THE HIGH COURT

COMMERCIAL

Record No. 2016/4809P

BETWEEN

THE DATA PROTECTION COMMISSIONER

Plaintiff

AND

FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

Defendants

OUTLINE SUBMISSIONS ON BEHALF OF BSA | THE SOFTWARE ALLIANCE

PRELIMINARY

1. On 19 July 2016 this Court (McGovern J) made an order joining (*inter alia*) BSA Business Software Alliance, Inc., doing business as BSA | The Software Alliance (hereafter "*BSA")* as an *amicus curiae* to these proceedings in the context of the application brought by the Data Protection Commissioner (hereafter "*the DPC"*) for a reference to the Court of Justice of the European Union ("*the CJEU")* pursuant to Article 267 of the Treaty on the Functioning of the European Union ("*the TFEU"*).

2. These submissions are intended to assist the Court in addressing the relief sought at relief number 2 of the Commissioner's Statement of Claim, as follows:

> *"A reference to the [CJEU] pursuant to Article 267 [TFEU] and paragraph 65 of the ruling of the CJEU in Case C-362/14 Schrems v Data Protection Commissioner, 6 October 2015, in order to obtain a preliminary ruling on the validity of the SCC Decisions insofar as applies to data transfers from the EU to the US, having regard to the Charter .. and in particular to Article 7 and/or 8 and/or Article 47 thereof."*

3. As the Court will be aware from the pleadings and the submissions of the parties, the "SCC Decisions" whose validity is sought to be the subject of such a reference, comprise three decisions of the European Commission (hereafter "the Commission") adopted pursuant to Article 26(4) of Directive 95/46/EC of the European Parliament and 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 (hereafter *"the Directive").*[1]

4. Each of these SCC Decisions provides a set of standard contractual clauses which, if adopted by data controllers and/or processors,[2] presumptively permits the transfer of personal data to a third country (i.e. a non-EU state) even though that third country *"does not ensure an adequate level of protection within the meaning of Article 25(2)"* of the Directive. While it will be necessary to look in more detail at the SCC Decisions below[3] – in particular because so little attention is paid to them in the Draft Decision of the DPC[4] – this feature of them is one that warrants immediate emphasis. The SCC Decisions derogate from Article 25 of the Directive (which was, of course, the subject of the CJEU judgment of 6 October 2015 in respect of Mr Schrems' first complaint[5] *(*hereafter *"Schrems")*) and permit data transfers to jurisdictions that do not ensure *"an adequate level of protection*": indeed their whole purpose is to enable data transfers to such jurisdictions, reflecting an important fact, expressly reflected in the Directive itself, that "*cross-border flows of personal data are necessary to the expansion of international trade."* [6]

[1] Commission Decision 2001/497/EC of 15 June 2001, Commission Decision 2004/915/EC of 27 December 2004 and Commission Decision 2010/87/EU of 5 February 2010. For completeness, there is also a fourth decision, relating to a previous version of SCCs, since repealed, namely, Commission Decision 2002/16/EC of 27 December 2001 – no longer available for new uses but which continues to have effect for certain arrangements put in place prior to 15 May 2010.

[2] Hereafter, for convenience, referred to as "*data processors"*.

[3] For ease of reference, in this matter, reference will be made to Commission Decision 2010/87/EU, which appears to be the only SCC Decision germane to the complaints made by Mr Schrems in any event. However, so far as relevant for these proceedings, the Decisions are materially identical.

[4] Draft Decision of the Data Protection Commissioner under section 10(1)(b)(ii) of the Data Protection Acts, 1988 and 2003 of 24 May 2016 (hereafter "*the Draft Decision*"). A copy of the Draft Decision is to be found (*inter alia*) as exhibit "*JOD1*" to the Affidavit of John V O' Dwyer sworn on 31 May 2016.

[5] C-362/14

[6] Recital (56) of the Directive. The critical importance of SCCs for international trade and economic activity, including economic activity within the EU, is abundantly clear from the evidence before the Court. In addition to the Affidavits sworn on behalf of BSA and Digital Europe, very substantial evidence has been put before the Court by Facebook, in particular the Affidavit and Report of Dr Joshua Meltzer (including paragraph 12.2 which addresses the economic impact of a ban on the expert of data from the EU to the US). BSA has sworn an Affidavit though Thomas

5. It follows from the above – though this is not evident from the Draft Decision – that the issues presented here differ significantly from the issues that arose in *Schrems*. At issue there, at least indirectly, was the adequacy of the level of protection for personal data in the United States, though in fact the CJEU did not address that issue in its Judgment.[7] As will be explained, that is not the issue in these proceedings. It follows that the analysis undertaken by the CJEU in *Schrems* does not bear directly on the issues raised here, still less does it suggest the conclusion that the SCC Decisions are invalid. As the Commission stated in the aftermath of the *Schrems* decision, there is a "*clear distinction*" between transfers of data under Article 25 of the Directive (with which *Schrems* was concerned) and transfers pursuant to Article 26.[8] As the Commission also emphasised, the decision in *Schrems* did not affect Article 26 transfers.[9] [10]

6. Even this brief analysis allows one to draw a conclusion that, having regard to the terms of the Draft Decision, is significant, namely, that a finding that the United States – or any other jurisdiction – does not ensure "*an adequate level of protection*" for personal data transferred to it, would not in itself provide a basis for asserting the invalidity of the SCC Decisions or for excluding the transfer of personal data to the United States in reliance on SCCs or any of the other derogations provided for in Article 26. So much is clear from the express and unambiguous provisions of Article 26 itself.

Boué. Earlier in the proceedings an issue was raised by the DPC as to the entitlement of an amicus to adduce evidence. However, no objection has, to date, been taken to Mr Boué's Affidavit and, if any such objection is raised, the matter can be addressed by the Court at that stage.

[7] See paragraphs 97 and 98. In *Schrems*, the CJEU held that the Commission had not made necessary findings about the level of protection provided by US law in the national security context and so the Commission's decision finding that the Safe Harbour programme offered adequate protection could not be upheld. Here, because Article 26 is as a matter of hypothesis, intended to provide for transfers to third countries that do not offer adequate protection, such an inquiry is not relevant.

[8] *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)* (Com (2015) 566 final; 6 November 2015 (hereafter "*the Commission Communication*")

[9] "*In the absence of an adequacy decision under Article 25(6) of Directive 95/46/EC and irrespective of the use of SCCs and/or [binding corporate rules] personal data may still be transferred to entities established in a third country to the extent that one of the alternative derogations set out in Article 26(1) of Directive 95/46/EC applies.*" (the Commission's Communication at page 8; emphasis added)

[10] "In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. *In any case, this will not prevent data protection authorities to investigate particular cases, for instance on the basis of complaints, and to exercise their powers in order to protect individuals." S*tatement of the Article 29 Working Party, available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

7. These submissions are structured by reference to the following broad headings:

(a) The SCC Decisions will first be considered.

(b) The Draft Decision will then be addressed.

(c) Finally, these submissions will address whether the need for a reference has been established and in that context will also address the terms of the question the DPC seeks to have referred.

8. It may first be helpful to set out briefly what appear to BSA to be the key points that emerge from this analysis:

- As already stated, there is a "*clear distinction*" between transfers to third countries that ensure an adequate level of protection under Article 25 of the Directive and transfers to third countries that have not been found to ensure an adequate level of protection under Article 26.

- In common with the other derogations provided for in Article 26, SCCs are intended to facilitate the transfer of personal data from the EU to third countries that *ex hypothesi* do not "*ensure an adequate level of protection*" for the purposes of Article 25.

- It follows that the issue of whether the United States, or any other third country, does or does not "ens*ure an adequate level of protection*" is not determinative for an assessment under Article 26, and even less so in respect of the validity of the SCC Decisions. Despite this fact, the first question asked by the DPC in her Draft Decision is "*whether, by reference to the adequacy criteria identified in Article 25(2) of the Directive 95/46/EC ("the Directive"), the United States ("the US") <u>ensures adequate protection</u> for the data protection rights of EU citizens.*" (Emphasis added).

- The SCCs impose significant obligations on data controllers and provide significant protections for data subjects to which the Draft Decision ought to have given due consideration.

- In addition, the SCC Decisions give national data protection authorities (DPAs) – including the DPC – very important supervisory, oversight and enforcement powers. In particular, Article 4 of each of the SCC Decisions gives DPAs the power to prohibit or suspend data flows in certain circumstances. Again, these important safeguards and protections have not been adequately considered in the Draft Decision.

  To the contrary, the Draft Decision focuses, almost to the exclusion of any other consideration, on the issue of available remedies, particularly judicial remedies, in the United States. This is, in BSA's respectful submission, too narrow a focus and, as a result, the Draft Decision provides an incomplete factual and legal context in which to consider Mr Schrems' *Reformulated Complaint*.

- The Draft Decision in particular fails to address a number of matters which, in BSA's respectful view, are of fundamental importance:

  - The Draft Decision fails to address, or even to identify, the context in which the concerns regarding government access to data transferred to the United States must be assessed, namely that of national security/law enforcement.

  - As a result, the Draft Decision fails to consider ways and means to analyse and resolve factually inconsistent or potentially conflicting requirements in law and practice which are, on any view, highly relevant to any assessment of the position in the United States.[11]

[11] Even if this was an Article 25 "*adequate level of protection*" case - which it is not - given the holding in *Schrems* that this effectively involves a test of *essential equivalence* (see para 73 of the CJEU Judgment), it is clear that the law and practice of the EU and/or EU Member States is relevant.

- The DPC, it is respectfully submitted, addresses the unduly narrow issue of whether the nature and scope of the judicial remedies available in the United States satisfied Article 47 of the Charter; the correct analysis requires a much broader assessment of whether any limitations on the protection of personal data transferred from the EU to the United States (including, but not limited to, any limitations on recourse to a judicial remedy in the United States) go beyond what may be necessary and proportionate to meet objectives of general interest recognised by the EU (to use the language of Article 52 of the Charter) or (to use the language of Article 4(1)(a) of the SCC Decisions) "*go beyond the restrictions necessary in a democratic society"* and "*are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses."*

- Thus Article 4(1)(a) of the SCC Decisions provides for essentially the same balancing exercise as Article 52 of the Charter and therefore enables the requirements of the Charter including (but not limited to) Articles 7, 8 and 47 to be accommodated and reconciled.

- The validity of transfers under Article 26, including transfers effected pursuant to the SCC Decisions, cannot properly be considered or determined on an *a priori* basis or by the application of any sweeping proposition of law. Rather, these issues are fact sensitive and require an assessment of all of the circumstances of the data transfer at issue, including the categories or types of data being transferred, the application of the SCCs and so on. These issues arise in the context of any investigation under Article 4 of the SCC Decisions and, equally, they arise in the context of any issue concerning the validity of those SCC Decisions.

- In light of the above, the Draft Decision provides an inadequate basis for a reference to the CJEU. It is not necessary or appropriate to make the reference sought by the DPC.

- In the event that the Court nonetheless considers it appropriate to make a reference, BSA considers that the form of reference suggested by the DPC is too narrow and would wish to have the opportunity to contribute to the formulation of the question(s) to be referred.

THE SCC DECISIONS

GENERAL

9. Article 26(4) of the Directive empowers the Commission to decide "*that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2"* and, where it does so, Member States "*shall take the necessary measures to comply with the Commission's decision."*

10. Article 26(2) in turn allows a Member State to authorise a transfer or set of transfers to a third country "*where the controller adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights."* It also provides that "*such safeguards may in particular result from appropriate contractual clauses*".

11. As already observed, Article 26 operates by way of derogation from Article 25 of the Directive and expressly applies to authorise the transfer of data to a third country which "*does not ensure an adequate level of protection within the meaning of Article 25(2)."*[12] It follows that the Community legislature (here the European Parliament and EU Council) were clearly of the view that appropriate contractual provisions could provide a sufficiently robust level of protection for data subjects specifically in scenarios where their data were being transferred to a third country which does not offer "*an adequate level of protection"*.

12. While these proceedings are concerned with transfers to the United States, Article 26 applies in principle to transfers to *any* third party country and is not premised or conditional on any particular scope of judicial remedy being available to the data subject in that third country or, indeed, any judicial remedy being available there. The fundamental premise of Article 26, as far as SCCs is concerned at least, is that the contract pursuant to which data are transferred of itself provides sufficient

[12] Article 26(2) of the Directive

protection to data subjects, both in terms of substantive protection and availability of remedies.

13. Article 29 Working Party guidance reinforces this point. As that guidance explains, contracts are "*a means by which adequate safeguards can be provided by the data controller when transferring data outside of the Community … to a third country where the general level of protection is not adequate*."[13] Using contractual clauses can "*make up for the absence of oversight and enforcement mechanisms*"[14] in a third country not deemed to offer an adequate level of data protection.

14. The derogations provided for in Article 26, including that relating to the use of SCCs, (referred to now as "*standard data protection clauses"*) have been maintained in the General Data Protection Regulation (GDPR), a complete overhaul of data protection law that comes into effect in the EU on 25 May 2018, demonstrating the continued relevance and validity of the SCC Decisions. Indeed, far from limiting reliance on the derogations, the GDPR substantially extends the derogations in Article 26, recognising that flows of personal data are necessary for the continued existence and expansion of international trade,[15] and also recognising the limited value of the "*adequacy system"* under Article 25.[16]

15. The practical importance of Article 26 generally, and of the SCC Decisions in particular, is demonstrated by the fact that only a small handful of countries have been deemed "*adequate*" under the Article 25(6) procedure. The vast majority of countries in the world – over 180 – have not yet been positively assessed as providing an adequate level of data protection. In a period of more than 20 years since adoption of the Directive in 1995, the Commission has determined the existence of an adequate level of data protection in relation to *only* nine countries[17] and three regions[18].

[13] Article 29 Working Party Opinion on the Protection of Individuals with regard to the Processing of Personal Data (WP 12), page 16.

[14] *Ibid.* page 18.

[15] As referred to in the first sentence to Recital 101 of the GDPR .

[16] Now article 45 of the GDPR.

[17] Andorra, Argentina, Canada, Faroe Islands, Israel, New Zealand, Switzerland, the United States (in relation to data transferred pursuant to the EU-U.S. Safe Harbour, and now EU-U.S. Privacy Shield), and Uruguay

[18] Guernsey, Isle of Man, and Jersey

16. But for the derogations in Article 26, the system established by the Directive would be unworkable; personal data would largely be held captive in Europe, thwarting the ability of the EU to trade with the majority of the world's countries and of European businesses to operate across EU borders. Such a prohibition would be disproportionate, and contrary to the Charter of Fundamental Rights of the EU (for example, in relation to Article 16, enshrining the freedom to conduct a business[19]) and other objectives of the Union under the EU Treaties. In short, the EU legislature recognised that business requires a different, pragmatic mechanism to supplement the adequacy standard contained in Article 25 and so recognised the need for derogations as set out in Article 26.

17. For example, in the context of the freedom to conduct a business, the CJEU in *Mc Fadden* concluded that a legal measure which *"first, places a burden on the access provider capable of affecting his economic activity and, second, is capable of restricting the freedom available to recipients of such a service from benefiting from access to the internet . . . infringes the former's right of freedom to conduct a business, protected under Article 16 of the Charter, and the right of others to freedom of information, the protection of which is provided for by Article 11 of the Charter*." The Court then restated its established case-law that "*[w]here several fundamental rights protected under EU law are at stake, it is for the national authorities or courts concerned to ensure that a fair balance is struck between those rights."*

18. As the evidence before the court demonstrates, use of SCCs for the purposes of transferring data out of the EU has become critical to the functioning of the modern data-centric economy and global IT sector.

19. Thousands of companies use the standard contractual clauses for millions of data transfers to countries all over the world *every single day* – precisely as the EU legislature had intended. In that regard, the affidavit of Thomas Boué sworn on 17

[19] *See, e.g.*, Case C□484/14 *Mc Fadden*, at paragraphs 82-84, and earlier in the cases cited by the CJEU in those paragraphs.

November 2016 on behalf of BSA, sets out, *inter alia*, survey results that demonstrate the indispensable nature of the SCCs.

THE SAFEGUARDS IN THE SCCS

20. The extensive safeguards contained in the SCCs were adopted after an exhaustive process of consultation and consideration that sought and reflected the views of all EU institutions and the Member States. Each of the Commission's SCC Decisions was adopted in accordance with a "*comitology*" process. This process begins with a Commission proposal. The Article 29 Working Party then issues an opinion on the proposal. The proposal then requires approval from the "*Article 31 Committee*," composed of Member States' representatives. If approved, the proposed decision is then adopted by the College of Commissioners. Throughout this process, the European Parliament and the Council may request the Commission to maintain, amend or withdraw the adequacy decision on the grounds that it exceeds the implementing powers provided for in the Directive. Scrutiny and negotiations around the second set of "*controller to processor"* SCCs (enacted by Commission Implementing Decision 2004/915/EC), for example, lasted approximately eight years.[20]

21. The safeguards in the SCCs represent binding contractual commitments, including to secure personal data, restrict access to data, and control any further transfers of data.[21] The SCCs also create rights for individuals to enforce obligations on organisations that transfer and receive their personal data, and enable independent auditors and EU Member States' data protection authorities to conduct audits[22]. In order to mitigate the risks associated with transfers to non-adequate countries, the safeguards applied to EU citizens' personal data transferred pursuant to the SCCs are robust.

---

[20] *See* Kuner, C, *Improper Implementation of EU Data Protection Law Regarding Use of the Standard Contractual Clauses in Germany* (October 6, 2006). Available at SSRN: http://ssrn.com/abstract=1444813.

[21] Clause 4 of Commission Decision of 15 June 2001, clause 1 of Commission Decision of 27 December 2004 and Clause 4 of Commission Decision of 5 February 2010.

22 For example Clause 8 of Commission Decision of 5 February 2010.

22. The SCC Decisions also narrowly limit the extent to which a party to the SCCs may comply with foreign law enforcement demands for access to data without violating the SCCs.[23]

23. Significantly, the SCCs grant data subjects a right of action against the parties for breach of the various protections under the SCCs.[24] As noted by Kelleher in *Privacy and Data Protection Law in Ireland*[25], in order to deal with the doctrine of privity of contract, the Data Protection Acts provide, at Section 11 (6) that "*the data subject shall have the same right… to enforce a clause of the contract conferring rights on him or her or relating to such rights and… to compensation or damages for breach of such clause, that he or she would have if he or she were party to the contract."*[26] These rights, which can include damages, specific performance, or other injunctions, can be enforced in the EU in accordance with EU and national law, notwithstanding the fact that the breaches occurred in a third country.[27] Therefore – and crucially – data subjects are given a judicial remedy within the EU by the SCCs.

24. The redress that is available ensures that the safeguards are properly respected and enforced where they are infringed. For example:

- **Data subject right to sue / seek court orders**. The third party beneficiary rights clause gives affected data subjects the right to sue the exporter, and under certain circumstances the importer, for damages suffered as a result of breaches of the SCCs by any party or sub-processor.

- **Fall-back remedies**. Even in instances where the data exporter cannot be sued (e.g. because it has ceased to exist), the data subject can still exercise contractual rights against the data importer, or even against its sub-processors.

23 Thus Clause 5(d)(i) of the 2010 Decision requires a data importer to promptly notify the data exporter of any legally binding request for disclosure of personal data by a law enforcement authority unless otherwise prohibited.

24 For example, Clause 6(1) of the 2010 Decision provides that a data subject who has suffered damage as a result of a breach of certain obligations is entitled to receive compensation from the data exporter for the damage suffered.

25 (2nd ed; 2015) at para 18.27

26 See also clause 3 of the 2010 Decision to which section 11(6) gives effect.

27 Thus, Clause 7(1)(b) of the 2010 Decision provides that a claim for compensation for damages may be brought by a data subject in the courts of the member state in which the data exporter is established.

- **Regulatory oversight**. The parties contractually commit to cooperate with Member States' data protection authorities, ensuring oversight of their activities.

- **Scope of investigation**. Data subjects can also complain directly to a Member State's data protection authority. Further, the data exporter and data importer expressly commit to the data protection authority having the power to conduct audits, even over the importer, as if it were in the data protection authority's jurisdiction.

- **Disputes resolved under local law**. Importantly, any dispute between the data subject and the data exporter is resolved in accordance with the governing law of the data exporter (i.e. EU law) – not the law of the country to which the data were exported. It allows data subjects to invoke local law to interpret and enforce the parameters of the safeguards described above.

The parties also commit to abiding by the final and binding decisions of competent courts of the data exporter's country of establishment (*de facto* submitting them to EU law).

25. These important safeguards were not sufficiently considered by the DPC in the Draft Decision. Rather, in just a single paragraph of text, they are dismissed on the basis that they are not binding on any US government agency or public body and, accordingly, (according to the Draft Decision) *"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."* [28] But, with respect, this simply does not follow and the analysis disregards the fundamental distinction between Article 25 and Article 26. As already explained, Article 26 generally, and the SCC Decisions in particular, are not premised on an effective remedy, whether judicial or otherwise, being available in the third country. Rather, the SCCs themselves provide a remedy (or, more correctly, a series of remedies) in the transferring EU Member State. That inbuilt series of remedies is intended to

[28] At paragraph 61.

ensure that the SCCs accord fully with the requirements of the Charter, including the specific provisions of Article 47.

ARTICLE 4 OF THE SCC DECISIONS

26. In addition, the DPC has not taken account of the safeguards in Article 4 of the SCC Decisions and, in particular, Article 4(1)(a). Mr Schrems' Submissions recognise the relevance, and indeed the importance, of Article 4(1)(a).[29] However, BSA disagrees with Mr Schrems' conclusion that the Commissioner "*has in fact determined the applicability of the conditions for which Article 4(1)(a) provides*". [30]

27. Article 4(1)(a) provides that DPAs are empowered to:

> *"prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:*
>
> > *(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society … where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses.*" (Emphasis added)

28. In parallel, the clauses contained in that SCC Decisions provide that national security disclosures are permitted *only* if required by "*mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society . . . that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the*

[29] At paragraph 51-57 of his Submissions

[30] At paragraph 553 of his Submissions.

State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses."[31]

29. Thus, where "*it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society … where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses"* national DPAs – here the DPC – are empowered to intervene.

30. Here, it appears, the DPC has not given any consideration to her powers under Article 4(1)(a). This is a significant omission for a number of related reasons:

- First, and fundamentally, the mechanism in Article 4(1)(a) is an essential element of the SCC regime, which provides a critical safeguard for EU data subjects whose data are transferred pursuant to the SCCs.

- Second, the availability of this remedy suggests that, even if it were the case that Mr Schrems' *Reformulated Complaint* is factually and/or legally well-founded – and BSA does not accept that it is – the complaint would not go to the validity of the SCC Decisions but, rather, would fall to be addressed though the mechanism of Article 4(1)(a). The SCC Decisions provide an express mechanism for addressing a situation where the transferee of data transferred to a third country via SCCs is subject to "*requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society"* and "*are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses"*. On which basis, therefore, could it be said that the existence of such a situation calls the validity of the SCC Decisions into question?

[31] Clause 5, footnote 1.

- Third, and significantly, Article 4(1)(a) highlights in very stark terms that any analysis of the "*mandatory requirements*" imposed by a third country cannot be done in a vacuum. Instead, these must be assessed in relation to the "*restrictions necessary in a democratic society*". That assessment, in turn, must balance privacy interests in relation to other interests (in this case, national security interests). The Draft Decision does not undertake this assessment. It does not identify as an issue, much less address, whether the requirements of US law in relation to the disclosure of personal data and/or the limitations of available remedies in relation to such disclosure, in the context of the protection of national security and/or the prevention or investigation of serious crime, "*derogate from the applicable data protection law [in a manner] which [goes] beyond the restrictions necessary in a democratic society"* and/or is "*likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses"*.

THE DRAFT DECISION

31. The bulk of the Draft Decision addresses an issue which, as already explained, is not one which actually arises in these proceedings, namely whether the United States ensures "*adequate protection for the data protection rights of EU citizens*".[32]

32. Furthermore, as already indicated, the analysis in the Draft Decision addresses, to the exclusion of all other considerations, what ought, on any view, to be only one aspect of any assessment of the adequacy of protection in any third country – the availability of remedies/redress, especially judicial remedies/redress.

33. In focusing on adequacy, BSA respectfully suggests that the Draft Decision does not address a number of crucial matters (in addition to the failure to address Article 4(1)(a) of the SCC Decision, as just discussed) :

- It fails to address, or even to identify, the context in which the concerns regarding government access to data transferred to any third country, including the United States, must be assessed, namely, that of national security/law enforcement.

- It does not consider EU and Member States' law and practice in this area, which is, on any view, highly relevant to any assessment of the position in the United States. It does not apply the correct analytic framework as specifically set out in the SCC Decisions. The Draft Decision, it is respectfully submitted, addresses the unduly narrow issue of whether the nature and scope of the judicial remedies available in the United States satisfied Article 47 of the Charter. However, the appropriate analysis that should have been undertaken, requires a much broader assessment of whether any limitations on the protection of personal data transferred from the EU to a third country, in this case the United States, (including, <u>but not limited to</u>, any limitations on recourse to a judicial remedy in that third country) go beyond what may be necessary and proportionate to meet objectives of general interest recognised by the EU (to

[32] The issue is formulated in these terms at para 37 of the Draft Decision and is then addressed over the following 12 pages of text (paragraphs 39-60).

use the language of Article 52 of the Charter) or (to use the language of Article 4(1)(a) of the SCC Decisions) "*go beyond the restrictions necessary in a democratic society*" and if they do, whether those limitations "*are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses.*"

34. As regards the first of these points, the Draft Decision does not identify or address the fact that complaints made by Mr Schrems clearly relate to issues of access/disclosure in the context of national security/law enforcement and any issue of the availability of adequate remedies obviously arises in the same context.

35. The test set out in the SCC Decision mirrors that in the Directive itself. The Directive expressly provides for specific limitations and clear deference in its requirements in the areas of national security and law enforcement. Thus, Article 13 of the Directive states that

> "*(1) Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences….*". (Emphasis added)

36. These restrictions in matters of national security were acknowledged by the European Court of Human Rights ("*ECtHR*") in *Leander v. Sweden* – "*…an effective remedy under Article 13 must mean a remedy that is as effective as it can be, having regard to the restricted scope for recourse inherent in any system of secret surveillance for the protection of national security*."[33]

37. This is underscored by the terms of recitals (13), (16) and (43) and Article 3(2), first indent of the Directive, and is reflected in expansive provisions in the Data

[33] 23 (1987) 9 EHRR 433, Paragraph 84.

Protection Acts 1988 and 2003: see, *inter alia*, section 1(4) and section 8(a) and (b) of that legislation.

38. Similar provisions are now found in Article 23 of the GDPR.[34]

39. In BSA's respectful submission, no reasonable assessment of whether the United States, or any third country, ensures "adequate protection for the data protection rights of EU citizens" – if that were the issue here, which it is not – is possible without having regard to these significant limitations and exclusions in EU data protection law.

40. As already explained, these proceedings are not here concerned with Article 25 and the issue of an adequate level of protection does not arise, or certainly does not arise in the same way or to the same extent, in the context of Article 26. Article 26 does not require that there be an adequate level of protection in the third country to which data are transferred; on the contrary, Article 26 is premised on the absence of such protection. If, in the context of the SCC Decisions, the issue of an adequate level of protection arises at all, it is as one – and only one - potentially relevant factor in an Article 4(1)(a) assessment in terms of adducing appropriate safeguards. As already observed, no such assessment has been undertaken by the DPC but, if it had, then equally no reasonable assessment of the adequacy issue in this (Article 26) context could disregard the significant limitations and exclusions in EU data protection law.

41. It is clear from the Draft Decision that the DPC has not, in fact, considered these issues at all.

42. Equally, the Draft Decision does not address the laws and practice of EU Member States regarding the accessing of data in the national security and law enforcement context, and the availability – or not – in the EU, of judicial or other remedies for data subjects in this context. Indeed, there is no assessment by the DPC of the Irish

[34] Article 23(1) provides "*Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security…..*"

position and, in particular, the availability, or otherwise, of remedies. For example, as noted by Facebook in its Submissions,[35] unless the collected personal data are being used as evidence against an individual, in a criminal prosecution, it is likely that the targeted individual will never find out about the relevant surveillance. Further, there is a limited complaints mechanism available whereby complaints are made to a complaints referee, being a designated Circuit Court Judge.[36] Even if a data subject becomes aware of a contravention, the decision of the complaints referee is final, as there is no provision for an appeal of the decision. Indeed, in the event that a data subject became aware of a contravention, it may only be open to bring a constitutional claim or a tort claim against the State, albeit with significant hurdles.

43. If the appropriate framework of reference were, as the DPC suggests it is, the adequacy of protection in the United States, then the DPC is obliged to consider whether that protection is "*essentially equivalent*" to the level of protection available in the EU.[37] That necessarily involves a consideration of the position in the EU which the Draft Decision does not contain.

44. It is indeed a striking feature of the Draft Decision that it concludes, even if only provisionally, that there is no adequate protection for personal data transferred to the United States, without considering whether it is "*essentially equivalent*" to protection in the EU.

45. In that regard, BSA invites the Court to consider the *FRA Report: Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU ('FRA Report')*[38]**.** That document notes that "*the different remedial avenues are often fragmented and compartmentalised, and the powers of remedial bodies curtailed when national security is involved*".[39] Indeed, the FRA Report notes that there are few European cases which challenge surveillance practices and the reasons

[35] Paragraph 223-231

[36] Section 9 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and Section 10 of the Communications (Retention of Data) Act 2011

[37] *Schrems*, paragraph 73

[38] This is appended to Mr Robertson QC's expert report, filed on behalf of Facebook.

[39] As described at pages 59-76 of the FRA Report

for same include strict procedural rules and evidence and legal standing but also the fact that targets of such national security surveillance are not notified of the fact that their communications have been intercepted. Indeed, the FRA Reports make clear that eight member states do not have any right to information or access.

46. The report of Geoffrey Robertson QC is also highly relevant in this context.

47. In this jurisdiction, very limited rights are given to data subjects in relation to surveillance and/or interception undertaken by military intelligence or the Gardaí: see the provisions of the Postal and Telecommunications Services Act 1983, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and the Communications (Retention of Data) Act 2011.

48. EU law cannot, BSA submits, be construed as requiring third countries to which personal data are transferred pursuant to Article 26 SCCs, to apply standards of protection higher than the standards applicable within the EU or to disregard the interests of national security and/or law enforcement when they are central and legitimate concerns of every Member State in the EU.

49. This point is reinforced by the fact that, within the EU and the broader Council of Europe membership, it has long been accepted that rights of privacy, important as they are, cannot to be regarded as absolute and must, in appropriate circumstances, defer to the State's interest in national and public security and law enforcement. Again, consideration of these issues is markedly absent from the Draft Decision.

50. For example in *Klass v Federal Republic of Germany*[40] the ECtHR had to consider legislation in Germany which permitted State authorities to open and inspect mail and listen to telephone conversations to protect against "*imminent dangers*" threatening the "*free democratic constitutional order*" and "*the existence or the security*" of the State. The Court recognised that any of the permitted surveillance measures, once applied to a given individual would result in interference with an individual's Article 8 rights. However, the Court went on to consider whether the

[40] (1979 – 80) 2 EHRR 214

interference was justified in order to safeguard national security and to protect democratic society as a whole. Indeed, further case law on Article 7 and 8, including *Volker and Markus Schecke*[41] and *Schwarz*[42] are set out in Facebook's Submissions[43] together with the European Court of Human Rights decision in *Kennedy v UK*[44].

51. More recently in *Tele 2,* [45] Advocate General Saugmandsgaard considered whether certain national laws in Sweden and the UK were consistent with the right to privacy and other fundamental rights set out in the Charter. Advocate General Saugmandsgaard considered, in some detail, the judgment in *Digital Rights Ireland* and concluded that bulk metadata retention obligations can be permissible so long as certain requirements are met.

52. Mr Robertson QC in his expert report[46] helpfully summarises the Advocate General's reasoning in relation to the relevant requirements as follows:

a) Legal basis – the legal basis must be "*adequately accessible and foreseeable*".

b) The necessity to observe the essence of the rights enshrined in Articles 7 and 8. It was considered that the retention of bulk metadata would not violate the essence of Articles 7 and 8 of the Charter where, *inter alia*, it was subject to appropriate safeguards to protect the data against the risk of abuse or unlawful access and use.

c) An objective of general interest to the EU is "*the fight against serious crime"*. The Advocate General noted that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest to the Union. The same may be said of the fight against serious crime in order to ensure public safety. However, the Advocate General

[41] Joined cases C-92/09

[42] C-291/12

[43] Paragraph 127-139

[44] [2010] ECHR 682

[45] Joined Cases C-203/15 and C-698/15.

[46] Exhibited to his Affidavit sworn on 7 November 2016, at page 20

was of the opinion that combatting ordinary offences and the smooth conduct of proceedings other than criminal proceedings are not objectives in the general interest that are capable of justifying a general data retention obligation.

d) Appropriateness of the measure with regard to the objective in question was also a consideration. For example, data retention is liable to contribute to the fight against serious crime.

e) A measure would only be considered necessary if no other measures exist which would be equally appropriate and less restrictive.

f) The requirement of proportionality within a democratic society flows from, *inter alia*, Article 52(1) of the Charter. In that regard, it has been consistently held that a measure which interferes with fundamental rights may be regarded as proportionate only if the disadvantages caused are not disproportionate to the aims pursued. Advocate General Saugmandsgaard was of the view that it was important to clarify the nature of the disadvantages which people might suffer.

53. In *Opinion 1/15* Advocate General Mengozzi adopted a similar approach to Advocate General Saugmandsgaard in his consideration of the proposed passenger name record data transfer treaty with Canada. There, the Advocate General noted that transfer of such data could result in an interference with Articles 7 and 8 of the Charter but considered the justification for such interference. Again, he considered it clear that combatting terrorism and serious international crime to ensure public safety constituted an objective of general interest within the meaning of Article 52(1) of the Charter. The Advocate General also considered whether the proposed treaty was proportionate and struck a fair balance between protecting personal data and combatting terrorism and/or serious crime.

54. The CJEU gave its judgment in *Tele2* on 21 December 2016. The Court held (*inter alia*) that Article 15 of the ePrivacy Directive,[47] read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, precluded national legislation which provided for the "*general and indiscriminate*" retention of traffic and location data of subscribers. The Court's analysis and conclusions are consistent with the views expressed by the Advocate General in his Opinion and the views of Mr Robertson. In particular:

a) The Court makes it clear that the fight against serious crime, in particular organised crime and terrorism, is an objective of general interest, one characterised by the Court as "*fundamental*" : § 103

b) Article 15 of the ePrivacy Directive, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does <u>not</u> prevent a Member State from adopting legislation permitting, as a preventative measure, the targeted retention of traffic and location data for the purpose of fighting serious crime, provided that such retention is limited to what is strictly necessary: § 108 & the further discussion at §109 -111.

c) The measures at issue in Case 203/15 exceed what are strictly necessary and cannot be considered to be justified within a democratic society: §104-107

d) Targeted access to retained data was, in principle, permissible in relation to the objective of fighting serious crime. Additionally, broader access was permissible: "*where for example vital national security, defence or public security interests are threatened by terrorist activities"* and *"where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combatting such activities"*: §119, as well as the discussion in the following paragraphs.

[47] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (referred to as " the ePrivacy Directive").

e) Competent national authorities were not obliged to notify persons affected if and for as long as such a notification was liable to jeopardise the investigations being undertaken by them: §121

55. The analysis adopted in these cases (and there are many more where such issues have been considered)[48] is reflected in the provisions of Article 52 of the Charter and also echoes the language of Article 4(1)(a) of the SCC Decisions.

56. As the Commission explains in the "*frequently asked questions relating to transfers of personal data from the EU/EEA to third countries"* (the "*European Commission SCC FAQ*"), "*the condition 'necessary in a democratic society' derives from Articles 8 to 11 of the European Convention on Human Rights and extensive case law [that] has been developed by the European Court of Human Rights on this issue. The same principle is also included in Council of Europe Convention 108 in respect of restrictions on the data protection principles (Article 9).*"[49]

57. The European Commission SCC FAQ[50] goes on to explain that further precision in the wording of this derogation would be impossible given that SCCs are intended to be used to transfer data to countries across the world: "*A general principle of the EU data protection legal framework is that any restrictions of the basic data protection principles must be limited to those which are necessary for the protection of fundamental values in a democratic society. These criteria cannot be laid down for all countries and all times but should be considered in the light of the given situation in the country in question.*" This analysis is entirely consistent with the CJEU's decision in *Tele2*.

58. Again, this simply serves to highlight the absence of any such analysis in the Draft Decision.

[48] See e.g. *Weber and Saravia v Germany* [2006] ECHR 1173. Indeed, there are other competing rights which need to be considered including Article 2 in relation to the right to life including the right to human dignity, Article 3 which respects the right to physical and mental integrity, Article 11 which protects freedom of expression. The balancing of competing rights was also considered in *Google Spain*.

[49] *See* European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", available at: http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf.

[50] *Ibid.* at page 31.

59. As regards the position in the United States, the evidence of US law available, largely adduced by Facebook, illustrates the narrow focus and conclusions reached by the DPC. First, it is clear from the Draft Decision that the DPC fails to identify the substantive protections/safeguards available in US law and instead focuses almost exclusively on the issue of remedies. It appears from Facebook's evidence that there is no "*general and indiscriminate*" access to data in the United States. Second, BSA is concerned that the DPC's position on the remedies available in US law is based on certain misunderstandings in circumstances where the evidence of US law which is before the Court, in particular that of Facebook, is materially different to that contained in the Draft Decision. In essence, the material before the Court appears to establish that US law provides a substantive level of protection to data subjects.

WHETHER THERE SHOULD BE A REFERENCE

60. In the context of a proposed reference a number of propositions are well settled. First, in the context of an application for a reference to the CJEU under Article 267, the Court has complete discretion (though not in cases where the validity of an EU act is properly at issue).[51] Second, prior to a reference the Court must ensure that the factual and legal context is established. Third, reference must be necessary for the effective resolution of a dispute.[52]

61. In the present circumstances a number of issues arise:

- First, Mr Schrems does not make any claim, whether in the Reformulated Complaint or in his defence that the SCC Decisions are invalid.

- Second, and perhaps more importantly, for the reasons identified above, the DPC has not adequately investigated Mr Schrems' complaint.

- In particular, Article 4(1)(a) of the SCC Decisions appears to provide an effective and appropriate mechanism to address so much of the Reformulated Complaint as goes beyond the factual complaint apparently made by Mr Schrems as to the terms of the contractual provisions actually relied on by Facebook.

- In these circumstances, it appears to BSA that no issue properly arises in these proceedings as to the validity of the SCC Decisions and therefore it would not be either necessary or appropriate to refer any such issue to the CJEU.

- In any event, and without prejudice to the foregoing, any reference now would be wholly premature.

[51] As confirmed by McKechnie J in *Digital Rights Ireland Limited v Minister for Communications* [2010] 3 IR 251

[52] *Goshawk Dedicated Ltd v Life Receivables Ireland [2009] IESC 7*

62. If a reference were to be made, then it is essential that the proper legal and factual context should be identified. In *Digital Rights Ireland v Minister for Communications*[53] McKechnie J quoted from the CJEU judgment in *Irish Creamery Milk Suppliers Association v Ireland* [54] where the Court stated as follows:

> *"The need to provide an interpretation of Community law which will be of use to the national court makes it essential… to define the legal context in which the interpretation requested should be placed. From that aspect it must be convenient, in certain circumstances, for the facts of the case to be established and for questions of purely national law to be settled at the time the reference is made to the Court of Justice so as to enable the latter to take cognisance of all the features of fact and of law which may be relevant to the interpretation of Community law which it is called upon to give".*[55]

63. In *Recommendations to national courts and tribunals in relation to the initiation of preliminary ruling proceedings*[56] the CJEU emphasised the importance of the factual (and legal) context being known to the national court before a reference is made.

> "19. *It is, however, desirable that a decision to make a reference for a preliminary ruling should be taken when the national proceedings have reached a stage at which the referring court or tribunal is able to define the legal and factual context of the case, so that the Court of Justice has available to it all the information necessary to check, where appropriate, that European Union law applies to the main proceedings. In the interests of the proper administration of justice, it may also be desirable for the reference to be made only after both sides have been heard."*

64. Indeed, it is well established that, in the event that the description of the factual and legal context is inadequate, the CJEU may be prevented from applying the desired

[53] [2010] IEHC 221

[54] [1981] ECR 735

[55] Paragraph 6

[56] 2012/C 338/01

precision to certain of the questions raised with the result that, in certain circumstances, the CJEU will have no choice but to hand down a ruling where it leaves open certain aspects of the questions raised.[57]

65. Here, as already explained, the DPC is seeking a reference on the basis of an investigation that is incomplete and a Draft Decision that fails entirely to address a significant number of matters of fundamental importance. It follows that, if there is to be a reference, this Court needs to address those issues and make appropriate findings on them to enable the CJEU to address the referred question(s) appropriately.

66. BSA would obviously wish to assist the Court in relation to the formulation of any Order of Reference, including (but not limited to) the question or questions referred. However, it appears premature and inappropriate to address this issue further at this stage.

[57] As described by Broberg and Fenger in *Preliminary References to the European Court of Justice*, 2nd ed, Oxford University Press 2014, at page 292, when discussing case C-266/96 *Corsica Ferries France* [1988] ECR I-3949, Paras 21-8.

SUMMARY OF CONCLUSIONS

67. In summary it is respectfully submitted that:

1. There is a "*clear distinction*" between mechanisms that permit transfers to third countries that ensure an adequate level of protection under Article 25 of the Directive and transfers to third countries that have not been found to ensure an adequate level of protection under Article 26.

2. The SCCs are intended to facilitate the transfer of personal data from the EU to third countries that *ex hypothesi* do not "*ensure an adequate level of protection*" for the purposes of Article 25.

3. The issue of whether the United States, or any other third country, does or does not "*ensure an adequate level of protection*" is not determinative for an assessment under Article 26, and even less so in respect of the validity of the SCC Decisions.

4. The SCCs impose significant obligations on data controllers and provide significant protections for data subjects.

5. The SCC Decisions give DPAs – including the DPC – very important supervisory, oversight and enforcement powers. In particular, Article 4 of each of the SCC Decisions gives DPAs the power to prohibit or suspend data flows in certain circumstances.

6. The DPC is seeking a reference on the basis of an investigation that is incomplete and a Draft Decision that fails to address a significant number of matters of fundamental importance.

7. Article 4(1)(a) of the SCC Decisions appears to provide an effective and appropriate mechanism to address so much of the Reformulated Complaint as goes beyond the

factual complaint apparently made by Mr Schrems as to the terms of the contractual provisions actually relied on by Facebook.

8. In these circumstances, it appears to BSA that no issue properly arises in these proceedings as to the validity of the SCC Decisions and therefore it would not be either necessary or appropriate to refer any such issue to the CJEU.

9. If the Court is minded to make a reference, it will need to address those issues which the DPC ought to have addressed but did not and make appropriate findings on them to enable the CJEU to address the referred question(s) appropriately.

10. BSA would obviously wish to assist the Court in relation to the formulation of any Order of Reference, including (but not limited to) the question or questions referred. However, it appears premature and inappropriate to address this issue further at this stage.

KELLEY SMITH
MAURICE G COLLINS
23 December 2016

Word count: 9,638 (including footnotes)