 702 surveillance so that starting with less than 100,000 targets the agencies can acquire an extremely large number of communications. While this is an enormous number it is a very tiny proportion of the total number of internet communications. The Upstream programme works in a fundamentally different manner. It necessarily involves making enormous numbers of non relevant communications available for surveillance by the NSA. The NSA searches a vast number of communications and retains the communications which it "acquires" or "collects" from the vast number of communications to which it has access. It has access to the content as well as the metadata of the communications.

32. It is inherent in a targeted search that a large body of data is searched. There is a distinction between bulk searching and bulk acquisition, collection or retention. The evidence establishes that under Upstream there is mass surveillance in the sense that there is mass searching of communications. The search is for targeted communications and in this sense it is not indiscriminate.

33. The issue to be determined is whether, in light of the definition of processing in the Directive and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, there is mass indiscriminate processing of data by the United States government agencies. The High Court concluded that this was so on the basis of the definition of processing in the Directive. This issue is covered by the fourth question referred to the Court.

Article 47 of the Charter

34. The DPC submitted that the laws of the United States do not respect the essence of the right pursuant to Article 47 for everyone whose rights and freedoms guaranteed *inter alia* by Articles 7 and 8 of the Charter and of the Directive are violated to an effective remedy before an independent and impartial tribunal. The High Court held that there are a number of possible causes of action potentially open to EU citizens in respect of processing of their data by government intelligence agencies in the United States but that there are substantial obstacles to recovery in respect of some causes of action such that in reality an EU citizen is most unlikely to obtain a remedy for unlawful acquisition or processing of his personal data. In effect there are possible claims for damages under 18 U.S.C. s.2712 if the plaintiff can establish that the action was a knowing and reckless violation of the statute or there is a possibility of relief under the Administrative Procedures Act if the claim is not expressly or impliedly precluded. Some causes of action require the plaintiff to establish that he or she has suffered damage, which has been held to mean pecuniary damage. This limitation on the right to seek a remedy does not apply under EU law (*Schrems* para. 89).

35. The High Court concluded that despite the number of possible causes of action, it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by the intelligence agencies. Retrospective judicial remedies would likely be unavailing to victims of governmental overreaching in the conduct of surveillance for the purpose of national security. US law never requires the subject of surveillance to receive notification at any time of the surveillance (unless the subject is a defendant in a criminal or administrative action). The DPC submits that this is critical to the right to an effective remedy as guaranteed by Article 47 of the Charter. The experts on the law of the United States accepted that

most people never know that they have been the subject of surveillance and if they do not know that effectively they can never sue.

36. The DPC submitted that the essence of an Article 47 right is a right to the possibility of a judicial remedy or at the very least a remedy from an independent tribunal. She argued that the law in relation to standing in the United States makes it extremely difficult to establish standing for an EU citizen with no substantial connection with the United States who alleges interference with his personal data. It was accepted by the experts on behalf of Facebook, that it would be exceedingly difficult to challenge secret surveillance by government agencies for EU citizens (Professor Swire) and that it was likely that retrospective judicial remedies will be unavailing (Professor Vladeck). The DPC says that the effect of the rules of standing in the United States is to make the bringing of cases practically impossible or excessively difficult (*Verholen v. Sociale Verzekeringsbank Amsterdam* (cases C-87/90, C-88/90 and C-89/90) and *Unibet (London) Ltd and Unibet (International) Ltd v. Justitiekanslern* (case C-432/05)). The DPC submits that this fails to respect the essence of the fundamental right to an effective remedy guaranteed by Article 47. She says that the United States rules on standing in the area of national security as set out in cases such as *Clapper v. Amnesty International* US, 133 S.Ct. 1138 [2013] and *Wikimedia Foundation v. NSA* (4th Cir. 15-2560) are far more stringent than those established by ECHR (*Zakharov v. Russia* (case 47143/06)).

37. Facebook argued that the CJEU in *Schrems (*para. 95) established that it was only if there was *no possibility* of a remedy before a national court that the essence of the Article 47 right to an effective remedy was not respected. This was not the case in the United States and therefore the essence of the Article 47 right was respected.

38. It argued that when looking at the processing of data for the purposes of national security one does not look at the rights enshrined in the Directive. The test is not whether there is a high level of protection or an adequate level of protection or sufficient safeguards. The question is whether the interference with the rights of the data subject for national security purposes exceeds that which is strictly necessary and proportionate. Are the measures strictly necessary to achieve the objective of preserving national security? Further, when considering remedies available to individuals in the context of national security, the court should consider the entire regime of the particular jurisdiction. The decisions of ECHR recognise that the concept of an effective remedy cannot carry the same meaning in the context of secret intrusive measures because the efficacy of such measures depends upon their remaining secret. Therefore, an effective remedy within the meaning of Article 13 of the ECHR must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance (*Klass v. Germany* (App. No. 5029/71) [1978] 2 EHRR 214). Relying on the decision in *Silver v. The United Kingdom* (1983) 5 EHRR 347, Facebook submitted that the aggregate of the protections and remedies available in the United States provides an effective remedy as required by Article 47 of the Charter.

39. This dispute gives rise to the fifth question in this reference.

The SCC Decision and the laws of third countries

40. It was argued by BSA and Digital Europe that the standard contractual clauses authorised by the SCC Decision 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 data protection authorities pursuant to Article 4.1 of

the SCC Decision (now Article 28(3) of the Directive) to suspend or ban data flows to a particular third country. The SCCs therefore provide "adequate safeguards" within the meaning of Article 26(2) of the Directive. They 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. They each submitted that the power of a data protection authority to prohibit or suspend data flows to a particular third country was crucial to assessing the validity of the SCC Decision. While a data subject may have no direct remedy against agencies in the third country, the data subject could call upon a data protection authority to suspend or prohibit flows of data to that third country and it was open to the data protection authority to protect data subjects by making such an order. 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. The SCCs were not and are not intended and could not have been intended to remedy inadequacies arising from the third country's legal protections. If effective judicial remedies in third countries are a prerequisite for lawful transfer under Article 26(2), it can never be satisfied.

41. The SCCs cannot bind the sovereign authority of a third country and its agencies. This was not contended. This conclusion means that the terms of the SCCs themselves do 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 is subject to unlawful interference. The remedy, on this construction, must be found in the exercise of the

power under Article 4 to suspend or ban data flows. It is for this reason that questions 6, 7 and 8 are referred to the Court for a ruling.

Privacy Shield

42. The Commission adopted Decision (EU) 2016/1250 ("the Privacy Shield Decision") on 12th July, 2016 after the ruling by the CJEU in *Schrems* declared that the Safe Harbour Decision was invalid. In order to provide for "an additional redress avenue accessible for all EU data subjects" the US government decided to create the Ombudsperson Mechanism (Recital 116). The ombudsperson will be appointed by the Secretary of State and will be independent from the intelligence community but operate within the Department of State. Thus the ombudsperson will be part of the executive branch of government. The ombudsperson will deal with requests received from EU citizens in relation to their personal data. There is no requirement to demonstrate that the requestor's data has in fact been accessed by the US government through its signals intelligence activities. The ombudsperson will investigate the complaint working closely with United States government officials including independent oversight bodies to ensure that requests are processed on the basis of necessary information and resolved in accordance with applicable laws and policies. The response from the ombudsperson will confirm (1) that the complaint has been properly investigated and (2) that the US laws, statutes, executive orders, presidential directives and agency policies providing the limitations and safeguards described in the annex to the Privacy Shield decision had been complied with or, in the event of non compliance, that such non compliance has been remedied. Critically, the Privacy Shield ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the ombudsperson confirm the specific remedy that was applied.

43. Facebook and the United States argued that if there was any inadequacy in the remedies available to EU citizens whose personal data is transferred to the US that the provision of the ombudsperson mechanism met the alleged deficiency. This was accepted by the Commission in Recitals 122, 123 and 124 of the Privacy Shield Decision. Facebook argued that the legal regime analysed by the Commission is essentially the same as the legal regime which falls to be considered by the Court as the ombudsperson mechanism applies to data transferred to the US pursuant to the SCC Decision as well as to transfers made pursuant to the Privacy Shield Decision. Therefore, there is no distinction between the adequacy assessment to be made pursuant to the Privacy Shield Decision and the adequacy assessment to be made in respect of the SCC Decision. In those circumstances it argued that either the national court was bound by the adequacy decision of the Commission or, in the alternative, that it should defer to the greater expertise and research conducted by the Commission in comparison to the analysis and research conducted by the DPC and that the conclusions of the Commission should be preferred.

44. The DPC argued that the ombudsperson is not independent of the executive and therefore does not constitute an independent tribunal within the meaning of Article 47. It is not established by law, it is not permanent, it does not give decisions or reasons and it does not grant compensation. The office does not meet the indicia of a tribunal established by the CJEU in *Denuit* [2005] ECR I-239 para. 12. Crucially the decisions of the ombudsperson are not subject to judicial review. It is also arguable that the remedy is not an effective remedy as required by Article 47. If the data of an EU citizen has been illegally seized, processed or shared, while the "non compliance" with US law may have been remedied, there is no possibility of recovering damages or obtaining a declaration or an injunction to prevent future

wrongdoings as the ombudsperson will neither confirm nor deny that the requestor has been subjected to electronic surveillance.

45. The issue whether the protections afforded to EU citizens whose data is transferred to the US are protected as required by Union law following the adoption of the Privacy Shield Decision and the establishment of the Privacy Shield ombudsperson requires to be determined by the Court in order to determine the validity of the SCC Decision. For this reason, questions eight and nine of the reference are referred to the Court.

Validity of the SCC Decision

46. The answers to these questions are necessary in order to determine the validity of the SCC Decisions, the purpose of the proceedings and the reference to the Court. The final question asks the logical conclusion of the prior questions, whether the SCC Decisions violate Articles 7, 8 and/or 47 of the Charter and therefore whether the SCC Decisions should be declared to be invalid.

REFERENCE TO THE COURT OF JUSTICE OF THE EUROPEAN UNION

1. In circumstances in which personal data is transferred by a private company from a European Union (EU) member state to a private company in a third country for a commercial purpose pursuant to Decision 2010/87/EU as amended by Commission Decision 2016/2297 ("the SCC Decision") and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter of Fundamental Rights of the European Union ("the Charter")) apply to the transfer of the data notwithstanding the provisions of Article 4(2) of TEU in relation to national

security and the provisions of the first indent of Article 3(2) of Directive 95/46/EC ("the Directive") in relation to public security, defence and State security?

2. (1) In determining whether there is a violation of the rights of an individual through the transfer of data from the EU to a third country under the SCC Decision where it may be further processed for national security purposes, is the relevant comparator for the purposes of the Directive:

(a) The Charter, TEU, TFEU, the Directive, ECHR (or any other provision of EU law); or

(b) The national laws of one or more member states?

(2) If the relevant comparator is (b), are the practices in the context of national security in one or more member states also to be included in the comparator?

3. When assessing whether a third country ensures the level of protection required by EU law to personal data transferred to that country for the purposes of Article 26 of the Directive, ought the level of protection in the third country be assessed by reference to:

(a) The applicable rules in the third country resulting from its domestic law or international commitments, and the practice designed to ensure compliance with those rules, to include the professional rules

and security measures which are complied with in the third country; or

(b) The rules referred to in (a) together with such administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms and non judicial remedies as are in place in the third country?

4. Given the facts found by the High Court in relation to US law, if personal data is transferred from the EU to the US under the SCC Decision does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?

5. Given the facts found by the High Court in relation to US law, if personal data is transferred from the EU to the US under the SCC Decision:

(a) Does the level of protection afforded by the US respect the essence of an individual's right to a judicial remedy for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?

If the answer to (a) is yes,

(b) Are the limitations imposed by US law on an individual's right to a judicial remedy in the context of US national security proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes?

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

(2) What are the matters to be taken into account in assessing whether the level of protection afforded to data transferred to a third country under the SCC Decision satisfies the requirements of the Directive and the Charter?

7. Does the fact that the standard contractual clauses apply as between the data exporter and the data importer and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in the SCC Decision preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of the Directive?

8. If a third country data importer is subject to surveillance laws that in the view of a data protection authority conflict with the clauses of the Annex to the SCC Decision or Article 25 and 26 of the Directive and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of the Directive to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of Recital 11 of the Directive, or can a data protection authority use its discretion not to suspend data flows?

9. (1) For the purposes of Article 25(6) of the Directive, does Decision (EU) 2016/1250 ("the Privacy Shield Decision") constitute a finding of general application binding on data protection authorities and the courts of the member states to the effect that the US ensures an adequate level of protection within the meaning of Article 25(2) of the Directive by reason of its domestic law or of the international commitments it has entered into?

(2) If it does not, what relevance, if any, does the Privacy Shield Decision have in the assessment conducted into the adequacy of the safeguards provided to data transferred to the United States which is transferred pursuant to the SCC Decision?

10. Given the findings of the High Court in relation to US law, does the provision of the Privacy Shield ombudsperson under Annex A to Annex III of the Privacy Shield Decision when taken in conjunction with the existing regime in the United States ensure that the US provides a remedy to data subjects whose personal data is transferred to the US under the SCC Decision that is compatible with Article 47 of the Charter?

11. Does the SCC Decision violate Articles 7, 8 and/or 47 of the Charter?

ANNEX

1. Judgment of the High Court of 3rd October, 2017 [2017] IEHC 545

2. Booklet of Pleadings

3. Order for reference dated as perfected by the Registrar of the High Court dated.....2018

Dated.....12/4.....2018

Ms. Justice Caroline Costello

Judge of the High Court of Ireland