provider is compelled to give the communications sent to or from that selector to the government. The NSA receives all data collected through PRISM. In addition, the CIA and the FBI each receive a select portion of the data collected through PRISM. A selector must be a specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number. People are targeted and selectors are tasked. Only selectors used by non-US persons reasonably believed to be located abroad may be tasked. The government estimates that 89,138 persons were targeted under s. 702 during 2013. In 2015 there were 94,368 persons targeted under s. 702. A decision of the FISC from 2011 reveals that the government acquired more than 250,000,000 communications under this programme.

183. Upstream differs from PRISM in several respects. The acquisition occurs with the compelled assistance of service providers that control the telecommunications backbone – the network of cables, switches and routers - over which telephone and internet communications transit, rather than with the compelled assistance of internet service providers or similar companies. Upstream collection includes telephone calls as well as internet communications. Through Upstream collection the experts said that the NSA copies and searches streams of internet traffic as data flows across the internet backbone.

184. Prior to April, 2017 the situation with regard to Upstream was as follows. NSA Upstream collection acquired internet transactions that were *"to"*, *"from"*, or *"about"* a tasked selector. With respect to *"to"* and *"from"* communications, the sender or a recipient is a user of a s. 702 tasked selector. This is not necessarily true for an *"about"* communications. An about communication is one in which the tasked selector is referenced within the acquired internet transaction, but the target is not necessarily a participant in the communication. Collection of *"about"*

communications involves searching the **content** of internet communications traversing the internet backbone which are subjected to Upstream surveillance. The internet transactions are first filtered to eliminate potential domestic transactions and then screened to capture only transactions containing a tasked selector. Transactions which pass both screening operations are acquired by the NSA. As of 2011, the NSA acquired approximately 26.5m internet transactions a year as a result of Upstream collection. Necessarily, this is a small portion of the amount of Internet transactions subjected to the filtering process and of the number of worldwide Internet communications.

185. Upstream also captures Multiple Communications Transactions (MCTs). MCTs are Internet transactions that contain more than one discrete communication within it. If a single discrete communication within an MCT is to, from or about a s. 702 tasked selector and, at least, one end of the transaction is foreign, the NSA will acquire the entire MCT. This may include communications between persons who have no connection whatsoever with the s. 702 target and are not themselves targets for surveillance for national security purposes or otherwise.

186. On 26th April,2017, the FISC released an opinion addressing the United States government's submissions seeking reauthorization to conduct surveillance under s.702 of FISA. The experts said that the opinion states that the government will not "acquire" or "collect" communications that are merely about a target but it does not indicate that the NSA has stopped copying and searching communications as they pass through its surveillance equipment prior to "acquisition" or "collection". The opinion left unchanged the government's long standing ability to query s. 702 data using non-US person identifiers. The opinion authorises the conduct of surveillance for a year and is

a binding decision of the FISC. The government will have to reapply for authorization next year.

Mass surveillance?

187. There was a dispute between Mr. Schrems on the one hand and Facebook and the United States on the other hand as to how surveillance by the United States intelligence agencies should be characterised. Facebook and the United States said that in practice the surveillance was very targeted; it was not indiscriminate and it was not mass surveillance. Mr. Schrems on the other hand pointed to the vast number of communications acquired pursuant to the PRISM programme and to the method by which UPSTREAM operated. Ms. Gorski, who gave evidence on his behalf, was of the opinion that UPSTREAM involved searching billions of Internet transactions crossing the internet backbone and this must be regarded as mass surveillance. She referred to the generalised access by the government of the United States to the content of communications under s. 702 Upstream surveillance.

188. The United States government acknowledges that in certain circumstances it collects signals intelligence in bulk and that it may result in the collection of information about persons whose activities are not of foreign intelligence or counter intelligence value (PPD-28, s. 2). It maintains that it is not engaged in mass or indiscriminate surveillance.

189. Service providers are required by law to comply with directions served upon them by the relevant agencies and thus potentially the intelligence agencies have access to all of the data held by the service providers as a matter of law and practice. Collection of data from the service providers pursuant to PRISM is targeted. An individual is the target. An email address or mobile phone number that is associated with the target is the selector and it is tasked and the service provider is directed to

provide the communications responsive to the selector. As stated above, in 2015 there were 94,386 targets. However, this can multiply up to a very large number of communications. Targets communicate with non targets. Targets can have multiple selectors. In 2011, the government acquired more than 250,000,000 communications under s. 702 surveillance. PRISM accounts for approximately 90% of s. 702 surveillance so it can be seen that starting with less than 100,000 targets can result in the acquisition of an extremely large number of communications indeed. Of course, it is fair to say, as was pointed out on behalf of Facebook, that this in itself, though large, constitutes a very tiny proportion of the total number of internet communications.

190. UPSTREAM operates differently. It necessarily involves making huge numbers of non relevant communications available for surveillance by the NSA. The NSA then searches this vast number of communications. It retains the communications which it "acquires" or "collects" from the vast number of communications to which it has access. It has access to the content as well as the metadata of these communications.

191. It is of course inherent in targeted searching that a large body of data is searched. The true difference between Mr. Schrems on the one hand and Facebook on the other hand, was the focus by Mr. Schrems on the making available and initial searching of billions of communications passing through the internet backbone, while Facebook focused upon the fraction of these communications which was actually acquired or collected and therefore subsequently retained and made available for analysis.

192. There is a distinction between bulk searching and bulk acquisition, collection or retention. In my opinion, the evidence clearly establishes that under UPSTREAM there is mass surveillance in the sense that there is mass searching of communications.

The search is for targeted communications and is in that sense not indiscriminate. Even when targeted it involves the collection of non relevant data as explained above.

193. The Directive defines processing of personal data as including any operation or set of operations which is performed upon personal data such as collection... or otherwise making available the data. On the basis of this definition and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, it is clear that there is mass indiscriminate **processing** of data by the Unites States government agencies, whether this is described as mass or targeted surveillance.

Evidence on Relevant Data Protection Law in the United States

194. One of the experts described data protection law in the United States as an overlapping and labyrinthine array of statutory and non-statutory authorities. It is a complex web of constitutional law, sector specific federal statutes, state statutes and common law rules. This section of my judgment necessarily is a summary of the evidence adduced at trial and does not purport to be an exhaustive or comprehensive statement of the laws of the United States in this area.

195. The basic principle is that surveillance is legal unless forbidden and there is no requirement ever to give notice in relation to surveillance.

196. Data protection and data privacy rights, whether express or implied are to be found in the First and Fourth Amendments to the Constitution. The First Amendment, which relates to freedom of speech, did not feature in the evidence at trial.

The Fourth Amendment

197. The experts identified the Fourth Amendment to the Constitution as being the most important protection against unlawful government surveillance. The Fourth Amendment applies to searches and seizures that take place within the US (such as on

data transferred to the US). The prevailing assumption is that, as the law currently stands, non-EU citizens lacking substantial voluntary connection with the United States (such as the majority of EU citizens) may not bring a Fourth Amendment case. Thus, the foremost protection under US law against unlawful government surveillance is not available to most EU citizens. They may benefit indirectly from the protections guaranteed by the Fourth Amendment to those entitled to its protections.

Individual remedies available to EU citizens under US law

A. 18 U.S.C. Section 2712 (Stored Communications Act)

170. Section 2712 (a) permits a person who is aggrieved by a "willful" violation of certain specific statutory provisions to sue for damages. It applies to the Wiretap Act and the Stored Communications Act (together the Electronic Communications Privacy Act) and to three sections of FISA.

171. These are 50 USC sections 1806 (a), section 1825 and section 1845. Section 1845 is of no relevance to Mr. Schrems' reformulated complaint.

Section 1806 (a) prohibits the use or disclosure by Federal officers or employees except for lawful purposes of information acquired from an electronic surveillance within the United States for foreign intelligent purposes.

172. Section 1825 prohibits the use or disclosure by Federal officers or employees except for lawful purposes of information acquired from physical searches within the United States for foreign intelligent purposes.

173. The court may award as damages (1) actual damages, but not less than $10,000, whichever amount is greater and (2) litigation costs reasonably incurred. "Willful" in the context of a claim for damages under s. 2712 (a) has been held to mean both knowing and reckless violations of the statute.

174. Section 2712 amounts to an express waiver of sovereign immunity for the government. Damages may be recovered from the government. It is an exclusive remedy against the United States. Therefore, no relief other than damages may be obtained for breaches of these provisions.

175. Because s. 2712 provides an exclusive remedy for damages against the United States, it precludes action under the Administrative Procedures Act (as discussed below) for any of the causes of action listed in s. 2712. It does not apply to ss. 1810 or 1861 of FISA (s. 215 of PATRIOT Act).

176. There are minimisation procedures and other provisions in relation to ss. 1806, 1825 and 1845 which concern only United States persons – defined as US citizens and lawful residents or US corporations. Therefore, EU citizens who are not US citizens or residents would not be able to bring a claim under s. 2712 for non-compliance with the minimisation procedures or these other provisions.

B. 50 USC Section 1810

177. Under s. 1810 an affected person (other than a foreign power or an agent of a foreign power) who has been subjected to electronic surveillance, or about whom information obtained by electronic surveillance of such person has been disclosed or used, in violation of the provisions of s. 1809 can recover

(1) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of the violation, whichever is greater;

(2) punitive damages and

(3) reasonable attorneys' fees and other costs .

178. Section 1810 is not included within s. 2712. It does not operate as a waiver of sovereign immunity which means that the United States cannot be held liable under the section. Any case must be brought against the individual actors. Under s. 1810 the disclosure must be in breach of s. 1809 which means the plaintiff must prove willful/intentional violation of the section. There have been no prosecution of officers or employees under s. 1809 and the section was described by Professor Vladeck on behalf of Facebook as very narrow and difficult to prove.

179. Even if a plaintiff under s. 1810 could prove willful violation the plaintiff must still overcome possible issues of sovereign immunity and official immunity. Because there is no waiver of sovereign immunity with regard to the United States, it is arguable that sovereign immunity may extend to officers acting in their official capacity. If it does not, officers may still rely upon official immunity. The test is: the officer must have violated clearly established law of which a reasonable officer would have known. It is clear that the liability is personal and therefore the head of an agency may be entitled to claim official immunity in respect of proceedings brought under s. 1810 (even if he or she cannot assert sovereign immunity).

180. Professor Vladeck accepted that both of these possible immunities may prove substantial obstacles to relief. On the other hand, he was of the opinion that if the plaintiff could prove his or her case, it was likely that the government would indemnify the individual officer.

C. 50 USC Section 1806

181. Claims brought for willful violation of s. 1806 (a) are brought under s. 2712. Section1806 (e) provides an exclusionary remedy for a person against whom evidence gained by electronic surveillance is being introduced in criminal or administrative proceedings. The person against whom the evidence is being introduced has the right

to bring a motion to suppress the evidence gained by electronic surveillance if it is shown that the information was unlawfully obtained or that the surveillance was not made in conformity with an order of authorisation or approval. It does not of itself provide a remedy for unlawful processing of personal data.

182. To date, only eight criminal defendants have received notices of s. 702 surveillance. The only adversarial rulings by US courts on the legality of surveillance under FISA s. 702 to date have come through s. 1806 motions to suppress.

D. Electronic Communications Privacy Act (ECPA)

183. The Electronic Communications Privacy Act governs when electronic communications and wire communications can be intercepted or monitored. It is an exceptionally complex piece of legislation. It consists of the Wiretap Act and the Stored Communications Act (SCA). The Wiretap Act applies to the interception or accessing of information while in transmission. The SCA applies to the unauthorised access of stored communications. Remedies under the ECPA are generally available to both US citizens and foreign nationals and non citizens are entitled to protections of the ECPA. It is unclear whether suits can proceed against the agencies themselves in addition to the individual officers.

184. Section 2712 confers a cause of action for willful violation of the Wiretap Act or the SCA. Under the Wiretap Act it is a crime for persons to intentionally *intercept* or *procure* electronic communications, including email, unless certain exceptions apply. It is a violation of the Wiretap Act to *disclose* communications if the person making the disclosure knew or had reason to know that the communication was intercepted in violation of the ECPA.

185. Under the SCA it is illegal to obtain, alter or prevent authorised access to a wire or electronic communication while it is in electronic storage in such system if a person

"intentionally accesses without authorisation a facility through which an electronic communication service is provided" or "intentionally exceeds an authorisation to access that facility".

186. Claims for damages under the Wiretap Act or the SCA apply to wrongful collection and not just use and disclosure.

E. Privacy Act and Judicial Redress Act

187. The Privacy Act allows US citizens to access their records or information pertaining to those individuals held by governmental agencies and to review those records and have copies made. The head of any agency may promulgate rules to exempt certain systems of records from the Act. There is no blanket exemption for records collected by a particular agency. However, there are regulations prohibiting the disclosure of records pertaining to the functions and activities of the NSA. All systems of records maintained by the NSA are exempt from disclosure to the extent that the system contains information properly classified under an executive order and that is required by executive order to be kept secret in the interest of national defence or foreign policy. Thus, the NSA has exempted itself from the most significant protections afforded to individuals. As the NSA is the primary agency responsible for foreign intelligence signals gathering, this means that the Privacy Act for all practical purposes is likely to provide no remedy to an EU citizen.

188. In any event, it is necessary to establish that the disclosure was intentional or willful and that the disclosure had an adverse effect on the plaintiff. It is necessary to establish pecuniary loss and damage. Non economic harm is insufficient. *Federal Aviation Authority. v. Cooper* 137 S.Ct. 1441 (2012)

189. The experts stated that Privacy Act suits face numerous hurdles including subject matter exemptions, classified documents, the "routine use" exception, *F.A.A. v.*

Cooper limiting damages and most importantly the exemption of national security records from the coverage of the Privacy Act.

190. The Judicial Redress Act extended the protections of the Privacy Act to the covered records held by designated agencies in respect of covered countries. As of the 1st of February, 2017, all EU countries, with the exception of the United Kingdom and Denmark, are covered countries for the purposes of the Judicial Redress Act. However, the NSA is not a designated agency for the purposes of the Act therefore citizens of the EU may not bring a Privacy Act/JRA suit against the NSA.

191. There are also issues concerning the definition of covered records and covered countries which means that data initially transferred to a private company in the US and then acquired by a US government agency may not be a covered record. As the United States is not defined as a covered country, this may mean that sovereign immunity has not been waived with the result that any suit against any agency would be barred by a plea of sovereign immunity.

192. On the 25th of January, 2017, a new executive order on the topic of immigration was issued by President Trump. Section 14 states: -

> *"Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residence from the protection of the Privacy Act regarding personally identifiable information."*

The legal effect of the executive order is uncertain. The experts agree that the provision is a change in policy from the previous administration which had expanded the number of agencies that applied administrative Privacy Act protections to mixed systems of records (databases containing both US and non-US person information).

This order has been superseded as of the date of judgment but no evidence was given of the terms of the latest version of this executive order.

193. In practice it is extremely unlikely that the Privacy Act will afford a remedy for breaches of data protection to an EU citizen.

Administrative Procedure Act

5 U.S.C. Section 702

194. Only Professor Vladeck placed emphasis on the Administrative Procedure Act as a possible source of remedy. It was not referred to by Professor Swire who gave evidence on behalf of Facebook or Mr. Robert Litt in his letter to the Commission included as an annex to the Privacy Shield Decision. Professor Richards and Mr. Serwin who gave evidence on behalf of the DPC both discounted it as a meaningful avenue of redress for EU citizens.

195. The Administrative Procedure Act is precluded if a plaintiff has a remedy under an alternative statutory provision. By reason of the provisions of s. 2712 this means that the Act is precluded in relation to suits brought pursuant to the Wiretap Act, the SCA and ss. 1806, 1825 and 1845 of FISA. Claims under FISA 1810 and 1861 (s. 215 PATRIOT Act) are not precluded from the Administrative Procedures Act as discussed above.

196. The Act provides that *"any person suffering legal wrong because of agency action or adversely affected or aggrieved by agency action is entitled to seek judicial review."* Even where the Act applies the remedies available are subject to limitations. A plaintiff must establish that he or she falls within "the zone of interest" of the Act and that the action complained of is "a final agency action". It is not clear whether monitoring a particular individual's communications for the purposes of national security is "a final agency action" under the APA, but Professor Vladeck believes that

a directive to a service provider would qualify as a final agency action. He adduced no authority to support this opinion. A plaintiff may obtain injunctive or declaratory relief (provided the complained of action has not ceased) but not damages under the APA.

Standing

197. While there are a variety of possible judicial remedies open to EU citizens in respect of possible unlawful processing of their private data by United States agencies as I have set out, in all cases it is necessary for a plaintiff to establish that he or she has standing to bring the suit. This is a very complex matter in the context of secret government surveillance. All of the evidence show that it is an extraordinarily difficult hurdle for a plaintiff to overcome. It constitutes a substantial obstacle to maintaining any of the causes of action discussed.

198. Under Article III of the US Constitution, a plaintiff must have standing to bring suit before a federal court as a precondition to bring a claim. The party invoking federal jurisdiction bears the burden of establishing the following three elements:

(1) that it has suffered an injury in fact – an invasion of a legally protected interest which is (a) concrete and particularised and (b) actual or imminent, not conjectural or hypothetical;

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

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

199. In *Clapper v. Amnesty International* US, 133 S.Ct. 1138 [2013] the Supreme Court considered the imminence test of "injury in fact" in the context of alleged

unlawful surveillance by the Director of National Intelligence of the communications of the plaintiffs. The court held that it meant "certainly impending". It rejected the formulation of the Second Circuit that "objectively reasonable likelihood" that communications will be interfered with was sufficient to meet the test of "injury-in-fact".

200. This decision makes it more difficult for plaintiffs to establish standing in the absence of express notice that they personally have been surveilled. This is particularly significant as there is no notification obligation. The experts agreed that in the absence of notice that a plaintiff has been the subject of surveillance (and thus his data processed), it would be very difficult to challenge that surveillance. In the vast majority of cases persons surveilled will never receive notice of the fact –and therefore they will not be in a position to challenge the surveillance both because of their ignorance of a possible claim and their inability to establish standing as required by *Clapper*.

201. The application of the test depends upon what is called the posture of the case. A plaintiff's standing to sue can be challenged on the basis of the pleaded case by a motion to dismiss, in which case the plaintiff is required to show that he has plausibly pleaded his case in order to survive the motion to dismiss. The facts are assumed in his favour but they must amount to a legal wrong, if proven. His standing may also be challenged by a motion for summary judgment. If that occurs, it is not sufficient for the plaintiff to plead plausible allegations; he must adduce evidence to support his claim and if he fails to do so his action will be dismissed.

202. *Clapper* was an application for summary judgment and the plaintiffs failed because they failed to prove facts that the injury alleged was imminent.

203. *Wikimedia Foundation v NSA* (4th Cir. 15-2560) was a decision of the Fourth Circuit of Appeals on a motion to dismiss the claims of the plaintiffs delivered on 23 May, 2017. Wikimedia engages in more than 1 trillion international communications a year in almost every country on the globe. It challenged the Upstream programme pursuant to s. 702 based on the manner in which Upstream operates as acknowledged by the PCLOB report, the vast number of its communications and the geographical diversity of the people with whom it communicates. It said its communications almost certainly travers every international backbone link connecting the United States with the rest of the world. If the NSA is monitoring a single internet backbone link then the NSA is intercepting, copying and reviewing at least some of its communications. Wikimedia. The court held that Wikimedia had plausibly alleged that its communications travelled all of the roads that a communication can take and that the NSA seizes all of the communications along at least one of those roads. It therefore had standing at a motion to dismiss stage to sue for a violation of the Fourth Amendment.

204. The court emphasised the importance of the distinction between motions to dismiss and summary judgments in determining whether the plaintiff had standing to sue. The court held that Wikimedia had standing as it had pleaded an actual and ongoing injury. Because it pleaded an actual injury, the analysis of an impending injury set out in *Clapper* did not apply. On the other hand the court held that none of the other plaintiffs had plausibly pleaded a case – their case was different to that of Wikimedia- and therefore dismissed their claims at the motion to dismiss stage of the proceedings.

205. In addition to proving that the complained of wrong had occurred (actual) or was imminent, a plaintiff must also satisfy the "concrete and particularised" limb of the test. "Particularised" means that it affects the plaintiff in a personal and individual way.

"Concrete" means that the harm may not be hypothetical. It must be real not abstract. It may be intangible and still concrete, but a bare procedural violation of a statutory right is not sufficient. (See *Spokeo v. Robbins*) 135 S. Ct. 1892 (2016) Therefore a simple violation of an individual's statutory right may not be sufficient of itself to establish standing.

206. Interference with data was accepted by the court as sufficient to establish standing for the purposes of a claim for a violation of the Fourth Amendment in *Wikimedia.* The experts disagreed whether *Spokeo* meant that a plaintiff suing for violation of a statutory right would be required to show more than interference with his data in order to satisfy the concrete limb of the test for standing ie whether he was required to show damage. In *FAA v Cooper* 1320S. Ct 1441 (2012) the Supreme Court held that for a claim under the Privacy Act the plaintiff was required to prove pecuniary loss.

207. The experts all agreed that standing is notoriously indeterminative and that it is possible to find cases across a range of possibilities. Many cases have been dismissed for want of standing and others have not. There is significant uncertainty in the federal district courts over exactly when *Clapper* does and does not foreclose standing. There was a dispute among the experts as to the degree of the uncertainty and thus the difficulty in establishing standing. The experts agree that the government failure to notify individuals subject to its secret surveillance programs makes it more difficult for plaintiffs to establish standing.

208. The difficulties with regard to standing can be illustrated by two recent decisions. In *ACLU v. Clapper*, 785F3d 787 (2nd Cir. 2015) the second circuit was concerned with a s. 215 programme which authorised the collection of all of the metadata of all of the customers of Verizon in the United States. The FISC had

authorised this metadata programme on 41 occasions pursuant to s. 215 of the PATRIOT Act. Edward Snowden leaked the actual FISC order and it was thus clear that it applied to all customers of Verizon. ACLU was a customer of Verizon. Thus, it was able to satisfy the test for injury in fact as set down in *Clapper v. Amnesty International* as it could show an actual injury and not an imminent injury.

209. But for the fact the particular programme collected the data of **all** of the customers of Verizon, ACLU might not have been able to satisfy the test for standing in light of the decision in *Clapper v. Amnesty International.*

210. The case highlights the significance of the absence of notice. ACLU had no notice of the metadata programme and therefore was unaware of the fact that it was subject to surveillance and could not sue in respect of the surveillance. It was only as a result of the illegal leaks of Mr. Snowden that it became aware of the surveillance and that it had a possible cause of action.

211. The case also illustrates the importance of judicial review. The second circuit struck down the metadata programme in its entirety on the basis that it exceeded the statutory authorisation for such surveillance (to obtain foreign intelligence). This was so even though the programme had received prior authorisation from the FISC on 41 occasions.

212. It underscores the importance of remedies to protect the rights of individuals, not just the particular plaintiff. If the case had not been brought, the programme would not have been declared unlawful and the surveillance of millions of persons could have continued unchallenged. Incidentally, it should be noted that the case was brought on the basis of the Administrative Procedure Act and the Fourth Amendment, and an EU citizen would have been confined to the action under the APA, with all the technical difficulties involved in bringing forward such a claim.

213. The second case is *Wikimedia.* Wikimedia was held to have standing at the motion to dismiss stage of the proceedings because it could plausibly allege that its communications were so vast that they must travel **all** the roads that a communication can take **and** that the NSA seizes **all** of the communications along at least one of those roads. There will be very few other plaintiffs able to advance such acclaim. On the other hand the other plaintiffs, who included Amnesty International, Human Rights Watch and the National Association of Criminal Defense Lawyers, were held not to have standing even at this stage of the proceedings. Their case was that the NSA is intercepting "*substantially all*" text-based communications entering and leaving the United States. However, they could not assert enough facts about Upstream's operational scope to plausibly allege a dragnet that must capture their communications and, following *Clapper,* an *"objectively reasonable likelihood"* that their communications would be intercepted was not sufficient.

Systemic Safeguards and Oversights

214. The FISC oversees the activities of the agencies who obtain orders for the collection of data under s. 215 or the annual certifications that provide the basis for collection of data under s. 702. As stated above, there is no judicial approval of individual selectors to query the data collected under s. 215 or tasked for collection under s. 702. The FISC operates *ex parte* and in secret. Its orders and opinions are classified, unless they are declassified. Increasingly, more material has been declassified. There is no judicial oversight of the collection of foreign intelligence outside the US, including pursuant to transit authority, under executive order 12333.

215. The FISC (and the FISCR) is supported by a standing panel of five individuals that have an expertise in national security matters as well as civil liberties. From this group the court may appoint an individual to serve as an a*micus curiae* to assist in the

consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law. This ensures that there can be a suitably qualified interlocutor to engage with the government on what would otherwise be *ex parte* applications.

216. Professor Swire on behalf of Facebook gave evidence of the fact that the FISC has in the past refused to authorise certain programmes, has rigorously scrutinised the targeting and minimisation procedures and issues of non-compliance with these procedures which have been reported to the court. Where data has been obtained without due authorisation, the FISC has directed the destruction of the data.

217. The opinion of the FISC of 26 April, 2017 illustrates very close scrutiny by the FISC of the applications for certificates pursuant to s. 702 of FISA. The court is required to ensure that the requirements of the statute are satisfied and that procedures are reasonable in light of the Fourth Amendment. The opinion also illustrates the court monitoring and supervising compliance with its orders. The opinion referred to "significant non-compliance with NSA minimization procedures" which it said were widespread. It detailed a number of violations of earlier orders by the FBI and the CIA. It said that the NSA had failed to give the court timely notice of the issue and revealed "an institutional lack of candour" and emphasised that this was a very serious Fourth Amendment issue. The government was forced to end "about" collection under Upstream in light of the non-compliance with the previous procedures which protected the privacy of US persons.

218. The US intelligence agencies are subject to various review and oversight mechanisms. According to PPD-28, s. 4 (a) (iv), the policies and procedures of the intelligence community elements *"... shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information... "*.

These measures include periodic auditing. Multiple oversight layers have been put in place including civil liberties or privacy officers, Inspectors General, the office of the Director of National Intelligence Civil Liberties and Privacy Office and the President's Intelligence Oversights Board.

219. The civil liberties or privacy officers supervise procedures to ensure that the relevant agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints. Each agency has its own Inspector General with responsibility to oversee foreign intelligence activities. They are authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority in connection with Office of the Director of National Intelligence (ODNI) or the programmes or activities of agencies. Inspectors General may issue non-binding recommendations for corrective action. Their reports are made public and sent to Congress. Civil liberties and privacy officers periodically report to Congress and the PCLOB.

220. The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency within the executive branch composed of five presidential appointees. It receives reports from the civil liberties and privacy officers of several departments and agencies and regularly reports to congressional committees and the President. Currently and for some months it has only one member and is inquorate.

221. In addition, the Department of Justice and the Department of Defence each provide extensive oversight of intelligence activities. In the NSA alone there are over 300 employees dedicated to compliance issues.

222. Agencies are required to report incidents of non compliance with the rules and procedures authorising the collection of signals intelligence. The reports are to the head of the particular intelligence community element, the Director of National

Intelligence and the Intelligence Oversight Board. This is to ensure that an issue will be addressed at the highest level. They are also reported to FISC.

223. In considering the weight to be attached to these extensive provisions it is worth bearing in mind the limitations which have been shown to exist notwithstanding the best efforts of those concerned in carrying out this very extensive oversight of the intelligence agencies. It is apparent from the opinion of the FISC of 26 April, 2017 that it is dependent upon the agencies acting promptly and with candour, something that may, at times, be lacking. In this regard, I should note that the FISC authorised the revised targeting and minimization procedures despite the reported instances of non-compliance with prior orders of the court based largely on "the extensive oversight conducted within the implementing agencies" and by the Department of Justice and ODNI. It held that "due to those efforts, it appears that compliance issues are generally identified and remedied in a timely and appropriate fashion". Further, it should be remembered that the programme that was struck down in *ACLU v Clapper* on the basis that it far exceeded what was authorised by the statute had been authorised by the FISC on 41 occasions.

224. In addition to executive oversight mechanisms, the US Congress, specifically the House and Senate Intelligence and Judiciary committees, have oversight responsibilities regarding all US foreign intelligence activities, including US signals intelligence. The President is obliged to keep the congressional intelligence committees fully and currently informed of the intelligence activities of the United States including any significant anticipated intelligence activity. The President is to ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees as well as any corrective action that may have been taken or is

planned in connection with such illegal activity. The oversight committees have subpoena power and access to classified information.

225. The USA FREEDOM Act 2015 requires the government to disclose to Congress and the public each year the number of FISA orders and directives sought and received as well as estimates of the number of US and non-US persons targeted by surveillance. There has been an increased emphasis on declassifying the opinions of the FISC and the targeting and minimisation procedures adopted by the respective agencies pursuant to the orders of the FISC.

Conclusions in Relation to the Evidence Regarding Remedies

226. There are a variety of very significant barriers to individual EU citizens obtaining any remedy for unlawful processing of their personal data by US intelligence agencies.

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

228. The necessity for a plaintiff to establish that he has standing to sue constitutes a very substantial obstacle to any legal remedy. *Clapper v. Amnesty International* has made it exceedingly difficult to challenge secret government surveillance programmes, according to Professor Swire, who gave evidence on behalf of Facebook. Establishing an objectively reasonable likelihood that one has been the subject of surveillance is insufficient to satisfy the standing requirement. (*Clapper v. Amnesty International*, *Wikimedia v. NSA*).

229. The absence of express notice makes it even more difficult to meet the threshold for standing set by the Supreme Court in *Clapper v. Amnesty International* (see *Wikimedia* in contrast to *ACLU v. Clapper*) even if the plaintiff believes that it is highly likely that their data have been or will be accessed and/or acquired by one or more of the US intelligence agencies.

230. Under FISA, the personal data of an EU citizen can be seized, accessed and retained by a US government agency without the agency proving probable cause prior to obtaining a warrant in respect of the individual EU citizen from the FISC. There is no need to obtain any authorisation for surveillance conducted under EO 12333.

231. By far the most significant avenue of redress for unlawful interference with personal data is a claim for violation of the provisions of the Fourth Amendment. Such a claim is not open to EU citizens lacking a substantial voluntary connection with the US.

232. There are a number of possible causes of action potentially open to EU citizens in respect of processing of their data by government intelligence agencies in the United States, but on closer analysis it becomes clear that there are substantial obstacles to recovery in respect of some causes of action such that in reality an EU citizen is most unlikely to obtain a remedy for unlawful acquisition or processing of his personal data (actions under the Privacy Act or s. 1810 of FISA). A motion to suppress evidenced to be adduced in a criminal trial pursuant to s. 1806 of FISA is not a general remedy for wrongful interference with personal data. This in effect leaves claims for damages under s. 2712 of ECPA or claims under the APA. Some causes of action require the plaintiff to establish that he or she has suffered damage, which has been held to mean pecuniary damage. This is a significant limitation on the right to seek a remedy that does not apply under EU law. In *Schrems* para. 89 the CJEU noted that it has

repeatedly stressed that to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the person concerned has suffered any adverse consequences on account of the interference.[4] For claims under s. 2712 a plaintiff is required to prove a willful violation of the statute by an individual actor. How difficult this may be will obviously depend upon the facts of the case.

233. A claim under the APA only lies if there is no other statutory claim available. This rules out many potential cases. Even where the claim is not precluded, there is uncertainty whether it extends to collecting, processing or retaining the data of a particular individual.

234. In my opinion, despite the number of possible causes of action, it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by its intelligence agencies. On the contrary, the individual remedies are few and far between and certainly not complete or comprehensive.

235. I accept the conclusion of Professor Vladeck that retrospective judicial remedies will likely be unavailing to victims of governmental overreaching in the conduct of surveillance for the purpose of national security.

227. Quite clearly there are extensive rules to ensure that data is obtained in accordance with law and data, once obtained, is not misused. This is not the same as of providing a remedy where the rules are broken and data is unlawfully collected or otherwise misused. Protections against excessive or inappropriate surveillance are essential to an acceptable system of State surveillance. It is vitally important to ensure that secret surveillance does not exceed what society deems to be the appropriate limitations for such surveillance. But no system can ever be perfect. This is clearly illustrated by the FISC opinion of 26 April, 2017. There is a fundamental difference

---

[4] See also *Digital Rights* and *Watson*

between protections and safeguards on the one hand and remedies on the other. A protection cannot be a remedy though obviously the better the protection the less likely it is that a recourse to a remedy will be required. A remedy is to be available when the protections have in a sense failed.

228. Professor Swire gave as his opinion that it is sometimes difficult to provide individual remedies in the intelligence setting because of the risk of revealing classified information to hostile actors. He stated *"the desirability of individual remedies, in intelligence systems must be weighed against the risks that come from disclosing classified information"*

229. Article 52 of the Charter requires that the essence of the right be respected. In this case, the essence of the right under Article 47 of the Charter is the right of an individual to an effective remedy before a tribunal. The question of the desirability of individual remedies as referred to by Professor Swire does not arise if the essence of this right is not protected.

Article 47 of the Charter

(I) Is it Engaged?

256. The DPC in considering Mr. Schrems' reformulated complaint did not conduct an adequacy assessment in respect of the laws of the United States in relation to data protection and privacy. She conducted an inquiry into the essence of Mr. Schrems' rights under Article 47 of the Charter and then considered whether the essence of the rights guaranteed by Article 47 of the Charter were protected when his personal data were transferred by Facebook to Facebook Inc. and thereby made available to be processed by the United States intelligence agencies.

257. This approach was heavily criticised by Facebook, the government of the United States and two of the other a*mici curiae.*

Submissions of Facebook

258. Facebook argued that the DPC had not analysed whether there was any infringement of Mr. Schrems' fundamental rights and freedoms guaranteed under Articles 7 and 8. It submitted that this was a precondition to any question of a right under Article 47 arising and that therefore her entire analysis was flawed and must be rejected.

259. It seems to me that this argument is inconsistent with the requirement that each right under consideration (in this case the right to an effective remedy in the event that there is a breach of the protection of the data privacy rights of EU citizens whose data are transferred to the United States) must be individually assessed and the requirements of each Article engaged must be satisfied. This was emphasised by both the Advocate General and the court in *Schrems* (opinion para. 170 and 173; ruling paras. 94-95) and the Advocate General in *Digital Rights* (paras 60 – 61). The case was predicated upon the question that, insofar as there are breaches of EU citizens' data protection rights in the US, do the EU citizens have the same type of effective remedy before an independent and impartial tribunal of the type envisaged by Article 47 in the United States? Therefore, it is this question which must be addressed.

260. Facebook argues that Article 47 applies to rights and freedoms guaranteed by the law of the Union. It submits that the national security of the individual member states remains the sole responsibility of each member state (Article 4 of TEU). It follows, according to Facebook, that Article 47 is not engaged at all.

261. In addition, Facebook argues that if the actions complained of in these proceedings occurred in a Member State there would be no question of an Article 47

right to an effective remedy as the Charter would not apply to the actions of a Member State in the area of national security. On that basis, it says, the laws and practices of the United States cannot fail the essential equivalence test enunciated by CJEU in *Schrems*.

Discussion

262. It seems to me that these submissions are incorrect. In *Schrems* it was accepted by the Advocate General and CJEU that Article 47 applied notwithstanding the fact that the interference with personal data of EU citizens in question resulted from surveillance by the United States intelligence services. At para. 173 of his opinion, Advocate General Bot noted that the referring court found that in the United States citizens of the Union have no effective right to be heard on the question of the surveillance and interception of their data. He considered that this amounted to an interference with the rights of citizens of the Union to an effective remedy, protected by Article 47 of the Charter. The CJEU likewise considered that Article 47 applied in the circumstances of that case (see para. 95). The Court, in those circumstances, had no difficulty in applying the essential equivalence test.

263. In *ZZ v. Secretary of State for the Home Department* [2004] EWCA Civ 1578 the CJEU considered a decision of the United Kingdom refusing a citizen of the European Union admission to the United Kingdom on public security grounds. The Directive engaged in that case was Directive 2004/38/EC which concerned the freedom of movement of persons and the question referred related to the interpretation of Article 30 (2) of the Directive read in the light in particular of Article 47 of the Charter. At para. 38 the court stated: -

> *"... although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision*

concerns State security cannot result in European Union law being inapplicable"

ZZ was concerned principally with the application of Article 47 of the Charter in the context of a decision by the relevant authorities not to disclose information to ZZ on the grounds of national security. Thus, it is clear that as a matter of principle Facebook's argument in this regard is incorrect.

264. Finally, it should not be lost sight of that the transfers of data to which Mr. Schrems objects are the transfers by Facebook to Facebook Inc. in the United States and clearly EU law is engaged in respect of these transfers. He thus has the benefit of the fundamental rights and freedoms guaranteed to him by the Charter including the rights guaranteed under Article 47. This applies even though the processing which may give rise to a claim is that which may arise from subsequent interference with his personal data by intelligence agencies of the United States.

265. For these reasons, I believe that Article 47 of the Charter is engaged in these proceedings.

(II) Do the laws of the United States respect the essence of Article 47?

Submissions of the DPC

266. The DPC submits that, pursuant to Article 47, everyone whose rights and freedoms guaranteed *inter alia* by Articles 7 and 8 of the Charter and of the Directive are violated, has the right to an effective remedy before an independent and impartial tribunal. It was accepted by all parties that, pursuant to Article 52 (1) of the Charter, this right could be limited. Any limitation on the exercise of the right must be provided for by law and respect the essence of the right and freedom.

267. The DPC says that US law does not respect the essence of the right guaranteed by Article 47 to an effective remedy before an independent tribunal and that therefore it is not necessary to conduct a proportionality assessment of US law.

268. The DPC submits that there is an absolute requirement on intelligence agencies who have, in one way or another, surveilled the data of EU citizens to notify the persons affected as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities: - (*Watson* para.121).

> *"Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed This is so as notification is in fact necessary to enable the persons, affected to exercise their right to a legal remedy."*

269. While *Watson* is a decision of CJEU on Article 47 of the Charter, the reasoning reflects the jurisprudence of ECHR. In *Zakharov v. Russia* (case 47143/06) [2015] ECHR 1065 the ECHR considered secret surveillance laws in Russia in a case brought by a journalist who believed, but could not prove, that he had been the target of surveillance by state authorities. At para. 287 the ECHR held as follows: -

> *"It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual*

affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. ***As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned****... In the cases of Association for European Integration and Human Rights and Ekimdzhiev and Dumitru Popescu (no. 2), the Court found that* ***the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective****... in the case of Kennedy the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications."* (emphasis added)

270. Article 52 (3) of the Charter provides that insofar as the Charter contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights shall be the same as those laid down by that Convention. The provision does not prevent Union law from providing more extensive protection. In this case Article 13 of the Convention provides the right to an effective remedy which corresponds to Article 47 in the Charter. It follows therefore that Article 47 cannot be interpreted as providing for a lesser remedy than Article 13 of the Convention as expounded in the jurisprudence of the ECHR.

271. The DPC submits that US law never requires that the subject of surveillance receive notification at any time of the surveillance. She argues that this is critical to the right to an effective remedy as guaranteed by Article 47 of the Charter. It was accepted by the experts on the law of the United States that most people never know that they have been the subject of surveillance and if they do not know that effectively they can never sue. Thus, the DPC agrees with the conclusion of Professor Brown in Brown et al. "Towards Multilateral Standards for Surveillance Reform", (2015) that US law does not satisfy the requirements of the ECHR in relation to Article 13 and thus does not satisfy the requirements of Article 47.

272. Secondly, the DPC submits that the essence of an Article 47 right is a right to the possibility of a judicial remedy or at the very least a remedy from an independent tribunal. She argues that the law in relation to standing in the United States makes it extremely difficult to establish standing for an EU citizen who alleges interference with his personal data. Professor Swire accepted that it would be exceedingly difficult to challenge secret surveillance by government agencies for EU citizens and Professor Vladeck stated that it was likely that retrospective judicial remedies will be unavailing.

273. This is to be contrasted with the situation under European Union law. In *Verholen v. Sociale Verzekeringsbank Amsterdam* (Cases C-87/90, C-88/90 and C-89/90) [1991] E.C.R. I-3757 para. 24 the ECJ held: -

> *"While it is, in principle, for national law to determine an individual's standing and legal interest in bringing proceedings, Community law nevertheless requires that the national legislation does not undermine the right to effective judicial protection and the* ***application of national legislation cannot render virtually impossible the exercise of the rights conferred by Community law.*** *"* (emphasis added)

274. In *Unibet (London) Ltd and Unibet (International) Ltd v. Justitiekanslern* (Case C-432/05) [2007] E.C.R. I-2271 the ECJ noted at para. 43 that: -

> *"... the detailed procedural rules governing actions for safeguarding an individuals' rights under Community law...* ***must not render practically impossible or excessively difficult the exercise of rights conferred by Community law...*** *"*(emphasis added)

275. The DPC says the effect of the rules of standing in the United States is to make the bringing of cases practically impossible or excessively difficult and that this effectively undermines the right to effective judicial protection. She submits that this fails to respect the essence of the fundamental right to an effective remedy guaranteed by Article 47.

276. She also argued that the US rules with regard to standing were more stringent than those accepted by the ECHR and this had the effect of rendering the remedies available under US law theoretical and illusory rather than practical and effective. In *Zakharov* the court summarised the case law of the ECHR and at para. 171 concluded: -

"The Court accepts that an ***applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures****, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies....* ***where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance****, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential*

users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law in abstracto, is justified. ***In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be***

a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures." (emphasis added)

277. It is submitted by the DPC that this test is far more liberal than the test to be found in the United States in cases such as *Clapper v. Amnesty International* and *Wikimedia*. Thus, the United States rules on standing in the area of national security are far more stringent than those established by ECHR.

278. The DPC highlighted the fact that the most important cause of action available in the United States to challenge unlawful interference with personal data, claims for a breach of the Fourth Amendment, are not available to EU citizens who do not have substantial voluntary connections with the United States and therefore are not available to the vast majority of EU citizens.

279. She also points to the extremely limited nature of the statutory remedies available to EU citizens and concludes that for all of the above reasons, the essence of the right to an effective remedy before an independent and impartial tribunal is not respected by the laws of the United States in the context of interference with the personal data of EU citizens by intelligence agencies on the grounds of national security. [5]

Submissions of Facebook and the United States

280. Facebook and the government of the United States argued that it was not appropriate to focus solely on the question of individual redress in the United States. They each urged that it was essential to consider the totality of the regime in relation to the authorisation of surveillance, the practice of targeting selectors, the minimisation

[5] I shall consider the Ombudsperson mechanism in the Privacy Shield decision below.

procedures, the multiple levels of oversight to ensure compliance with procedures, the procedures governing the acquisition of data, the storage of data, access by individuals and agencies to the raw data, retention and dissemination of the data.

281. They submitted that the essence of the Article 47 right was respected as EU citizens had available individual causes of action for substantive remedies before the courts in the United States. They emphasised that the CJEU in *Schrems* at para. 95 had established that it was only if there was *no possibility* of a remedy before a national court that the essence of the Article 47 right to an effective remedy was not respected. This is not the case in the United States and therefore the essence of the Article 47 right was respected.

282. In addition, they submitted that the DPC had overstated the difficulties of establishing standing in the United States and that, in essence, if an EU citizen had notice that he or she had been surveilled that he or she would likely have standing to sue for relief under one or more of the statutory remedies on the basis of *ACLU* and *Clapper v. Amnesty International*.

283. That being so, Facebook and the United States urged that a proportionality assessment is required before it can be said that any limitation on the exercise of a right or freedom recognised by the Charter is impermissible.

284. Facebook argued that when looking at the processing of data for the purposes of national security one does not look at the rights enshrined in the Directive. The test is not whether there is a high level of protection or an adequate level of protection or sufficient safeguards. The question is whether the interference with the rights of the data subject for national security purposes exceeds that which is strictly necessary and proportionate. Are the measures strictly necessary to achieve the objective of preserving national security?

285. Facebook referred to ECHR jurisprudence which has jurisdiction in the field of national security. It submitted that the case law establishes that when considering remedies in the context of national security, the court will consider the entire regime in the particular jurisdiction. It recognises that the concept of an effective remedy cannot carry the same meaning in the context of secret intrusive measures because the efficacy of such measures depends upon their remaining secret. Therefore, an effective remedy within the meaning of Article 13 of ECHR must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance (see *Klass v. Germany* (App. No. 5029/71) [1978] 2 EHRR 214 para. 69.)

286. Facebook noted that in *Silver v. The United Kingdom* (1983) 5 EHRR 347 at para. 113 the court synthesised the principles on the interpretation of Article 13 of ECHR to include the following: -

> "*... (a) where an individual has an arguable claim to be the victim of a violation of the rights set forth in the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress,*
>
> *(b) the authority referred to in Article 13 may not necessarily be a judicial authority but, if it is not, its powers and the guarantees which it affords are relevant in determining whether the remedy before it is effective,*
>
> *(c) although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so.*"

287. Facebook submitted that the aggregate of the protections and remedies available in the United States provides an effective remedy as required by Article 47 of

the Charter. It referred to the authorisation by the FISC of the annual certifications in respect of each of the intelligence agencies, the ongoing oversight exercised by the FISC in respect of the individual agencies, the multiple levels of oversight both within the agencies, the Department of Justice, the ODNI, the Directors General as well as Congressional oversight. It said that the scope of the individual remedies available in the US to EU citizens must be seen in this context of oversight before, during and after acquisition of personal data. When viewed in this way, it is clear that US law and practice provides greater protections to EU citizens in respect of their personal data than is in fact available to them in practice in individual Member States within the EU. The limitations on the data protection rights of EU citizens in the circumstances satisfy the strictly necessary threshold and genuinely meet objectives of general interest recognised by the Union and are needed to protect the rights and freedoms of others as required by Article 52 (1) of the Charter.

Response of the DPC

288. In response, the DPC argued that US law fails to satisfy the tests established by the ECHR. In *Sakharov,* the ECHR conducted precisely the type of proportionality test in respect of the law and practices of Russia which Facebook said ought to have been conducted by the DPC in relation to the regime in the United States. In two significant respects, (1) in relation to the obligation to give notice when notice would no longer jeopardise the surveillance actually conducted and (2) the rules in relation to standing, the laws of the United States failed to pass these tests. This is confirmed by Professor Brown where he states at p. 3 of his work that the Convention "... *sets a higher general standard than the US government's interpretation of its international human rights law obligations as applying only within its own territory.*" He notes at para. 3.4 that despite the relatively weak standards on foreign intelligence collection by EU

member states, the Convention sets relatively high standards in terms of compliance of all surveillance regimes with the rule of law. He identifies a number of minimum standards. The last two of these points are: -

> *"Persons who have been subjected to surveillance should be informed of this as soon as this is possible without endangering national security or criminal investigations, so that they can exercise their right to an effective remedy at least ex post facto; and*
>
> *The bodies charged with supervising the use of surveillance powers should be independent and responsible to, and be appointed by, Parliament rather than the Executive."*

289. The DPC submitted that the legal regime in the United States fails the strictly necessary test laid down in Article 52 (1) of the Charter in relation to interference with personal data on the grounds of national security. She submitted that there was no explanation why it is necessary to have strict rules in relation to standing with no latitude afforded to potential litigants to reflect the inherent difficulties in litigation in this area. She submitted that there was no explanation why notification along the lines similar to those described in *Watson* and *Zakharov* applied in the United States or why it was necessary to maintain in all cases for all time a policy of "neither confirm nor deny" that surveillance has taken place. Inherent in the *Watson* formula is accommodation for the danger posed by the so called "hostile vector attack".

Conclusion

290. To my mind the arguments of the DPC that the laws -and indeed the practices- of the United States do not respect the essence of the right to an effective remedy before an independent tribunal as guaranteed by Article 47 of the Charter, which applies to the data of all EU data subjects transferred to the United States, are well

founded. Furthermore, even if the essence of that right is respected, there are, for the reasons advanced by the DPC, well founded concerns that the limitations on the exercise of that right faced by EU data subjects in the United States are not proportionate and are not strictly necessary within the meaning of Article 52 (1) of the Charter.

291. The remaining issue therefore is whether the introduction of the Ombudsperson mechanism changes this assessment.

The Ombudsperson Mechanism

291. The Privacy Shield Decision was adopted after the CJEU in *Schrems* declared that the Safe Harbour Decision was invalid. Analysis by the working group, and the Commission highlighted concerns about the limits on individual redress for EU citizens in relation to data subjected to processing by the United States for purposes of national security. Recital 115 of the Privacy Shield Decision provides: -

> *"While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show 'standing', which restricts access to ordinary courts."*

292. It is thus clear that as of the 12th of July, 2016, when the decision was adopted, the Commission had concerns about the adequacy of the avenues for individual redress in the United States. Recital 116 records that: -

"In order to provide for an additional redress avenue accessible for all EU data subjects, the U.S. government has decided to create a new Ombudsperson Mechanism..."

293. The Ombudsperson will be appointed by the Secretary of State and will be independent from the intelligence community but operate within the Department of State. He or she will be part of the executive branch of government. The Ombudsperson will deal with requests received from EU citizens. Each EU citizen will send their individual requests to the supervisory authorities in his or her Member State. There is no requirement to demonstrate that the requester's data has in fact been accessed by the US government through its signals intelligence activities and the requester can deal with the matter through his own language. The supervisory authorities ensure that the request is in order and it is not frivolous, vexatious or not *bona fide*. They then forward the request to the EU individual complaint handling body. The EU body then submits the complaint to the Ombudsperson in the State Department.

294. The Ombudsperson will work closely with the United States government officials including independent oversight bodies to ensure that the requests are processed on the basis of necessary information and resolved in accordance with the applicable laws and policies. The Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policy. The response will confirm (1) that the complaint has been properly investigated, and (2) that the US laws, statutes, executive orders, presidential directives and agency policies providing the limitations and safeguards described in the annex to the Privacy Shield Decision have been complied with or, in the event of non-

compliance, that such non-compliance has been remedied. Critically, the Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Ombudsperson confirm the specific remedy that was applied.

295. There was some uncertainty as to whether the Ombudsperson mechanism applied in respect of EU citizens whose data is transferred pursuant to the SCCs. The mechanism is described in Annex A to the Privacy Shield Decision. On page 72 of the decision it records the fact that the new mechanism is: -

> "*to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), Derogations, or Possible Future Derogations*".

Clause 3 (B) requires the EU individual complaint handling body to verify that the request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to "*the Privacy Shield, SCCs, BCRs, derogations, or possible future derogations.*" In the circumstances, I am satisfied that it is open to an EU citizen who reasonably believes that his or her data have been transferred from the EU to the United States pursuant to the SCCs to make a request to the Ombudsperson through the mechanism established as part of the Privacy Shield Decision. It is therefore relevant to the assessment of the issues before the court.

Submissions of Facebook

296. Facebook relied upon the Ombudsperson mechanism. It said the Commission was of the view that the mechanism addressed any concerns regarding the adequacy of the individual avenues for redress in the United States. Recitals 122, 123 and 124 the Decision state: -

"(122) Overall, this mechanism ensures that individual complaints will be thoroughly investigated and resolved, and that at least in the field of surveillance this will involve independent oversight bodies with the necessary expertise and investigatory powers and an Ombudsperson that will be able to carry out its functions free from improper, in particular political, influence. Moreover, individuals will be able to bring complaints without having to demonstrate, or just to provide indications, that they have been the object of surveillance. In the light of these features, the Commission is satisfied that there are adequate and effective guarantees against abuse.

(123) On the basis of all the above, the Commission concludes that the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU-U.S. Privacy Shield.

(124) In this respect, the Commission takes note of the Court of Justice's judgment in the Schrems case according to which "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification of erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter." The Commission's assessment has confirmed that such legal remedies are provided for in the United States, including through the introduction of the Ombudsperson mechanism. The Ombudsperson mechanism provides for independent oversight with investigatory powers. In the framework of the Commission's continuous monitoring of the Privacy Shield, including through

the annual joint review which shall also involve the Ombudsperson, the effectiveness of this mechanism will be reassessed."

297. Facebook argues that the legal regime analysed by the Commission is (essentially) the same as the legal regime which falls to be considered by this court and that the Ombudsperson mechanism applies to the SCCs as well as to data transferred pursuant to the Privacy Shield Decision. Therefore, there is no distinction between the adequacy assessment to be made pursuant to the Privacy Shield Decision and the adequacy assessment which this court is asked to consider. In those circumstances, it argues that the court is bound by the adequacy decision of the Commission. In the alternative, if the court is not bound by it, then it should defer to the greater expertise and research conducted by the Commission in comparison to the analysis and research conducted by the DPC and should prefer the conclusions of the Commission to those of the DPC.

298. As discussed above, the DPC argues that the Privacy Shield Decision is a decision that there is adequate protection afforded to data transferred to the United States pursuant to all of the safeguards set out in the Privacy Shield Decision. In essence, these are threefold: the protections based upon the privacy shield principles (which are essentially private law remedies), the provisions of US law and the Privacy Shield Ombudsperson mechanism. As I have already held, the Privacy Shield Decision is not an adequacy decision binding upon the DPC and the court. However, it is difficult to see how the privacy shield principles (as opposed to the provisions of the laws of the United States and the Ombudsperson mechanism) could be relevant to the issues raised in Mr. Schrems complaint (leaving aside the fact that the data is not transferred pursuant to the privacy shield principles). It is fair to conclude therefore that the decision of the Commission in regard to the adequacy of the protections

afforded to EU citizens against interference by the intelligence authorities in the United States with the fundamental rights of EU citizens whose data are transferred from the Union the United States, conflicts with the case made by the DPC to this court.

Submissions of the DPC

299. The DPC submits that the Ombudsperson mechanism does not remedy the inadequacies in US law which she has identified. She says that the Ombudsperson is not independent of the executive and therefore does not constitute an independent tribunal within the meaning of Article 47. It is not established by law, it is not permanent, it does not give decisions or reasons and it does not grant compensation. It is not subject to judicial review. Each of these elements are requirements of an independent tribunal within the meaning of Article 47. Therefore, it does not alter her conclusion that the laws of the United States do not respect the essence of the right guaranteed by Article 47 of the Charter or, in the alternative, are not proportionate and strictly necessary within the meaning of Article 52 (1) of the Charter.

Discussion

300. Just as the DPC was required by the CJEU in *Schrems* to make her own independent inquiry into Mr. Schrems' complaint notwithstanding the provisions of the Safe Harbour Decision, so too this court, in fulfilling its role in the legal order of the Union and, in particular, the role referred to by the CJEU in its ruling in *Schrems* at paras. 64 and 65, must make its own assessment of the issues notwithstanding the assessment of the Commission enshrined in the Privacy Shield Decision. It is of course clear that there is no requirement that the third country provide identical protections to those provided for by EU law so long as there is an essential equivalence between the protections provided under Union law and under those in the third country. Under Union law the requirement is to "... *respect the essence of the*

fundamental right to effective judicial protection as enshrined in Article 47 of the Charter..." (*Schrems* para. 95).

301. It seems to me that there is a well-founded argument that the Ombudsperson mechanism does not respect the essence of that fundamental right. It does not afford EU citizens judicial protection. The Ombudsperson is not a judge and she is not on the face of it independent of the executive. The office arguably does not meet the *indicia* of a tribunal established the ECJ in *Denuit* [2005] ECR I-923 at para 12 that the body is established by law, is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law and whether it is independent. Critically, her decisions are not subject to judicial review. It is also arguable that the remedy is not an effective remedy as required by Article 47. If the data of an EU citizen have been illegally seized, processed or shared, while the "non compliance" may have been remedied, there is obviously no question of the person so wronged recovering damages or an injunction to prevent future wrongdoing or even a declaration to that effect, as the Ombudsperson will neither confirm nor deny that the requester has been subjected to electronic surveillance.

302. This is not to say that the response of the Ombudsperson is an unreasonable one in the context of the exigencies of national security, nor is that a matter for a national court to pronounce upon. On the contrary, there are good reasons why authorities should neither confirm nor deny whether or not an individual has been subject to surveillance. But these good reasons do not necessarily alter the assessment I have made with respect to the requirements of Article 47 of the Charter or the fact that I share what I consider to be the well-founded concerns of the DPC that the Ombudsperson mechanism does not remedy the issues with regard to individual redress in the Unites States.

Article 4 of the SCC Decisions

302. The remaining issue to be considered is whether the existence and provisions of Article 4 of the SCC decisions preserves the validity of the SCC decisions notwithstanding the laws and practices of the third country to which the data is transferred. As discussed above, Article 4 of the SCC decisions as originally drafted was replaced on the 16th December, 2016. It is the effect and implications of this text which is relevant to this judgment.

303. It was argued by a number of parties that the solution to the concerns raised by the DPC regarding the regime in the United States and in particular as concerns the issues of redress lay in her own hands: she could suspend or prohibit transfers of data by Facebook to Facebook Inc. pursuant to Article 4 of the SCC decisions if she believed that this was necessary in order to protect individuals with regard to the processing of their personal data. Even if, on the facts of this case, it was not appropriate to suspend data transfers to the United States, nonetheless the existence of Article 4 saved the SCC decisions from invalidity.

304. In order to examine this argument, it is necessary to consider the scope of the SCC decisions. Article 1 provides that the standard contractual clauses set out in the annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26 (2) of the Directive. Article 2 sets out the scope of the decision and Article 3 sets out relevant definitions. Article 4 now provides: -

> *"Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive 95/46/EC leading to the suspension or definitive ban of data flows to third countries in order to protect*

individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.'

Articles 5 to 8 of the decision provide that there is to be a review of the decision after three years, the commencement date, the repeal of earlier decisions, transitional arrangements and the fact that the decision is addressed to the Member States.

305. Article 4 is directed towards ensuring that the Member States notify the Commission and the Commission in turn notifies other Member States of the exercise by a competent authority of their existing powers pursuant to Article 28 (3) to suspend or ban transfers of data to third countries in order to protect individuals with regard to the processing of their data. It does not *confer* a power on a supervisory authority. In effect, the previous version of Article 4 has been removed from the SCC decisions. If Article 4 had simply been repealed, the supervisory authorities would nonetheless still retain their powers pursuant to Article 28 (3) of the Directive. Article 4 no longer operates as a saver provision in the SCC decisions analogous to the comparable provision in the Safe Harbour decision (Article 3) which was declared invalid by the CJEU in *Schrems*. The provisions of Article 4.1 (a) as originally drafted were specifically directed towards the legal regime in force in third countries. This is no longer the case. The supervisory authorities, in this case the DPC, enjoy the powers set out in Article 28 (3) of the Directive, no more and no less, when considering the protection of individuals with regard to the processing of their data.

306. Article 28 (3) sets out the powers to be conferred on supervisory authorities by the Member States in order that they may carry out their functions and obligations under the Directive in the light of the Treaties and the Charter. They are investigative powers, effective powers of intervention and powers to engage in legal proceedings.

Examples of effective powers of intervention include imposing a temporary or definitive ban on processing. This is a general power of supervisory authorities applicable to any and all processing operations within the EU. It also applies to processing comprising of transfers to third countries but it is by no means specific or limited to the latter situation. The power is not primarily conferred with a view to suspending data transfers to a third country pursuant to the SCCs where the supervisory authority contends that this is necessary in order to protect individuals with regard to the processing of their data, though undoubtedly the power extends to that situation. Neither is the power expressly related to complaints by individuals or associations, which are governed by Article 28 (4) of the Directive.

307. Given that it is a general power applicable to all processing governed by the Directive, it is useful to see if there are any indicators as to how the power should be exercised in the context of the SCC decisions. Recital 11 of Commission Decision 2010/87/EU provides:-

> *"Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In* ***exceptional cases*** *where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses* ***in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the***

warranties and obligations providing adequate protection for the data subject." (emphasis added).

308. Recital 11 shows that the power to prohibit or suspend a data transfer or a set of transfers based on standard contractual clauses should apply in exceptional cases. It applies where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations of the data exporter, the data importer and any sub-processor which are intended to provide adequate protection for the data subject. There can be any number of bases upon which this could be so and the legal regime of the third country is only one possible example of this exceptional case. The fact that it is described as an exceptional case would indicate that particular rather than systemic circumstances prevailing are envisaged.

309. Secondly, in *Com* [2013] 846 Final, the Communication from the Commission to the European Parliament and Council concerning the Safe Harbour Decision, the Commission noted at p. 7:-

> *"The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies. German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.* ***The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core***

mechanism for the transfer of personal data between the EU and the US." (emphasis added).

315. The Commission's concern that different data protection authorities were intending to take different decisions in relation to data transfers pursuant to the Safe Harbour Decision applies equally to any decision taken by either a data protection authority or a member state individually to suspend or prohibit transfers of data pursuant to the SCCs to the United States. The reason is clear. The perceived difficulty in permitting continued transfers of data to the United States pursuant to the SCCs decision is general and systemic rather than particular to the individual contractual arrangements concerning Facebook and Facebook Inc. and/or its sub-processers. The scope for what the Commission described as differences in coverage applies equally in this case. It is undesirable that identical data transfers could be permitted under the SCCs in one Member State but suspended or banned in another depending on whether or not the particular national authorities had investigated the issues surrounding the transfer of data to the United States or not, or had reached different conclusions regarding the likelihood of the data being subjected to a substantial adverse effect on the warranties and obligations provided by the SCCs or whether such a ban or suspension of data flows is required in order to protect individuals with regard to the processing of their personal data.

316. Thirdly, the power of the data protection authorities to suspend or ban the transfer of data to third countries is a discretionary power. Both the Directive and the CJEU in *Schrems* emphasised that the authorities shall act with complete independence in exercising the functions entrusted to them. If the SCC decisions are valid because the DPC has the *power* to suspend the transfers of data to the United States where this is necessary to protect the personal data of EU citizens, this can only be on the basis

that the DPC is *obliged* to suspend the transfer of data in circumstances where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject. In other words, if the argument is correct, she is obliged to make the order, and this in turn means that she does not have a discretion to refrain from acting.

317. Further, once the precondition to the exercise of the power is established, the likely substantial adverse effect on the warranties and obligation, she must then make an order suspending or banning the transfer of data. She cannot consider, for example, whether it is desirable that a common position across the EU should be established or weigh competing interests in the balance or take account of the wider implications of such an act before taking such an extremely significant step as to prohibit all transfers of data by Facebook to Facebook Inc. Such a construction is inconsistent with her independence in relation to her functions. It also seems to be inconsistent with the judgment of the CJEU in *Schrems* para 42 where the court said that the national supervisory authorities must ensure a fair balance between the observance of the fundamental right to privacy on the one hand and the interests requiring the free movement of personal data on the other hand.[6] But if the power is in fact discretionary, with the implication that she may refrain in certain circumstances from exercising it, notwithstanding the perceived inadequacies in the legal regime in the third country to which the data is transferred, then she may validly decide not to make an order suspending or banning the transfer of data to a third country. It therefore follows that the mere fact that the power to suspend data transfers exists does not save the SCC decisions from invalidity based upon the perceived inadequacies of the law of the third country.

---

[6] See also Case C-518/07 *European Commission v Federal Republic of Germany* (judgment of the CJEU delivered on the 9th March, 2010)

318. It seems to me that as the power is and remains discretionary, the validity of the SCC decisions cannot depend on the automatic exercise of a discretionary power. She is entitled to take the view that the suspension of data transfers is not appropriate in any given circumstances, even if the threat to the data privacy of EU data subjects is established. In this case, she has decided that this is so as the problem which she has identified is systemic and general rather than particular and related to the specific contracts in question. She has adopted an alternative means of dealing with the issue by bringing these proceedings and seeking to have her concerns considered by a national court and if necessary referred to the CJEU for a decision on the validity of the SCC decisions insofar as they apply to transfers of data to the United States.

319. It seems to me that not only is this a legitimate conclusion for her to reach but it is one that is clearly hers to make as an independent supervisory authority. It is reasonable to ask whether it is legitimate to use the power granted to a data protection authority pursuant to Article 28(3) of the Directive to resolve major international structural issues of the kind identified in these proceedings.

320. It is also to be borne in mind that she can only make orders pursuant to the provisions of national legislation. Section 11, subs. 7 and 8 of the Data Protection Acts states that the DPC may prohibit the transfer of personal data from the State to a place outside the State but that in determining whether to prohibit a transfer of personal data under s. 11 she must also consider whether the transfer "*would be likely to cause damage or distress to any person and [to] have regard to the desirability of facilitating international transfers of data.*"

321. It seems to me that there is certainly an issue to be resolved as to whether the fact that the DPC has power pursuant to Article 28(3) of the Directive to suspend or ban the transfer of data by Facebook to Facebook Inc. necessarily saves the SCC

decisions from invalidity. There is also an argument to be made as to whether, in the circumstances of this case, the DPC was obliged to exercise that power or whether, in the alternative, she was entitled to proceed as she did and to seek a ruling from the CJEU on the validity of the SCC decisions. For these reasons, I do not accept the submissions that Article 4 is the answer to all of the issues raised by the DPC and that accordingly a reference to the CJEU is neither appropriate nor necessary.

Mr. Schrems' Objections to a Reference

322. Mr. Schrems' objections to the reference sought by the DPC in these proceedings are different to those raised by Facebook and some of the *amici curiae*. Firstly, he says that he did not raise any objection to the validity of the SCC decisions whether in his reformulated complaint or otherwise. He says his primary complaint was that the relevant clauses in the agreement relied upon by Facebook to transfer data to Facebook Inc. did not conform to or comply with the provisions of the SCC decisions and that therefore Facebook could not rely on the decisions and was not entitled to the derogation from Article 25 of the Directive provided for by Article 26.

323. He said the DPC wholly failed to examine, investigate or determine his primary complaint and instead she accepted Facebook's contention that the agreement was in compliance with the SCC decisions. He submits that in the absence of such a determination by the DPC the proceedings are premature, misconceived, unnecessary and are based entirely on a hypothesis developed and maintained by the DPC that there is a challenge to the validity of the SCC decisions.

324. He also argued that even if it were the case that the SCC decisions applied, Mr. Schrems did not question the validity of the SCC decisions as Article 4 (1) permits the prohibition or suspension of data transfer where the law to which the data importer (Facebook Inc.) is subject does not provide adequate safeguards. On this basis, the

SCC decisions provide for circumstances where the third country's laws are inadequate and thus they do not interfere or conflict with the rights of individuals to privacy and data protection as ensured by and enshrined in Articles 7 and 8 of the Charter.

325. He submitted that on the facts established by the DPC the US does not provide adequate safeguards as required by EU law and therefore data transfers to the US between Facebook and Facebook Inc. ought to be suspended or prohibited, as he sought in his reformulated complaint.

326. He submitted that Article 267 of TFEU requires that a reference only be made when a question is properly raised and the answer to that question is necessary to enable the court to give judgment. He says that para. 65 of the judgment of CJEU in *Schrems* does not confer a free standing right on the DPC to make a reference to the CJEU. It clarifies that a reference must be necessary by reference to the underlying claim.

327. He also stated that the making of a reference is premature as the DPC has expressly stated that her investigations have not concluded and that her decision is in draft form only and explicitly subject to further submissions. It is only once the investigation is completed that it will be possible to determine whether Facebook in fact transfers data to Facebook Inc. pursuant to SCCs as it asserts and to determine whether there are other bases upon which Facebook transfers data to Facebook Inc. which may or may not be justified whether under the provisions of Article 25 or 26 of the Directive.

Response of the DPC

328. The DPC submitted that, as an independent authority, it was a matter for her how she conducts her investigations into Mr. Schrems' reformulated complaint. Facebook has acknowledged that it transfers data in large part pursuant to the SCC

decisions and particularly that of 2010. It has exhibited the agreement of November 2016 between Facebook and Facebook Inc. which governs the transfers. She is the statutory decision maker and the independent authority under the Directive and once a complaint is made to her it is a matter for her to determine the order and the manner in which she proceeds to decide upon the issues raised. She has reached the conclusion that she cannot now progress her investigation further in the absence of the ruling which she seeks in these proceedings. This is a matter within her jurisdiction and one in which the court ought not to interfere by, for example, as submitted by Mr. Schrems, directing that she complete her investigations into whether or not the terms of the agreement of November 2016 accord with the provisions of the SCC decisions or whether there are other legal bases upon which Facebook relies when transferring data for processing to Facebook Inc.

329. The DPC submitted that she believes Mr. Schrems is incorrect in his belief that Article 4 of the SCC decisions secures the validity of the decisions for the reasons discussed above. As Mr. Schrems' alternative position is that if he is wrong about Article 4, then he does challenge the validity of the SCC decisions, it follows that it is not correct to say that the issue does not arise from his reformulated complaint. She submits that she did not raise this issue based upon her own hypothesis, as was submitted by Mr. Schrems, but that it arises from point 2 of his reformulated complaint page 11 which states: -

> *"Even if the current and all previous agreements between "Facebook Ireland Ltd" and "Facebook Inc." would not suffer from the countless formal insufficiencies above and would be binding for the DPC (which it is not), "Facebook Ireland Ltd" could still not rely on them in the given situation of factual "mass surveillance" and applicable US laws that violate Art. 7, 8 and*

47 of the [Charter] (as the CJEU has held) and the Irish Constitution (as the Irish High Court has held)."

330. Finally, even if it were the case that Mr. Schrems did not, in terms, in his reformulated complaint challenge the validity of the SCC decisions, the DPC is entitled to determine what is the key question raised by the reformulated complaint. It is to be noted that in the proceedings as they originally unfolded, neither party challenged the validity of the Safe Harbour Decision, but the High Court (with whom the CJEU agreed) took the view that the proceedings involved a challenge to the validity of the Safe Harbour Decision. Therefore, even if Mr. Schrems did not in fact challenge the validity of the SCC decisions, this does not mean that reference to the CJEU is not necessary for the resolution of the proceedings and Mr. Schrems' reformulated complaint.

Discussion

331. It is clear from the decisions of the High Court and CJEU in *Schrems* that it is both legitimate and appropriate for both the DPC and the court to identify the true controversy raised by the complaint and the point which requires to be determined in order properly to conclude the investigation into Mr Schrems' complaint. I accept that the central issue for resolution is the validity of the SCC decisions and this can only be resolved by a decision of the CJEU. I believe that there is a strong argument that Article 4 of the SCC decisions does not provide the answer to the concerns raised by the DPC in relation to the remedial regime in the United States. That being so, Mr Schrems' reformulated complaint does raise the validity of the SCC decisions and therefore it is legitimate for the DPC to seek a reference to the CJEU to resolve this issue in order that she may complete her investigation in accordance with law.

332. This court lacks jurisdiction to pronounce upon the validity of the SCC decisions. The DPC says that she needs to know whether or not they are valid, given her concerns that they are not valid for the reasons set out in this judgment. There are two options open to the court: it can make the reference sought by the DPC to the CJEU or it can refuse to make the reference and dismiss the proceedings as no other relief is sought. In that event the court in effect will be endorsing the validity of the decisions and require the DPC to conclude her investigation into Mr Schrems' complaint on the basis that the SCC decisions are valid.

333. I have formed the view that I concur with the DPC that there are well founded grounds for believing that the SCC decisions are invalid and furthermore that it is extremely important that there be uniformity in the application of the Directive throughout the Union on this vitally important issue. This requires that there be consistency and clarity. On that basis, I believe that a reference is necessary and appropriate. It follows that the balance of the arguments raised by Mr Schrems against making a reference must be rejected. For these reasons and the reasons advanced by the DPC I do not accept that I should refuse to make a reference to the CJEU as requested by the DPC.

Conclusion

334. The court has jurisdiction to make a reference to the CJEU for a preliminary ruling on the validity of the SCC decisions under Article 267 of TFEU. The court may do so if it finds that the DPC has raised well-founded concerns as to the validity of the decisions of the Commission and the court shares those concerns. Union law and the Charter are engaged. The court is not obliged to reject the application based upon the Privacy Shield Decision. It is certainly arguable that neither the DPC nor the court is required to conduct a comprehensive adequacy analysis of the laws and practices of the

United states in relation to electronic surveillance on the grounds of national security, oversight systemic protections and individual remedies in order that they may reach a conclusion that the protection of the data privacy of EU citizens whose data is transferred to the United States for processing does not enjoy the high level of protection which it is guaranteed under Union law. It is arguably legitimate to analyse the remedial regime of a third country to whom the data is transferred for processing in isolation and on the basis of the evidence in relation to individual rights of redress for EU citizens whose data is wrongfully interfered with to concluded that there is a failure to satisfy the essence of the right guaranteed under Article 47 of the Charter as required by Article 52 (1) of the Charter. In the alternative, it is arguable that the limitations on the exercise of the right to an effective remedy before an independent tribunal, as required by Article 47, for EU citizens whose data privacy rights are infringed by the intelligence agencies are not proportionate or necessary or needed to protect the rights and freedoms of others. Neither the introduction of the Privacy Shield Ombudsperson mechanism nor the provisions of Article 4 of the SCC decisions eliminate the well-founded concerns raised by the DPC in relation to the adequacy of the protection afforded to EU data subjects whose personal date is wrongfully interfered with by the intelligence services of the United States once their personal data has been transferred for processing to the United States.

335. I therefore propose to refer the issue of the validity of the SCC decisions to the CJEU for a preliminary ruling. As every party to the proceedings indicated that if I decided to refer issues to the CJEU that they would like the opportunity to be heard as to the questions to be sent to the court, I will list the matter for submissions and then determine the exact questions I shall refer to the court for a preliminary ruling.