THE HIGH COURT

COMMERCIAL

Record No. 2016/4809P

BETWEEN

THE DATA PROTECTION COMMISSIONER

Plaintiff

-and-

FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

Defendants

AFFIDAVIT OF THOMAS BOUÉ

I, **THOMAS BOUÉ** of BSA | The Software Alliance, 44 Avenue des Arts, Belgium 1040, Brussels, aged 18 years and upwards, make oath and say as follows:

1. I am the Director General, Policy-EMEA of BSA Business Software Alliance, Inc., trading as BSA | The Software Alliance ('**BSA**'), and I make this affidavit for and on behalf of BSA, which I am duly authorised to do and from facts within my own knowledge save where otherwise appears and where so otherwise appearing I believe the same to be true.

2. On 19 July 2016 Mr Justice McGovern joined BSA and others, as an *amicus curiae* to the within proceedings in the context of the Data Protection Commissioner's ('**the Commissioner**') request to the Court for a reference to the Court of Justice of the European Union ('**CJEU**') pursuant to Article 267 of the Treaty on the Functioning of the European Union (**'the Proceedings'**).

3. Subsequently on 25 July 2016 the Court also made certain directions: those directions included the exchange of affidavits by any *amicus curiae* (though no determination has been made as to the admissibility of such affidavits in the event of that being disputed). I make this affidavit further to those directions. I note that John O'Dwyer, on behalf of the Commissioner, has sworn an affidavit with Replying Affidavits delivered by the Second Defendant, Mr Schrems and Mr Ashley Gorski, and the Replying Affidavits of Mr Peter Ratzel, Mr John DeLong, Mr Stephen Vladeck, Mr Peter Swire, Mr Joshua P. Meltzler, Ms Andrea Scheley, Mr Chris Bream, Ms Yvonne Cunnane, Mr Geoffrey Robertson and Michael Clarke on behalf of the First Named Defendant, Facebook Ireland Limited ('**Facebook Ireland**').

4. As is clear from the averments set out below, this case raises complex issues at the intersection of privacy, data protection, economic growth, national security and technology. This Court and any judgment of the CJEU has the potential to have enormous adverse consequences for thousands of companies, European and international, offering products and services in the European Economic Area ('**EEA**') and for their employees and customers.

5. Since its joinder as an amicus to the Proceedings, to assist this Honourable Court in understanding the use and importance of Standard Contractual Clauses (the '**SCCs**'), BSA conducted a wide-ranging survey of corporate data transfer practices.

6. I beg to refer to a folder of documents upon which marked with the letters and number '**TB1**' I have signed my name prior to the swearing hereof (the '**Folder**'). Throughout this affidavit, I refer to documents at various tab divisions of the Folder.

7. For ease of reference, this affidavit is structured using the following headings:

A. BSA

8. Details about BSA, its membership and activities (including in the context of *amicus* briefs) were set out in my earlier affidavit sworn in the context of the *amicus* application and so are not repeated here. Instead, I set out a brief summary about BSA and the services provided by its members which rely upon SCCs.

9. BSA is a not-for-profit international trade association whose members include international technology providers such as Apple, IBM, Microsoft, Intel, Siemens PLM, SAS, and Oracle and many other large and smaller innovators. A full list of BSA's membership is located at tab 1 of the Folder. A copy of BSA's Articles of Incorporation, which sets out BSA's functions is at tab 2.

10. BSA members' revenue in 2015, based on their most recent filings with the U.S. Securities and Exchange Commission, was nearly USD559 billion, of which an estimated USD130 billion can be attributed to business conducted in the EU. The most rapidly increasing portion of those revenues is attributable to services and technologies that European businesses and public sector organisations rely on to store, secure, analyse and manage data.

11. BSA has had an active presence and extensive operations in Europe for nearly 30 years. BSA's member companies each also have a strong European presence, with several having their European headquarters or substantial operations in Ireland. BSA member companies employ over 15,000 people in Ireland and partner with many Irish firms and with the Irish public sector.

12. BSA members provide critical technology infrastructure and services to businesses. In that regard, BSA members provide data analytics, data storage, and other technology services that are increasingly indispensable to both Irish and European businesses and public sector organisations in the modern economy. As is clear from the survey results discussed below, provision of these services depend upon the ability of BSA members to transfer personal data internationally at the request and direction of their customers and individuals, including from data centres and other substantial operations in Ireland.

13. The services provided by BSA members include, for example, the storage, management and securing of data and the analysis of that data to unlock insights. These businesses,

in turn, serve millions of customers in the EU and globally and are responsible for millions of EU jobs. Again, as is clear from the survey results described below, the SCCs play an indispensable role in the operation of these businesses, because they provide the legal basis necessary to permit any cross-border data transfers that are required for these transactions.

14. The movement of data by BSA members across national borders assists in driving the global economy. By way of example the services provided by BSA members are driving advances in medicines, healthcare for patients, food safety and security, sustainable consumption and urban planning, to name but a few. In my view the inability to make such advancements and achieve the societal benefits that accrue from these advancements could disadvantage the EU. Their net effect would be to lower the competitive potential of EU industries and ultimately deny or delay its citizens' access to beneficial products and services.

15. BSA and its member companies have a deep commitment to privacy and fundamental rights and a history of engaging in defence of those rights. There are many examples of this commitment – among them the 'Transparency Reports' published by BSA member companies, which indicate the extent of government requests for data they hold. These are publicly available and therefore I have not included them as exhibits to this affidavit. More generally, it is the practice of BSA member companies when they receive lawful information requests, to carefully review those requests, and to require that those requests be accompanied by the appropriate legal documents such as a subpoena or search warrant depending on the type of information requested.

BACKGROUND -SCCs & THE LEGAL ISSUE TO BE ADDRESSED

Legal issue to be addressed

16. EU data protection law restricts transfers of personal data to any country outside of the EEA. This restriction is set out in Article 25 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('**the Directive**') which has been implemented into Irish law by means of the Data Protection Acts 1988 and 2003.

17. It is important to note that the European Union – recognising the importance of data flows even in the mid-1990s – created two distinct mechanisms to enable routine transfers of personal data to countries outside of the EEA in a way that would ensure appropriate protection:

    (a) *First,* under Article 25(1) and Article 25(6) of the Directive, an entity can transfer personal data to a non-EEA country if that country is deemed by the European Commission to ensure "an adequate level of protection." Only eight countries (Andorra, Argentina, Canada, Faroe Islands, Israel, New Zealand, Switzerland and Uruguay) and three regions (Guernsey, Isle of Man, and Jersey) in the world have been deemed to provide such protection. This list does not include the United States. As an alternative, the EU and the United States reached an agreement in relation to the transfer of data between the EU and the United States utilising what is commonly known as the 'Safe Harbour' programme. The European Commission made a decision that conferred adequacy on data transfers to the United States made by companies pursuant to the Safe Harbour programme. As a result of the CJEU's decision issued on 6 October 2015 the Safe Harbour programme is no longer a legal basis for complying with the Directive with regard to the transfer of data between the EU and the US.

    (b) *Secondly,* to ensure that data could continue to flow to countries *not* deemed to provide an adequate level of protection, the legislation provided a derogation to ensure that transfers could take place to such third countries so long as the party transferring the data (the '**Data Controller**') "adduces adequate safeguards." Under Article 26(2) of the Directive, these safeguards can be set out in contractual clauses – e.g., SCCs. In practice, most enterprises operating in the EEA today rely on SCCs to transfer personal data to *any* country outside of the EEA that is not deemed to provide an adequate level of protection.

SCCs

18. The European Commission, pursuant to the Directive, established the SCCs in the form of template contracts that enterprises can use. The European Commission has issued two types of SCCs: '*controller to controller*', which enterprises commonly use to transfer data from one corporate affiliate to another, and 'controller to processor' which enterprises use to transfer data to entities that will process data on their behalf.

19. The safeguards in the SCCs are binding contractual commitments, including to secure personal data, restrict access to that data, and control any further transfers of that data. 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 State data protection authorities to conduct audits.

20. As referred to above, following its joinder as an amicus in the Proceedings, BSA conducted a wide-ranging survey of corporate data transfer practices. The survey was designed to assist this Honourable Court in understanding the use by BSA members and importance of SCCs to commerce and citizens. At paragraphs 28 - 49, I set out the results of this Survey, which inter alia, demonstrates the industry reliance on SCCs, the methods used by respondents to the survey to ensure SCCs are observed and the impact of the loss of SCC's. I also exhibit the results of a similar survey conducted by the International Association of Privacy Professionals ('**IAPP**') which was contained in its Annual Governance Report.

How SCCs are used in practice

21. By way of representative example of how the SCCs typically are used in practice: A bank wants to use special analytic software provided by a BSA member company to detect and reduce fraud. Assume that, in this example, servers and/or personnel who perform the necessary services are located outside of the EEA. Accordingly, to use the software, the bank must transfer data, including personal data such as payment transaction details, outside of the EEA. To help the bank ensure that these personal data transfers can be undertaken in compliance with European data protection law, the BSA member company may add the SCCs to the commercial terms for the service. Because the European Commission has approved the SCCs (as described in paragraphs 17 and 18 above), the substantive provisions in the SCCs are fixed and do not need to be negotiated; instead, the parties complete appendices to the SCCs in order to describe the data being transferred, the categories of individuals whose data are being transferred, and other details relating to the specific transfers. Details regarding the use of SCCs by the respondents to the BSA and IAPP surveys are set out at paragraphs 37-43.

22. The SCCs provide the legal foundation for millions of daily data transfers to countries outside the EEA. This practice, which for years has enabled international transfers to any country outside of the EEA, has become increasingly common in order to facilitate transfers to the United States, following the invalidation of the Safe Harbour.

23. The SCCs are also commonly used to transfer employee data. Employee data of international companies is often accessible from and/or stored in more than one country, particularly as many companies establish and apply certain employment conditions, such as benefits, at a global level. In such cases, access to relevant employee data must be available in multiple jurisdictions. The international nature of 21st century business means that an employee located in Dublin could be reporting to a manager in the United States or in any of the several other countries that are not deemed to provide adequate protection

The Proceedings

24. The SCCs are central to these Proceedings. The detailed factual background relating to the complaint of the Second Defendant, Mr Schrems, against Facebook Ireland, and the subsequent Irish judicial review proceedings and CJEU ruling delivered on 6 October 2015 in relation to Safe Harbour are set out in the Statement of Claim and so are not repeated here. In brief, however, as a result of the CJEU's decision issued on 6 October 2015 the Safe Harbour programme is no longer a legal basis for the transfer of data between the EU and the US. Subsequent to this ruling, at the invitation of the Commissioner, Mr Schrems reformulated his complaint against Facebook Ireland (the '**Reformulated Complaint**').

25. The Reformulated Complaint calls into question Facebook Ireland's usage of SCCs to transfer data to the United States. In response, the Commissioner has prepared a draft decision (the '**Draft Decision**') which concludes that there are well-founded objections in respect of the transfer of data to the United States pursuant to the SCCs. However, the Commissioner has determined that she could not conclude her investigation without obtaining a ruling from the CJEU on the validity of the European Commission's SCC Decisions (as defined in the Plenary Summons).

26. In his Defence, delivered on 9 September 2016, Mr Schrems denies that he made any claim that the SCCs are invalid. Instead, Mr Schrems pleads that in the Reformulated Complaint he complained that Facebook Ireland's Data Transfer and Processing Agreement, pursuant to which Facebook Ireland effects data transfers from Ireland to the US, did not comply with the SCCs.

27. Facebook Ireland has delivered a detailed defence in which it asserts, *inter alia*, that the Draft Decision lacks a proper factual basis and was issued without full consideration of relevant evidence. In addition, Facebook Ireland pleads that the invalidation of the

SCCs has the potential to significantly adversely affect international trade and commerce which would be inconsistent with other freedoms contained in the Charter and the Treaty on the European Union.

B. SURVEY RESULTS

28. As referred to above, two recent surveys were carried out in respect of the software industry's use of SCCs.

29. First, since its joinder as an amicus in the Proceedings BSA conducted a wide-ranging survey of corporate data transfer practices. The survey was designed to assist this Honourable Court in understanding the use of SCCs and their importance of SCCs to commerce and citizens. A copy of the BSA survey appear at tab 3 of the Folder and the BSA survey results appear at tab 4 of the Folder.

30. The BSA survey was conducted by way of an online poll open from mid-September 2016 to mid-October 2016. In addition to BSA's software companies participating in the survey, other U.S. and international industry organisations shared the survey with their member companies and urged them to participate. These industry associations represent companies with operations in the United States, the EEA, Asia and Latin America and includes companies active in banking, insurance, manufacturing, life sciences, and petrochemicals.

31. Secondly, the IAPP-EY Annual Privacy Governance Report 2016, was released in September 2016. It includes as part of its second annual study of data governance in organisations, the results of a survey which dealt with cross border data transfers. A copy of the IAAP Cross Border Data Transfer survey results appear at tab 5 of the Folder.

32. Both surveys reached broad and varied corporate audiences. 63 representatives from companies contributed to the BSA survey. More than three-quarters of respondents (78%) are in the technology sector. Some of the respondents are BSA members that provide software and data services and technologies to enterprises and public sector organisations. Their services and technologies enable customers to conduct their day-to-day operations, including storing and processing business, customer and citizen data; running business platforms; developing and hosting key business applications;

managing customer accounts and sales; conducting human resources management; and creating and distributing content.

33. The IAPP annually surveys its members, who are individuals holding privacy-related positions in commercial organisations and other settings. The IAAP reports that more than 600 of its members responded this year to a wide-ranging set of questions addressing data governance in their organisations, including cross-border data transfer practices.

34. To assist in understanding and analysing the results of the surveys I have broken them down into the following headings:

- Central Importance of SCCs;
- Use of SCCs;
- Additional Safeguards engaged to ensure SCCs are observed; and
- Other mechanisms for transferring data.

Central Importance of SCCs

35. The results of both surveys confirm the central importance of SCCs for European based enterprises doing business in the modern global economy. The surveys found that:

- Nearly all respondents rely on SCCs for transferring data from the EEA to the United States;
- European based companies are even more dependent than American companies on SCCs for data transfers from the EEA to the United States;
- A large majority of companies also use SCCs for transfers to Asia, the Americas and other regions; and
- A large majority of companies utilise SCCs not just to move data within their corporate group, but also to send or receive data from customers, and for other types of routine transfers including with third parties.

36. The BSA and IAPP surveys clearly demonstrate that SCCs are indispensable in the conduct of global data flows, including transatlantic movement of data, and so are the lifeblood of economic activity between the EEA and the rest of the world. If SCCs were to be judicially invalidated, the interests of European based companies would be damaged to an even greater extent than those of American companies. Further, since

SCCs are used by companies on a world-wide basis, the economic impact would extend beyond the transatlantic context. In short, the fundamentals of global commerce would be harmed. Europeans' privacy interests are also likely to suffer. SCC's require transparency and accountability of entities engaged in data transfers which act to further Europeans' privacy interests.

Use of SCCs

37. Today, thousands of European and non-European companies routinely rely on the SCCs to transfer customer data to locations outside the EEA – including, but not limited to, the United States. A typical example would involve a centralised system for all customer leads, contacts and accounts that enables a mobile sales team to access relevant customer records and coordinate. Many of these same customers also rely on products and services supplied by BSA member companies to undertake these data transfers, and therefore rely on the SCCs that BSA members provide. This enables enterprises to use the services of BSA members on a 24/7 basis to store, process, and transfer personal data no matter where in the world they are located.

38. As is clear from the BSA survey results, nearly all (89.5%) respondents told BSA that they rely on SCCs for transferring data from the EEA to the United States, irrespective of whether they are established within the EEA. Close to two-thirds (63.9%) of respondents have establishments in the EEA.

39. The IAPP documented a similarly great reliance on SCCs for transatlantic data flows. More than half (54%) of the wider variety of organisations represented in the survey transfer data between the EEA and the US. Virtually all businesses participating in the IAPP survey, not just software and technology companies, rely on data flows. More specifically, 96% of respondents from manufacturing companies indicated that their employers engage in transatlantic data flows. Nearly three-quarters (74%) of technology and telecommunications companies do likewise. Three-quarters (71%) of enterprises with between 25,000 and 74,000 employees confirmed to IAPP that they rely on transatlantic data flows, as do 79% of the largest companies (more than 75,000 employees).

40. Strikingly, IAPP found that it is European companies that rely most heavily on data flows from the EEA to the United States – 79% of the European respondents, compared to 62% of surveyed US firms. The vast majority (89%) of these European companies employ SCCs as the legal basis for accomplishing transfers to the United States. A very

large percentage of respondents from U.S. companies (79%) told IAPP that they too rely on SCCs to move personal data from the EEA to the United States.

41. The results of the BSA survey, which was conducted in September/October 2016 after the IAPP survey, confirm these findings. A large majority of companies (82.5%) reported to BSA that they use SCCs for transfers to other destinations besides the United States. Indeed, they rely on SCCs globally – for example, when data is sent to the Asia-Pacific region, Latin America, and Africa, as well as to parts of Europe outside of the EEA.

42. BSA's survey further revealed how extensively companies depend on SCCs. A large majority of companies use them for data transfers within their corporate group (88.6%), for transferring data to or receiving it from customers (68.6%), and for transfers beyond the intra-corporate and customer contexts (71.4%). International data transfers, in other words, are essential to all aspects of their activity, and not just limited to technical activities.

43. Again it is clear from the survey results that using SCCs for multiple purposes requires companies to resort to more than one type of clause. An overwhelming percentage (92.3%) employ controller-to-processor clauses, which is the variant relied upon by Facebook in this case. A large percentage (84.6%) also use controller-to-controller clauses in their business activities.

Additional Safeguards engaged to ensure SCCs are observed

44. As mentioned above BSA and its member companies have a deep commitment to privacy and fundamental rights and a history of engaging in defence of those rights. As is demonstrated by BSA's survey results, respondent companies to the BSA survey do not simply insert standard clauses into their third-party contracts as a mechanical matter. Rather, they described to BSA an impressively wide array of additional and voluntary measures they have developed to guarantee that the protections built into standard clauses actually work in practice. For example, companies undertake due diligence examinations to assess third parties' privacy practices before contracting with them. They have established codes of conduct or guidelines for third parties. Respondent companies also reported that they use internal committees to decide whether to approve contracts with third parties that incorporate SCCs.

45. Data transferors' vigilance does not cease with the signing of a contract. During the term of a contract, some respondents noted that they take additional safeguards to ensure SCCs are observed. They conduct regular audits of the third party's performance

in protecting personal data. Companies may perform audits themselves, or instead rely on external auditors, to examine the contractor's technical and organisational protection measures. Companies also regularly review the sufficiency of their internal controls. They also scrutinise their own compliance with any relevant privacy certifications administered by outside organisations.

46. These measures evince a commitment to rigour on companies' part in ensuring that SCCs operate effectively to protect personal information leaving the EEA. The measures employed go far beyond establishing a mere 'right in contract in favour of data subjects', as the Commissioner referred to in the Draft Decision. On the contrary, companies have elaborated a thorough and complex series of procedures built upon – and buttressing – contractual protections. SCCs are the base upon which this extended compliance architecture rests. The removal of SCCs as a compliance vehicle would undermine the additional protections that protect European data. I say and believe that without SCCs, this network of protections for personal data would disappear.

Other mechanisms for transferring data

47. SCCs, moreover, are not simply one among many mechanisms for data transfer. For more than a third (35%) of the companies BSA surveyed, they are the exclusive means relied upon for data flows from the EEA to the United States and elsewhere. Additionally, over half (51%) of the respondents use standard clauses as their principal method for data transfer.

48. Companies that do not depend exclusively on SCCs for international transfers may invoke several other bases under EU data protection law. The principal bases noted to BSA are the consent of the data subject, relied upon to some extent by 47% of responding companies, binding corporate rules (BCRs) (33%), and the E.U.-U.S. Privacy Shield, which attracted at the time of conducting the survey a relatively small (13%) number of companies.

49. These other bases for international transfers of data are not interchangeable. BCRs apply only to intra-corporate transfers of data, for example. Moreover, only 88 companies across the globe have had their BCRs approved by European data protection authorities and can therefore rely on them. Also, individual consent is not always feasible to obtain, and European data protection authorities do not favour reliance on consent for large-volume or periodic and recurring data transfers. In addition, a majority of

respondents (51%) indicated that they do not regard the Privacy Shield as a complete alternative to SCCs for data transfers from the EEA to the United States.

C. SUBSTANTIAL ECONOMIC AND SOCIETAL IMPLICATIONS OF THE PROCEEDINGS

50. As set out in the following paragraphs, the Proceedings have the potential to affect adversely not only BSA members but also a substantial number of other entities and individuals throughout the EEA.

51. Nearly two-thirds (65%) of the companies surveyed told BSA that an inability to rely on SCCs for transfers from the EEA to the United States would pose a *"very significant"* impediment to their operations in the US market. 24% indicated that the potential absence of SCCs would be significant for their US business activities. Similarly, close to three-quarters of survey respondents (73%) advised that without SCCs their operations in markets other than the United States would be very significantly impeded.

52. In the context of the economic impact of software, BSA has commissioned the Economist Intelligence Unit ('**EIU**') to consider the economic contributions of the software industry to the European Union and in particular in its five largest Member States. In this regard, the preliminary findings of the EIU are set out at tab 6 of the Folder. The significant contribution of the software industry to the Europe Union is clear from the preliminary results including direct value added gross domestic product contribution of €249 billion and the 3.1 million direct jobs.

53. On 15 November 2016 leading members of Europe's digital community delivered a letter to the Vice President of the Digital Single Market and the European Commissioner for Digital Economy and Society calling for the enactment of a regulation to provide for the free flow of data and to remove the unjustified data location rules/barriers across the EU. This letter confirms the extraordinarily high value of data-related activities in the EU. It also shows, in an intra-EU context, the importance of data flows, which would provide an estimated €415 billion to the EU's GDP (as published in *Mapping the Cost of Non-Europe 2014-2019 - European Parliamentary Research Service (April 2015)).* A copy of this letter appears at tab 7 of the Folder.

54. The societal impact of data flows between countries and continents and any interruption in data flows is also striking. Unlike ten or even five years ago, today, an estimated 2.5 quintillion bytes of data are generated across millions of devices and machines every

day. To put this into perspective, this is equivalent to nearly 60 billion 32Gb iPads - and growing rapidly. By 2020, the digital universe will have grown to reach 44 trillion gigabytes, more than doubling every two years. This means that if the digital universe were represented by the memory in a stack of tablets, that stack would have stretched 66 percent of the way to the Moon in 2013. By 2020, that stack would equal 6.6 times the distance between the Earth and the Moon. A copy of the study from 2014 entitled *'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things'* , which published these statistics, appears at tab 8 of the Folder.

55. In today's world of online services, it is overly simplistic to envisage this data sitting in a single specific place, in a specific country, on a specific server in a dark cool room with blinking lights. The engineering objective of data management design is efficiency: to be able to access information when needed, accurately, securely and quickly. Consequently, data is assigned for storage, retrieval and analysis based on where the computing capacity is best available. Physical location is certainly a consideration, to place the information where the user can best access it, but it is not the only consideration. In fact, from an engineering and efficiency perspective, requiring specific physical location may well degrade performance, access and security.

56. Just as important, very many interactions today involve international data transfers, such as using a smartphone app, a credit card, or a check-in kiosk at an airport, or confirming travel insurance coverage. Imposing geographical limitations on such transfers would deprive both enterprises and individuals of the value and convenience they seek. Taken to an extreme, if the SCCs were unavailable with respect to the United States and other countries, using a smartphone to send an email, withdrawing cash from an ATM, or confirming travel insurance would become nearly impossible.

57. The same would be true for European and American enterprises. If banks could not settle payments, or car makers transmit safety testing data, or cancer researchers work collaboratively, we would all be much worse off. If mechanisms such as SCCs are unavailable, all of these activities will become far more difficult and expensive, and might be entirely barred. If that happens, more cumbersome and less efficient ways to share data and collaborate will have to be found.

58. The impact of disrupting these flows is not merely theoretical. I refer to the report by the Information Technology Industry Council ('**ITIC**') which analyses the consequences to trade if international data flows were seriously disrupted or stopped, including:

- The negative impact on EU GDP could reach -0.8% to -1.3%. This is roughly equivalent to three to four times the economic decline that Europe experienced during the 2012 economic downturn;

- EU services exports to the United States would be expected to drop by 6.7%, and EU manufacturing exports could decrease by up to 11%; and

- The direct welfare effects for consumers would be equivalent to a loss of USD 102 billion to USD 170 billion, i.e., up to USD 338 per EU citizen.

A copy of the ITIC report entitled *'The EU-U.S. Privacy Shield: What's at Stake'*, from 16 February 2016, appears at tab 9 of the Folder.

59. In conclusion, I say that it is clear from the averments set out above, in particular the results of the survey conducted by BSA to assist the Court in understanding the role of and reliance on SCCs by industry and private citizens and the IAPP survey, that the outcome of these Proceedings has the potential to have significant economic and commercial consequences for thousands of companies, European and international, offering products and services in the EEA, and for their employees and customers.

SWORN by the said Thomas Boué

This 17 day of November 2016
at

before me a Notary Public and the said Thomas Boué has confirmed his identity to me by the provision of photographic identification being a drivers licence/passport issued by the relevant authority.

THOMAS BOUÉ

Vu pour la légalisation des signatures
de Thomas BOUE
apposées ci-dessus.

Pablo DE DONCKER
Notaire
Rue du Vieux Marché aux Grains, 51
1000 Bruxelles

NOTARY PUBLIC

This Affidavit is filed on behalf of by William Fry, 2 Grand Canal Square, Dublin 2.
Filed this day of November 2016.

THE HIGH COURT

COMMERCIAL

Record No. 2016/4809P

BETWEEN

THE DATA PROTECTION COMMISSIONER

Plaintiff

-and-

FACEBOOK IRELAND LIMITED AND MAXIMILLIAN SCHREMS

Defendants

AFFIDAVIT OF THOMAS BOUÉ

William Fry
Solicitors
2 Grand Canal Square
Dublin 2
D02 A342
www.williamfry.com

024205.0001