Our Ref: 3/15/766

DRAFT DECISION OF THE DATA PROTECTION COMMISSIONER

under Section 10(1)(b)(ii) of the Data Protection Acts, 1988 & 2003

DRAFT

Complainant:	**Data Controller:**
Mag. Maximilian Schrems AUSTRIA	Facebook Ireland Limited ("**FB-I**") 4 Grand Canal Square Grand Canal Harbour Dublin 2 IRELAND

PRELIMINARY POINTS

I. Introduction

(a) In the context of the investigation described herein, I am examining:

(i) whether, by reference to the adequacy criteria identified in Article 25(2) of the Directive 95/46/EC[1] ("**the Directive**"), the United States ("the **US**") ensures adequate protection for the data protection rights of EU citizens; and,

(ii) if and to the extent that the US does not ensure adequate protection, whether it is open to FB-I to rely on one or more of the derogations

[1] The full title of the Directive is 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.

provided for at Article 26 of the Directive to legitimise the transfer of subscribers' personal data to the US, if indeed, such transfers continue to take place following the demise of Decision 520/2000/EC ("the **Safe Harbour Decision**").

(b) While my investigation remains ongoing, I have formed the view, on a draft basis, and pending receipt of such further submissions as the Complainant and/or FB-I may wish to submit, that a legal remedy compatible with Article 47 of the Charter of Fundamental Rights of the European Union ("the **Charter**") is not available in the US to EU citizens 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. Against that backdrop, I consider that the SCC Decisions (as defined below) are likely to offend against Article 47 of the Charter insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US notwithstanding the absence of any possibility for any such citizen to pursue effective legal remedies in the US. I emphasise again that this view has been reached on a provisional basis, and this view, when articulated herein, is to be regarded as subject to receipt of such further submissions as the Complainant and/or FB-I may wish to make.

(c) As a matter of EU law, the validity of the SCC Decisions cannot be determined by me, or, indeed, by the national courts of this jurisdiction. Accordingly, I consider that I am bound by the judgment of the Court of Justice of the European Union ("**CJEU**") delivered on 6 October 2015 in proceedings titled *Schrems v. Data Protection Commissioner*[2] to engage in legal proceedings before a national court, without delay, so that (i) I may put forward to that national court the objections to the SCC Decisions, which I consider well-founded; and (ii) the national court may, in turn, if it shares my doubts as to the validity of those decisions, make a reference for a preliminary ruling by the CJEU for the purpose of establishing the validity or otherwise of the SCC Decisions.

[2] Case No. C-362/14

(d) Having regard to the nature of the rights engaged herein, the sequence of events that led to my investigation, and the fact that I consider that I cannot conclude my investigation without obtaining a ruling of the CJEU on the validity of the SCC Decisions, I also consider it appropriate that I should commence such proceedings before the national Court notwithstanding the fact that other elements of my investigation remain ongoing.

II. The Draft Nature of this Decision

This decision is issued in "draft" format to preserve the right of the Complainant and/or FB-I to make such further submissions as they may wish to make in relation to its terms, and to allow me to give full consideration to such submissions in due course. For the reasons outlined above, however, and in circumstances where (a) it is my intention to join the Complainant and FB-I to the proceedings before the national Court; (b) I am presently bound to comply with the terms of the SCC Decisions as a matter of both national and EU law; (c) my investigation to date has resulted in my having concluded, subject to further submissions, that there are well-founded objections to the SCC Decisions and doubts as to their compatibility with Article 47 of the Charter; and (d) I consider that I cannot conclude my investigation without obtaining a ruling of the CJEU on the validity of the SCC Decisions, I believe it is appropriate that I would commence those proceedings forthwith so that the substance of the Complainant's complaint, and the view I have formed in relation to portion of that complaint, can be examined and determined by a court of competent jurisdiction at the earliest possible opportunity.

BACKGROUND

Data transfers from the European Economic Area to third countries

1. Article 25(1) of the Directive establishes a general rule prohibiting the transfer of personal data outside the European Economic Area 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.

2. The criteria by reference to which the adequacy of the level of protection available within a third country is to be assessed are set out at Article 25(2) of the Directive.

3. With a view to ensuring the harmonious application of the general rule against third country transfers, Article 25(6) confers a power on the European Commission to make a finding that a particular third country does indeed ensure an adequate level of protection, so that, in principle, personal data may be transferred from any EU Member State to that third country. Where a decision containing such a finding is made, Member States are required to *"take the measures necessary to comply with the Commission's decision"* (see Article 25(6) of the Directive).

4. It is also open to the Commission 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. (See sub-Articles 25(3), 25(4) and 25(5) of the Directive).

5. As well as providing for findings that a particular third country ensures adequate protection, the Directive also makes provision for a number of derogations from the general prohibition on transfers out of the European Economic Area, so that, subject to the conditions laid down in the Directive, transfers to a third country may be undertaken even if it has not been not established that the third country in question ensures an adequate level of protection.

6. 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. For example, no issue will arise if *"the data subject has given his consent unambiguously to the proposed transfer."*

7. Separately, Article 26(2) provides that,

> *"without prejudice to paragraph 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 …"*

One specific mechanism identified as providing adequate safeguards in this context is that referenced within the text of Article 26(2) itself, i.e. *"appropriate contractual clauses"*.

8. Article 26(4) of the Directive in turn provides that, in accordance with the procedure referred to in Article 31(2) thereof, the Commission may decide *"that certain contractual clauses offer sufficient safeguards as required by paragraph 2."* Where the Commission makes a decision in such terms, Member States are bound to *"take the necessary measures to comply with the Commission's decision."*

9. Where the particular form of contractual clauses identified by the Commission as providing sufficient safeguards for the protection of individuals' data protection rights 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.

10. As at the date of this draft decision, the Commission has approved four sets of standard contractual clauses as fulfilling the requirements of Article 26(4) of the Directive. These 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;[3]

    (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;[4]

    (3) Commission Decision 2002/16/EC of 27 December 2001 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;[5] and,

[3] OJ L 181, 4.7.2001, p. 19
[4] OJ L 385, 29.12.2004, p. 74
[5] OJ L 6, 10.1.2002, p. 52

(4) 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 Parliament and of the Council.[6]

11. For ease of reference, these decisions are hereinafter referred to collectively as "the **SCC Decisions**". I note, however, that Commission Decision 2002/16/EC was repealed by Commission Decision 2010/87/EU and is no longer in force.

National data protection legislation

12. The data transfer rules established under Directive 95/46/EC were transposed into national law by means of the Data Protection (Amendment) Act, 2003. Amongst other things, that Act introduced a new Section 11 into the Data Protection Act, 1988. Section 11(2) provides that, where a finding has been made by the European 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 Data Protection Acts, 1988 and 2003. Likewise, Section 11(4)(c) 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 Commissioner shall comply with that decision.

13. Other notable features of Section 11 include sub-sections (7) to (12), inclusively, which vest in the Commissioner the power to serve a notice prohibiting the transfer of personal data from the State to any place outside the State, subject to a right of appeal to the Circuit Court in favour of party to whom any such notice is directed.

Transfers between the EU and the United States

14. On 26 July 2000, the European Commission adopted the Safe Harbour Decision, establishing the so-called 'safe harbour' arrangements for EU-US data transfers. Whilst the decision did not constitute the US as a third country recognised as ensuring "an adequate level of protection" for the purposes of Article 25(6) of the Directive, it nonetheless provided that EU-US transfers were permissible under its terms provided the entity to whom the data was being transferred self-certified that it complied with

[6] OJ L 39, 12.2.2010, p. 5

(a) the safe harbour privacy principles and (b) a set of "frequently asked questions", both published by the US Department of Commerce and incorporated into the Safe Harbour Decision at Annexes 1 and 2 thereof.

15. It appears to be commonly accepted that, over time, the safe harbour arrangements became the primary mechanism by which data controllers established in the EU sought to legitimise data transfers to the US.

16. In recent years, the relative importance of the safe harbour arrangements increased substantially, reflecting exponential growth in the volume of EU-US data transfers generated by large-scale technology companies operating on a global basis.

The Snowden Document Disclosure

17. In **June 2013**, Edward Snowden, a contractor engaged through a third party to undertake work for the US National Security Agency ("**NSA**"), disclosed documents revealing 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.

Complaint filed by the Complainant

18. On **25 June 2013**, the Complainant filed a complaint with the Office of the Data Protection Commissioner. In essence, the complaint contended that, in light of the Snowden document disclosure, the transfer of personal data relating to Facebook's European subscribers by FB-I to its US parent, Facebook Inc., was unlawful under both national and EU data protection law. This contention was made on the basis that the Safe Harbour Decision could not be said to legitimise such transfers in circumstances where (inter alia):

    (a) data privacy rights are protected in express terms under the Charter;

    (b) under a programme called "PRISM", and on the back of the data transfers effected under the safe harbour arrangements, the NSA was in a position to secure generalised access to European subscribers' data in a manner incompatible with subscribers' charter-protected data privacy rights; and,

(c) The safe harbour arrangements offered no meaningful protection for the data privacy rights of Facebook's European subscribers, leaving such subscribers without any means of vindicating their rights in the US, or obtaining redress in relation to damage suffered as a result of the NSA's actions.

19. In practical terms, the complaint sought to mount a full-frontal challenge to the Safe Harbour Decision.

20. On receipt of the Complainant's complaint, this Office took the view that, in circumstances where the European Commission had adopted the Safe Harbour Decision establishing and/or endorsing the safe harbour arrangements, the Commissioner was bound to accept that decision as binding upon him in light of Article 25(6) of the Directive and Section 11(2) of the Data Protection Acts, 1988 and 2003. Accordingly, the Commissioner declined to investigate the complaint, deeming it unsustainable in law. That position was challenged by the Complainant by way of judicial review proceedings commenced on **21 October 2013**. In those proceedings, orders were sought that would quash the Commissioner's refusal to investigate and direct the Commissioner to investigate and decide the complaint on its merits.

The European Commission's Response to the Snowden Document Disclosure

21. In response to concerns expressed by the European Commission arising from the Snowden document disclosure, the US agreed to participate in an *ad hoc* EU/US Working Group established in **July 2013** to facilitate a fact-finding exercise by the Commission under which the Commission would be afforded an opportunity to seek clarifications on the scope of the programmes revealed by Mr. Snowden, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to individuals in the EU, and the different levels of protection and procedural safeguards that apply to persons resident in the US and EU respectively.

22. On **27 November 2013**, the European Commission published a report setting out the findings of the EU Co-Chairs of the ad hoc EU/US Working Group. Amongst other things, the report noted that, in the course of the Working Group's discussions, the US had confirmed the existence of the PRISM programme, identifying it as a programme

authorised and/or operated under Section 702 of the Foreign Intelligence Surveillance Act, 1978 ("**FISA**"). More specifically, the US was recorded as having confirmed that, on the basis of Section 702 of FISA, electronically stored data, including content data, was collected *"by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube."*

23. The report went on to note the following points:

- *"The US also confirmed that Section 702 provides the legal basis for so-called 'upstream collection'; this is understood to be the interception of Internet communications by the NSA as they transit through the US 3 (e.g. through cables, at transmission points). Section 702 does not require the government to identify particular targets or give the Foreign Intelligence Surveillance Court (hereafter 'FISC') a rationale for individual targeting. Section 702 states that a specific warrant for each target is not necessary."* [7]

- *"The US stated that no blanket or bulk collection of data is carried out under Section 702, because collection of data takes place only for a specified foreign intelligence purpose. The actual scope of this limitation remains unclear as the concept of foreign intelligence has only been explained in the abstract terms set out hereafter and it remains unclear for exactly which purposes foreign intelligence is collected."* [8]

24. Under the heading "Summary of Main Findings", the report stated as follows:

"(1) Under US law, a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. Other elements remain unclear, including the number of EU

[7] Paragraph 2.1.1 of the Report

[8] Paragraph 2.1.1 of the Report

citizens affected by these surveillance programmes and the geographical scope of surveillance programmes under Section 702.

(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely:

i. Collection of data pertaining to US persons is, in principle, not authorised under Section 702. Where it is authorised, data of US persons is considered to be "foreign intelligence" only if necessary to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it relates to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.

ii. The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.

iii. Under both Section 215 and Section 702, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.

(3) Moreover, under US surveillance programmes, different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis).

(4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions

applicable to these programmes. This is especially relevant regarding Executive Order 12333.

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

25. On the same date, the Commission published a separate document titled "Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU." [9] In that document, and drawing on the findings of the ad hoc EU/US Working Group, the Commission noted (under the heading "Limitations and redress possibilities") that,

> *"… safeguards that are provided under US law are mostly available to US citizens or legal residents. Moreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes."*[10]

26. The document went on to make 13 specific recommendations in relation to changes the Commission considered would need to be made to the safe harbour arrangements in the context of ongoing negotiations with the US.

Judgments in the Complainant's Judicial Review Proceedings

27. The Complainant's Judicial Review proceedings came on for hearing in the High Court on **29 April 2014**. Judgment was delivered by Mr Justice Hogan on **18 June 2014**. Judge Hogan determined 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

[9] COM (2013) 847 Final

[10] Paragraph 7.2

the Commissioner was bound, absolutely, by the Safe Harbour Decision having regard to Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, the provisions of Article 25(6) of the Directive notwithstanding. Judge Hogan considered this approach to be necessary and appropriate in circumstances where he noted (in his formal request for a preliminary ruling) that "no issue was ever raised in these proceedings concerning the actions of Facebook Ireland/Facebook, as such … [so that] … the real question was whether the Commissioner was bound by the earlier findings to this effect by the European Commission in the Safe Harbour Decision. In other words, this was really a complaint concerning the terms of that decision rather than the manner in which the Commissioner had applied it …" [11]

28. The CJEU delivered its judgment on **6 October 2015**. Whilst 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 Court, the then Commissioner was not at liberty to adopt any measure contrary to its terms, the court nonetheless found that, as a matter of EU law, the Safe Harbour Decision did not preclude the conduct of an investigation into EU-US data transfers so that the Commissioner ought properly to have investigated the Complainant's complaint with all due diligence.

29. The CJEU also concluded that, as a matter of EU law, the Safe Harbour Decision was invalid. Amongst other things, the CJEU determined that, by failing to afford EU citizens any possibility of pursuing effective legal remedies in the US in connection with any alleged contravention of their rights under Articles 7 and/or 8 of the Charter, the safe harbour arrangements were in breach of Article 47 of the Charter. The Court addressed this point in the following terms:

> *"90. … the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States*

[11] See paragraph 19 of Judge Hogan's Request for a Preliminary Ruling under Article 267 TFEU, dated 17 July 2014.

authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

…

95. … legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law."

30. The judgment also recorded (at paragraph 87) the Court's finding that,

> *" … to establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in Digital Rights Ireland and Others, C 293/12 and C 594/12, EU:C:2014:238, paragraph 33 and the case-law cited)."*

31. In addition—and significantly for present purposes as will be explained further below—the CJEU also ruled as follows (at paragraphs 63—65):

"63. ... 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 Directive 95/46 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, as in the main proceedings, 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.

64. 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 subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in T & L Sugars and Sidul Açúcares v Commission, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

65. 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 subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal

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

32. Thereafter, the Complainant's Judicial Review proceedings came back before the High Court. On **20 October 2015**, an Order was made by Judge Hogan quashing the refusal to investigate the Complainant's complaint and remitting the complaint back to this Office for investigation.

Post-litigation investigation of the Complainant's complaint

33. Immediately thereafter, my office opened its investigation into the Complainant's complaint. In circumstances where there was by now no question but that EU/US transfers of Facebook subscriber data could no longer be undertaken under the safe harbour arrangements, the investigation has sought to establish whether, following the demise of the Safe Harbour Decision, the transfer of personal data relating to its European subscribers by FB-I to Facebook Inc. is lawful. To that end, I set out to examine (by reference to the Complainant's complaint as it relates to interferences on national security grounds with citizen's data privacy rights):

(a) 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,

(b) if and to the extent that the US does not ensure adequate protection, whether it is open to FB-I to rely on one or more of the derogations provided for at Article 26 of the Directive to legitimise the transfer of subscribers' personal data to the US, if indeed, such transfers continue to take place.

34. In practical terms, my investigation has proceeded in two distinct strands, running in parallel. **Strand 1** has comprised a factual investigation focused on establishing whether FB-I has continued to transfer subscribers' personal data to the US

subsequent to the CJEU Judgment of 6 October 2015. If and to the extent that it does, my investigation has also sought to examine the legal bases on which such transfers are effected. Separately, **Strand 2** 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.

35. My Office notified FB-I of the commencement of the investigation by letter dated **3 November 2015**. Separately, it invited the Complainant to reformulate his complaint so as to focus, not on the (now defunct) safe harbour arrangements, but on such derogations (if any) as may be relied on by FB-I to legitimise data transfers to Facebook Inc. post-6 October 2015. The Complainant duly submitted his reformulated complaint on **1 December 2015**. Having secured access in the interim to one or more of the data processing agreements to which FB-I and Facebook Inc. are party, that complaint referred to the nature and extent of those parties' reliance on the SCC Decisions. (A copy of the complaint is contained at **Annex 1** of this Draft Decision). In particular, Mr Schrems made the following complaints:

> "*'Facebook Ireland Ltd' has not proven that [its] alternative agreement was authorized by the DPC under Section 10(4)(ix) DPA. Even if it would be, such an authorization would be invalid and void in the light of the judgments C-362/14 and Schrems –v- the Data Protection Commissioner and therefore irrelevant in this procedure.*"
>
> *...*
>
> *Even if the current and all previous agreements between 'Facebook Ireland Ltd' and 'Facebook Inc' would not suffer from the countless formal insufficiencies above and would be binding for the DPC (which it is not), 'Facebook Ireland Ltd' could still not rely on them in the given situation of factual 'mass surveillance' and applicable US laws that violate Art 7, 8 and 47 of the CFR (as the CJEU has held) and the Irish Constitution (as the Irish High Court has held)."*

Strand 1 of the Investigation

36. In the course of exchanges between FB-I and this Office in relation to Strand 1, FB-I has acknowledged that it continues to transfer personal data relating to Facebook

subscribers resident in the European Union to its US-established parent and, further, that it does so, in large part, on the basis of its contention that—by means of the deployment of the form of standard contractual clauses set out in the Annexes to the SCC Decisions—the company 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.

Strand 2 of the Investigation

37. By definition, the SCC Decisions operate as a derogation from the requirements of Article 25(1) of the Directive. As such, they are deployed by EU-established data controllers where personal data is to be transferred to a third country that has not been the subject of an adequacy finding. Accordingly, to the extent that FB-I relies on the SCC Decisions to legitimise the transfer of subscribers' personal data to the US, I consider that two key questions require examination in the context of this part of my investigation. These are:

(1) Does the US ensure adequate protection for the data protection rights of EU citizens?

(2) If not, do 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?

Noting the observations made by Judge Hogan at paragraph 19 of his Request for a Preliminary Ruling of 17 July 2014, I consider it appropriate to formulate these questions in general terms, reflecting the fact that the Complainant's reformulated complaint requires a determination, not on the actions of FB-I or Facebook Inc, as such, but on the question as to whether the protections the SCC Decisions purport to provide, in fact provide adequate safeguards for the protection of the data privacy rights of EU citizens in accordance with Article 26(2) of the Directive.

38. As noted above, it is also important to bear in mind that these questions fall to be examined by reference to the Complainant's complaint as it relates to interferences with citizen's data privacy rights on national security grounds.

39. In examining the first of these questions, I have noted that, while the CJEU did not make a positive finding to the effect that the US does not ensure an adequate level of protection within the meaning of Article 25(2) of the Directive, it did nonetheless note that:

- *"[The Safe Harbour Decision] enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the person whose personal data is or could be transferred from the European Union to the United States."* [12]

- *"[The Safe Harbour Decision] does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is data is transferred from the European Union to the United States, interference which the State entitles of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.* [13]

40. The Court appears to have inferred from the absence of any such findings in the Safe Harbour Decision that, under the laws of the US, the data protection rights of citizens whose data is transferred from the European Union to the US is, as a matter of fact, at risk of interference by US State entities on national security grounds and that such interference is not subject to the range of safeguards that would apply in the EU. It appears that, in drawing that inference, the Court relied, at least in part, on the findings contained in the *ad hoc* EU/US Working Group Report dated 27 November 2013.[14]

41. I am aware that, subsequent to the report referred to in the immediately preceding paragraph, the laws of the US have been the subject of amendment, to include those changes described in the following terms in a Communication from the European Commission to the European Parliament and the Council dated 29 February 2016:

> *"In parallel, important initiatives were launched that led to significant changes in the US legal order. On 17 January 2014, President Obama*

[12] Para. 87

[13] At paragraph 88

[14] See paragraph 90 of the Judgment

announced reforms of U.S. signals intelligence activities which were subsequently laid down in Presidential Policy Directive 28 (PPD-28). Importantly, these reforms provided for the extension of certain privacy protections to non-Americans as well as a refocussing of data collection away from bulk collection towards an approach that prioritises targeted collection and access. The Commission welcomed those new orientations as an important step in the right direction. This reform process was also instrumental in informing the discussions with the U.S. on the EU-U.S. Privacy Shield. Further changes have been introduced since then. For instance, in June 2015 the U.S. passed the USA Freedom Act which modified certain U.S. surveillance programmes, strengthened judicial oversight and increased public transparency about their use. Finally, on 10 February 2016, the U.S. Congress passed the Judicial Redress Act which was signed into law by President Obama on 24 February 2016. [15]

42. In light of these changes, and given that, in its decision in *Schrems*, the CJEU did not have the opportunity to consider and weigh direct evidence of the nature and/or extent of the interferences with the Charter-protected rights of EU citizens once their personal data had been transferred to the US, or of the safeguards by which such rights are protected under US law, I consider it both necessary and appropriate that I should examine and form my own independent view on the question as to whether or not the US ensures adequate protection for the data protection rights of EU citizens whose data is transferred to that jurisdiction. To assist in this regard, I have sought independent expert advice on certain matters of US law. For the sake of completeness, I also note that I have received unsolicited submissions from the United States Government comprising copies of materials submitted by the United States to the European Commission in support of the Privacy Shield Framework.

43. My investigation is ongoing on this issue. However, on the basis of my examination of these issues to date, it appears to me, at the current stage of my investigation, and subject to such further submissions as may be made, that, notwithstanding the above-referred changes in the US legal order, it remains the case that, even now, a legal remedy compatible with Article 47 of the Charter is not available in the US to EU

[15] COM(2016)117 Final

citizens 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.

44. In this regard, it is important to note that EU citizens are not completely without redress in the US, and that a number of remedial mechanisms are available under US law.

45. The problem is, as will now be set out, that, considered by reference to EU law, there are both specific and general deficiencies in those remedial mechanisms:

(1) From a specific perspective, the remedies are fragmented, and subject to limitations that impact on their effectiveness to a material extent; moreover, they arise only in particular factual circumstances, and are not sufficiently broad in scope 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.

(2) From a more general perspective, the "*standing*" admissibility requirements of the US federal courts operate as a constraint on all forms of relief available.

46. Turning to the specific inadequacies with the remedial framework, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801 et seq) provides a number of remedies to challenge unlawful electronic surveillance. These include:

(1) The possibility for individuals to bring a civil cause of action for money damages against the US when information about them has been unlawfully and wilfully used or disclosed (18 U.S.C. §2712);

(2) The possibility for individuals to sue US government officials for damages where there has been unauthorized electronic surveillance or where information obtained by unauthorized electronic surveillance has been disclosed (50 U.S.C. §1810); and

(3) The possibility for individuals to challenge the legality of surveillance (and to seek to suppress the information) in the event that the US government intends to use or disclose any information obtained or derived from electronic

surveillance against the individual in judicial or administrative proceedings in the US (50 U.S.C. §1806).

47. These provisions are subject to a number of important limitations, material in their nature and extent. For example:

(1) An action under (18 U.S.C. §2712) requires a plaintiff to establish, not just that the use or disclosure of their information was unlawful, but that such violation was "wilful" in the sense that it was knowing or reckless (although it does not appear to be necessary to establish that the violation was done with the conscious objective of committing a violation).

(2) An action under 18 U.S.C. §2712 is further limited by the fact that 50 U.S.C. §1806 adopts a two-tiered protection, distinguishing between a "United States person", which, insofar as natural persons are concerned, is defined as "a citizen of the United States, [and] an alien lawfully admitted for permanent residence" (see 50 U.S.C. §1801(i)). The data of a "United States person" acquired under FISA is protected by what are described as "minimization procedures" (designed to minimize acquisition, retention and dissemination of information) (50 U.S.C. §1801(h)), which "minimization procedures" do not apply to the data of EU data subjects generally (as opposed to those lawfully admitted for permanent residence). Moreover, 50 U.S.C. §1845 stipulates that further provisions must be observed for use and disclosure of information acquired from pen registers or trap and trace devices concerning US persons. Thus, while all aggrieved persons (including all EU data subjects) may bring suit under 18 U.S.C. §2712, EU citizens who are not US citizens or residents would not be able to bring a claim under 18 U.S.C. §2712 for non-compliance with the minimization procedures or for non-compliance with the other provisions identified by 50 U.S.C. §1845.

(3) The significant limitation with 50 U.S.C. §1810 is that this provision does not operate as a waiver of sovereign immunity, which means that the US cannot be held liable under this section and the utility of pursuing individual officers may is questionable.

(4) While it may operate as an important safeguard within the overall statutory scheme established by FISA and while EU citizens have recourse to motions to suppress unlawfully obtained data, the possibility of challenging the legality of surveillance and suppression of information (50 U.S.C. §1806) does not, in reality, comprise a remedy for unlawful interference with personal data at all, given that it is not a free-standing mechanism that can be invoked, but rather is more akin to a defensive protection for the individual in administrative and judicial proceedings.

48. EU data subjects may also seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes, pursuant to:

(1) The Computer Fraud Abuse Act (18 U.S.C. §1030);

(2) The Electronic Communications Privacy Act (18 U.S.C. §§2701-2712); and

(3) The Right to Financial Privacy Act (12 U.S.C. §3417).

49. Again, these causes of action concern specific data, targets and/or types of access (e.g. remote access of a computer via the Internet) and are available under certain conditions (such as, intentional/wilful conduct, conduct outside of official capacity, harm suffered). The following points are relevant in that context:

(1) While the Computer Fraud Abuse Act (18 U.S.C. §1030) does afford a civil remedy in damages and/or injunctive relief where a person has suffered "*damage or loss*" due to a violation of the legislation, again there are a number of limitations. In the first instance, some US courts have held that federal government agencies and officials are immune from suit under the Computer Fraud Abuse Act. Courts are also split as to whether plaintiffs must allege both damage and loss in order to have a stateable claim under this legislation, albeit that some courts have concluded that alleging costs reasonably occurred responding to an alleged offence under the legislation may suffice. A requirement to allege specific damage and loss, as will be considered further below, is not in accordance with the requirements of Article 47 of the Charter as interpreted in the *Schrems* judgment (at paragraphs 87 and 89).

(2) The Electronic Communications Privacy Act consists of the Wiretap Act[16] and the Stored Communications Act ("SCA").[17] The provisions of these Acts are focussed on intentional unauthorised access to electronic communications (see 18 U.S.C. §§2701—2702), with the Wiretap Act applying to communications that are intercepted while in transmission, and the SCA applying to the unauthorized access of stored communications. Pursuant to 18 U.S.C. §2712, a person who is aggrieved by any wilful violation of the Wiretap Act[18] or the SCA[19] may bring an action in the US District Court against the US to recover damages for wrongful collection of information and/or wrongful use and disclosure of same. These claims are subject to the constraints of the requirement of a "*wilful*" violation (which has already been discussed above). There is also uncertainty as to the extent to which damages actions are available against governmental entities that breach either the Wiretap Act or the SCA.

(3) The Right to Financial Privacy Act (12 U.S.C. §3417) obviously focuses on disclosure of financial information.

50. The Freedom of Information Act ("**the FOIA**") is also a means for non-US persons to seek access to existing federal agency records, including where these contain the individual's personal data (5 U.S.C. §552). However, the FOIA is unsatisfactory from a remedial perspective, as it does not provide an avenue for individual recourse against interference with personal data in and of itself, but rather is intended to enable individuals to obtain access to relevant information held by national intelligence agencies. Even then, further limitations arise, and agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations.

51. It is also the case that the available remedies do not deal with certain legal bases available to US intelligence authorities to access and process data, such as Executive Order 12333, which confers various surveillance powers on intelligence agencies.

[16] 18 U.S.C. §2510 et seq.

[17] 18 U.S.C. §2701 et seq

[18] 18 U.S.C. §2510 et seq.

[19] 18 U.S.C. §2701 et seq

Accordingly, it is simply not possible to assess whether or not the remedies outlined above are sufficient to address the full extent of the activities of the intelligence authorities in question.

52. From the more general perspective identified above, an overarching issue applying to all of these causes of actions is that arising from US constitutional "*standing*" requirements, which are mandated by the "*case or controversy*" condition of Article III of the US Constitution. In that regard, I note that, in its recently-published draft decision on the implementation of the proposed "Privacy Shield", the European Commission has observed, in relation to the redress mechanisms available to EU citizens pre-Privacy Shield, that,

> *"even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available courses of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing", which restricts access to ordinary courts."*

53. I understand that, as a matter of US law, an individual must satisfy each of the following three requirements in order to establish "standing" sufficient to maintain an action in law:

(1) That he or she has suffered an injury in fact, i.e. an invasion of a legal protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical;

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

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

54. On their terms, I consider that these requirements appear to be incompatible with EU law in circumstances where, as a matter of EU law, it is not necessary to demonstrate an adverse consequence as a result of an interference with Articles 7 and 8 of the

Charter in order to secure redress of a violation of the said Articles. As the CJEU observed at paragraph 87 of its judgment in *Schrems:*

> *"To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference."*

55. The extent to which the "standing" requirements applicable under US law would appear to operate to limit an individual's capacity to access a remedy in this context in a manner incompatible with EU law is illustrated by the decision of the US Supreme Court in *Clapper v. Amnesty International USA*[20]. In that case, the plaintiffs sought to pursue allegations that certain amendments to FISA were unconstitutional because of the plaintiffs' stated belief that there was an objectively reasonable likelihood that their communications with foreign contacts would be intercepted in the future, or, alternatively, because they were already suffering injury because they found themselves having to take costly and burdensome measures to protect the confidentiality of their international communications. The US Supreme Court held that the plaintiffs lacked standing because, inter alia, their fears were "highly speculative" in nature, and because "they could not demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm." I consider that such an approach is not reconcilable with that outlined in *Schrems* where the CJEU made it clear that a claimant cannot be required to demonstrate that harm has in fact been suffered as a result of the interference alleged.

56. It is also relevant to note in this context that, under the Federal Rules of Procedure applicable in the US, a claim may only be pursued by a claimant where the claimant's lawyer certifies that "the factual contentions [made] have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery."[21] Taken with the analysis adopted by the Court in *Clapper* in connection with the making of "speculative" claims regarding alleged violations of data privacy rights, the Federal Rules of Procedure

[20] 133 S. Ct. 1138 (2013)

[21] Fed. R. Civ. P. 11(b)(3)

would appear to preclude the bringing of precisely the kind of complaint now before me.

The Privacy Act & the Judicial Redress Act

57. Subject to a range of exemptions, the Privacy Act confers on US citizens a statutory right to access records or information held about them by government agencies, to review such records, and to have a copy made. The Act also limits the extent to which federal agencies can share and disclose information about private individuals. In the event of a violation by such an agency of particular provisions of the Act, the individual affected may bring a civil action in which a range of reliefs may be granted, including but not limited, to damages.

58. I note that, on 24 February 2016, the Judicial Redress Act ("**JRA**") was signed into law in the US, albeit that it will not become effective until the expiry of a period of 90 days after its enactment. I understand that, in practical terms, the JRA extends certain of the existing rights of action (and remedies) available to US citizens under the Privacy Act to non-US citizens (including citizens of the European Union) such that an EU citizen will be able to bring suit in a federal district court for certain Privacy Act violations by designated government agencies in the US. In this regard, the JRA provides that, with respect to "covered records", a citizen of a "covered country" may bring a civil action against a federal agency and obtain civil remedies, broadly in the same manner, to the same extent, and subject to the same limitations as a US citizen or permanent legal resident under identified provisions of the Privacy Act.

59. Whilst, on the face of it, the JRA purports to open up access for EU citizens to remedies that were not previously available to them, the effectiveness of those remedies is subject to a number of important limitations and/or restrictions, including the following:

    (1) Not all of the remedies available to US citizens under the Privacy Act have been extended to non-US citizens. Notably, it will not be open to an EU citizen to bring a civil action in the event that a designated agency "fails to maintain any record concerning any individual with such accuracy, relevant, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights , or opportunities of, or benefits

to the individual that may be made on the basis of such record and consequently a determination is made which is adverse to the individual" (5 U.S.C. Section 552a(d)(1)(C)).

(2) Certain of the remedies that will be made available to non-US citizens will be available only in those cases where an agency intentionally or wilfully discloses a record in violation of a limited number of provisions of the Act and where that disclosure can be shown to have had "an adverse effect" on the individual. As noted above at paragraph 47, the requirement to establish that a disclosure complained of was made wilfully necessarily operates to limit the effectiveness of the remedy now to be made available to non-US citizens.

(3) More importantly, although not yet clear because the JRA has not yet been applied by the courts, it is reasonable to expect that existing limitations that apply to such remedies as are available to US citizens under the Privacy Act will also apply to such remedies as will be available to non-US citizens under the JRA. This point is of particular importance in the context of any examination of the remedies available to EU citizens in contexts where US national security interests are engaged because (for example) regulations have been adopted by the National Security Agency under relevant statutory exemption schemes, the effect of which is to foreclose the availability of remedies for US citizens under the Privacy Act in respect of records exempted by the NSA or properly classified pursuant to Executive Order to protect US national security interests. To the extent that such exemptions are likewise applied to restrict the availability of remedies for non-US citizens under the JRA, it necessarily follows that the JRA will be of no utility in the context of a complaint such as that made by the Complainant herein.

(4) Certain of the definitions deployed in the JRA would also appear to operate to limit the remedies afforded non-US citizens by its terms. The definition of the terms "designated Federal agency or component," "covered record" and "covered country" require consideration in this context.

(5) The Act will apply only to a "designated Federal agency or component", defined as meaning a Federal agency or component of an agency designated by

the US Attorney General in accordance with subsection (e) of the Act. As matters stand, it is unclear whether agencies such as the National Security Agency will be brought within its scope. It is also important to note that, with some limited exceptions, no agency may be brought within the scope of the Act "without the concurrence of the head of the relevant agency, or the component of the agency to which the component belongs." In practical terms, therefore, the intended scope of the JRA is capable of becoming greatly narrowed.

(6) A country or regional economic integration organization must meet certain requirements to be designated a "covered country," including entering into an agreement with the US regarding privacy protections for shared information. A reading of this definition on its face implies that private entities located within the US will not fall within the definition of a "covered country". This point will have relevance where there are transfers of data from the EU to US private entities and where the transferred data in turn comes into the possession of a US security agency.

(7) The Act provides that the term "covered record" has the same meaning as the term "record" in the Privacy Act, once the record is transferred "by a public authority of, or private entity within," a covered country, "to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses." This definition is problematic in two respects.

a. First, it is not clear if a record originating in a foreign covered country (or a private entity therein) that was provided to the designated agency or component indirectly (for example, by or through a related private entity established in the US) could still be considered a "covered record."

b. Second, interpretation of the term "covered country" affects the designation of a record as a "covered record". As noted above, a strict reading of the definition of the term "covered country" would indicate that the US itself would not be considered a "covered country."

> Because the JRA implicates sovereign immunity, a US court may strictly construe the statutory language to find that a record that was transferred to a designated US Federal agency or component, not directly by an authority or private entity within a foreign covered country, but indirectly by or through a related private entity established within the US, would thus not qualify as a "covered record."

(8) Clearly, a narrow reading of the terms "covered country" and "covered record" would impact directly (and adversely) on the accessibility of remedies under the JRA, Importantly, such a reading would result in a situation where a remedy would not be available to the Complainant in the context of the complaint presently under investigation.

(9) I have set out above, in general terms, the position as I understand it to be in connection with the issue of standing as it arises under US law. A particular "standing" arises in relation to the capacity of a non-US citizen to access a remedy under the JRA. Specifically, I understand that the US Supreme Court has held that a claimant seeking to recover statutory damages under the Privacy Act must prove, not just that "actual damages" have been incurred, but that he or she has incurred pecuniary loss or damage. Given that the JRA operates by extending Privacy Act remedies to non-US citizens, it follows that a requirement to prove pecuniary loss or damage will also operate as a pre-condition to the availability of particular remedies under the JRA. On the basis of the CJEU's findings in *Schrems*, such a requirement is not compatible with EU.

60. For all of the reasons outlined above, therefore, I have formed the view, subject to consideration of such submissions as may be submitted in due course by the Complainant and FB-I that, at least on the question of redress, the objections raised by the CJEU in its judgment in *Schrems* have not yet been answered.[22]

61. It is also my view that the safeguards purportedly constituted by the standard contract clauses set out in the Annexes to the SCC Decisions do not address the CJEU's

[22] In circumstances where it has not yet been adopted, I have not analysed or taken into account the new suite of arrangements contemplated by the "Privacy Shield" Agreement concluded between the EU and the US.

objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in *Schrems*. Nor could they. On their terms, the standard contract clauses in question 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. Importantly for current purposes, there is no question but that the SCC Decisions are not binding on any US government agency or other US public body; nor do they purport to be so binding. It follows that they 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. On this basis, I have formed the view, subject to consideration of such further submissions as may be filed by the Complainant and FB-I, that the protections purportedly provided by the standard contract clauses contained in the Annexes to the SCC Decisions are limited in their extent and in their application. So far as the question of access to an effective remedy is concerned, it is my view that they cannot be said to ensure adequate safeguards for the protection of the privacy and fundamental rights and freedoms of EU citizens whose data is transferred to the US.

62. Accordingly, I consider that the SCC Decisions are likely to offend against Article 47 of the Charter insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US in the absence in many cases of any possibility for any such citizen to pursue effective legal remedies in the US in the event of any contravention by a US public authority of their rights under Articles 7 and/or 8 of the Charter. That being the case, I consider that the Complainant's contention that SCC Decisions cannot be relied on to legitimise the transfer of the personal data of EU citizens to the US in such circumstances is well founded.

63. As a matter of EU law, however, the validity of the SCC Decisions cannot be determined by me, or, indeed, by the national courts of this jurisdiction. Accordingly, I consider that I am bound by the judgment of the CJEU delivered on 6 October 2015 to engage in legal proceedings before a national court so that (a) I may put forward to that national court the objections to the SCC Decisions, which appear to me to be well-founded; and (b) the national court may in turn, if it shares my doubts as to the

validity of those decisions, make a reference for a preliminary ruling by the CJEU for the purpose of establishing the validity or otherwise of the SCC Decisions.

Conclusions, Findings & Draft Decision

64. I have formed an the view, pending receipt of such further submissions as the Complainant and/or FB-I may wish to submit, that a legal remedy compatible with Article 47 of the Charter is not available in the US to EU citizens whose data is transferred to the US and whose personal data 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. Against that backdrop, I consider that the SCC Decisions are likely to offend against Article 47 of the Charter insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US notwithstanding the absence of a complete framework for any such citizen to pursue effective legal remedies in the US.

65. As a matter of EU law, the validity of the SCC Decisions cannot be determined by me, or, indeed, by the national courts of this jurisdiction. Accordingly, I consider that I am bound by the judgment of the CJEU delivered on 6 October 2015 in *Schrems v. Data Protection Commissioner* to engage in legal proceedings before a national court, without delay, so that:

    (i) I may put forward to that national court the objections to the SCC Decisions, which I consider well-founded; and;

    (ii) the national court may, in turn, if it shares my doubts as to the validity of those decisions, make a reference for a preliminary ruling by the CJEU for the purpose of establishing the validity or otherwise of the SCC Decisions.

66. I intend to commence such proceedings without delay.

67. Having regard to the nature of the rights engaged herein, the sequence of events that led to my investigation, and the fact that I consider that I cannot conclude my investigation without obtaining a ruling of the CJEU on the validity of the SCC Decisions, I also consider it appropriate that I should commence such proceedings

before the national Court notwithstanding the fact that other elements of my investigation remain ongoing.

68. A final decision will be issued following conclusion of the said proceedings. A party to the within complaint procedure who is aggrieved by the said final decision in relation to Mr Schrems' complaint against FB-I will be entitled to appeal that decision to the Circuit Court under Section 26 of the Acts within 21 days of receipt of notification of the final decision.

_____

Helen Dixon
Data Protection Commissioner
24 May, 2016.