THE HIGH COURT

COMMERCIAL

Case No. 2016/4809P

THE DATA PROTECTION COMMISSIONER PLAINTIFF

and

FACEBOOK IRELAND LTD.
AND DEFENDANTS
MAXIMILLIAN SCHREMS

HEARING HEARD BEFORE BY MS. JUSTICE COSTELLO
ON THURSDAY, 16th FEBRUARY 2017 - DAY 6

6

Gwen Malone Stenography Services certify the following to be a verbatim transcript of their stenographic notes in the above-named action.

_____

_____

GWEN MALONE STENOGRAPHY SERVICES

APPEARANCES

For the PLAINTIFF:	MR. MICHAEL COLLINS SC MR. BRIAN MURRAY SC MS. C. DONNELLY BL
Instructed by:	MR. DAMIEN YOUNG PHILIP LEE SOLICITORS 7/8 WILTON TERRACE DUBLIN 2
For the 1ST DEFENDANT:	MR. PAUL GALLAGHER SC MS. NIAMH HYLAND SC MR. FRANCIS KIERAN BL
Instructed by:	MASON HAYES & CURRAN SOUTH BANK HOUSE BARROW STREET DUBLIN 4
FOR THE 2ND DEFENDANT:	MR. EOIN McCULLOUGH SC MR. JAMES DOHERTY SC MR. SEAN O'SULLIVAN BL
Instructed by:	AHERN RUDDEN QUIGLEY 5 CLARE STREET DUBLIN 2
FOR UNITED STATES OF AMERICA:	MS. EILEEN BARRINGTON SC MS. SUZANNE KINGSTON BL
Instructed by:	McCANN FITZGERALD RIVERSIDE ONE 37-42 SIR JOHN ROGERSON'S QUAY DUBLIN 2
FOR BSA The Software Alliance:	MR. MAURICE COLLINS SC MS. KELLEY SMITH BL
Instructed by:	WILLIAM FRY SOLICITORS 2 GRAND CANAL SQUARE DUBLIN 2

FOR DIGITAL EUROPE:	**MR. MICHAEL CUSH SC** **MS. NESSA CAHILL BL**
Instructed by:	**A&L GOODBODY** **28 NORTH WALL QUAY** **NORTH WALL** **DUBLIN 1**
FOR ELECTRONIC PRIVACY INFORMATION CENTER:	**MR. COLM O'DWYER SC** **MS. GRAINNE GILMORE BL**
Instructed by:	**McGRATH McGRANE** **SUITE 323** **THE CAPEL BUILDING** **MARY'S ABBEY** **DUBLIN 7**

INDEX

THE HEARING RESUMED AS FOLLOWS ON THURSDAY, 16TH FEBRUARY 2017

MS. JUSTICE COSTELLO: Good morning.

REGISTRAR: In the matter of Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 11:04

MR. MURRAY: Judge, I was just dealing with the last of the reports which is Mr. Richards' report, you'll find it in Tab 6, and I had concluded at paragraph 79.

11:04

Judge, what I propose to do is, when I have finished opening this report, which I don't think will take terribly long, I will then try to gather together the various points that Mr. Collins made last week and that are reflected in our submissions to set out, in the light of the evidence that you have just seen, the essential structure of the case that we make having regard to the authorities. 11:04

So, Judge, at paragraph 80 he moves to address the specific issue of standing doctrine in the privacy cases and he explains that standing doctrine: 11:05

"*Frequently implicates cases that bring claims in which the legal wrongs sought to be remedied is new or involves a remedy for intangible harm, particularly where the harm alleges departs from traditional common law notions of physical or pecuniary harm. It is thus no surprise that earlier leading privacy cases drew* 11:05

heavily for environmental law in cases raising theories of environmental or aesthetic harm with complex causation, he gives examples of those, while newer ones seem to increasingly involve privacy law, with their emphasis on psychological or dignitary injuries. 11:05

81. In the lower court across the field of privacy law, litigation of 'privacy harm' is an important issue and numerous privacy claims have been dismissed for wanting of standing. As Professor McGeveran puts it 11:06
well discussing class action litigation against private companies 'developments in privacy law, particularly standing doctrine, have also increased the obstacles to private suits, including class actions'. To be sure, he says, standing doctrine is not a complete obstacle. 11:06
McGeveran notes that 'privacy class action suits will remain a significant legal threat to companies for the foreseeable future', but standing doctrine remains a real obstacle to privacy litigation by plaintiffs across the board in the United States, whether they are 11:06
suing companies or the government."

I would obviously emphasise that description, *"a real obstacle to privacy litigation"*.

11:06

And then he moves to consider two Supreme Court cases, the first you've heard many times, the **Clapper -v- Amnesty International** case, but I will just open his summary of it, Judge, at paragraph 82:

"Lawyers, journalists, and human rights activists who spoke frequently with non-US clients and contacts about sensitive topics brought a challenge to Section 702 of FISA. The plaintiffs argued that section 702 harmed them by violating their First and Fourth Amendment rights. The plaintiffs argued that because their communications were with people that the government considered suspicious, they reasonably believed that those communications were being monitored. They also claimed that in order to protect their privacy and other fundamental rights, they had spent substantial amounts of both time and money, including traveling out of the United States to speak with their clients rather than using telephones or emails that the government was likely monitoring. Nevertheless, a majority of the Supreme Court dismissed their claim on standing grounds under the first prong of the analysis for failure to allege a constitutionally-sufficient injury in fact. After explaining the 'cases and controversies' requirement that is rooted in the separation of powers, and noting that 'we have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs', the Court explained the governing test: 'To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling. Although imminence is concededly a

somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes - that the injury is certainly impending. Thus, we have repeatedly reiterated that threatened injury must be certainly impending to constitute 'injury in fact', and that [a]llegations of possible future injury are not sufficient."

And then Mr. Richards says at paragraph 83: 11:08

"*83. Applying this test, the Court concluded that the plaintiffs had not alleged a constitutionally-sufficient injury because it was speculative about whether the government would 'imminently target' their communications under section 702, they had no actual knowledge of the government's targeting practices, and that even if their being targeted was imminent, they could not prove that the targeting was being authorized by Section 702 (which they were challenging), rather than another of the various methods of government surveillance (which they were not). The Court also rejected the plaintiffs' alternative argument that they had incurred costs to avoid surveillance on the ground that they could not 'manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending. Any ongoing injuries that respondents are suffering are not fairly*

traceable to section 702'. Because their injuries were thus neither 'imminent' nor 'fairly traceable' to section 702, they lacked an injury in fact that could be redressed by a favourable ruling and thus standing to challenge the government's surveillance programme." 11:09

Judge, I mean you did at the end of yesterday fairly allude to the, I suppose, complexity of the legal matters that are before you, but, if I can respectfully say so, what this issue presents is a question, the component parts of which can be very simply identified and their application to this court readily or to this case readily expressed. 11:09

The plaintiffs in **Clapper** had a reasonable well founded apprehension that their communications were amenable or likely to be accessed under the régime that they were challenging. The United States Supreme Court held that that was not sufficient, that apprehension was not sufficient to generate standing. Just if one stops there. 11:10 11:10

That's the law of the United States, obviously, pending another decision of the United States Supreme Court it remains the law. So there is no dispute about that. 11:10

And bear in mind that the Plaintiffs in this case were, as explained by Ms. Gorski in her evidence on Friday, a range of persons who might reasonably themselves

believe that they were liable to have their communications surveyed because of the nature of their contacts abroad with journalists, NGOs and so forth. So that's the law in the United States.

11:11

In our respectful submission that formulation of standing does not provide an effective judicial remedy. We say it doesn't provide an effective judicial remedy for the purposes of the Article 47 of the Charter and indeed, I might say in passing, there would appear to be a substantial body of opinion that it doesn't provide an effective judicial remedy in United States law. But, insofar as you are concerned, the issue is: Is that an effective remedy for the purposes of Article 47 of the Charter?

11:11

Now it may be or it may not be, but what is absolutely clear in our respectful submission is that the argument that it is *not* an effective remedy, it cannot be described as ill-founded, it is a well founded argument which in its own terms is sufficient in our respectful submission to generate the type of doubt referred to by the Court of Justice in paragraph 66 of **Schrems**.

11:11

And when you look at the commentaries, they'll be dealt with, I'm sure, in greater detail by the various experts when they are being cross-examined, when you look at the commentaries in United States law addressing concerns expressed within the United States

11:12

itself in relation to the chilling effect of these doctrines on litigation of this kind, I would venture to suggest that the proposition that an argument that Article 47's requirements are not met, that that argument is so ill-founded as to not give rise to the basis for a reference, which is necessarily the argument, although it won't be expressed in those terms I'm sure that Mr. Gallagher has to advance, that argument is an untenable argument. 11:12

As I said at the end of the day it may be right or it may be wrong but it is certainly a substantial issue that presents itself. And when we look, as I will ask you to do later this morning again, at how the Court of Justice has defined 'harm' such as to give rise to an entitlement to a judicial remedy, such as to give rise to an entitlement in certain circumstances to compensation, how the Court of Justice has defined harm, the matter in our respectful submission clearly - the requirements fixed by Article 47 clearly are not met when a litigant is faced with this type of test. 11:13 11:13

And that of course is, stands on its own, but of course it is exacerbated by the fact that there is no obligation to notify that's generally applicable in US law. There are certain circumstances in which there may be such obligations, but as a matter of practice the undisputed evidence, and she wasn't challenged on this on Friday, Ms. Gorski, is that, certainly insofar 11:13

as FISA is concerned, most people who are surveyed who are the subject of the surveillance never know that fact.

Again we will see how that, combined with the very stringent test of standing applicable in this type of litigation which **Clapper** directs itself, in our respectful submission renders the remedies in the United States ineffective insofar as Article 47 is concerned. The implication of that obviously is a matter of dispute which I'll come back to later. 11:14 11:14

Mr. Richards continues:

"*84. One of the great ironies about **Clapper** is that much of the speculation about the government's targeting practices could have been resolved if the government had disclosed (including confidentially to the Court) whether the plaintiffs' communications were being monitored, and what targeting or minimization procedures were being used. This suggestion was actually made to the Court at oral argument, but the Court rejected it in its opinion on what were apparently national security grounds. The Court explained that it is not the Government's burden to disprove standing by revealing details of its surveillance priorities. Moreover, this type of hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is*

currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program. Even if the terrorist's attorney were to comply with a protective order prohibiting him from sharing the Government's disclosures with his client, the court's post-disclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets.

11:15

85. The second recent Supreme Court decision to discuss standing doctrine in the privacy context is one decided this past summer, ***Spokeo -v- Robins****.* ***Spokeo*** *involved a claim made by a consumer that a data broker had violated the Fair Credit Reporting Act of 1970, a federal consumer protection statute that imposes a data protection regime on consumer reporting agencies. The plaintiff consumer alleged that the data broker had reported false information about him, but the data broker had countered that because the false information was favourable to the consumer, there was no injury and thus no standing to sue. The Supreme Court held for the data broker on standing grounds - specifically under the rationale that the consumer had failed to allege an injury in fact that was both 'concrete' and 'particularized'. The Court explained that '[f]or an injury to be 'particularized', it must affect the plaintiff in a personal and individual way. Particularization is necessary to establish injury in*

fact, but it is not sufficient. An injury in fact must also be concrete. A 'concrete' injury must be 'de facto'; that is, it must actually exist. When we have used the adjective 'concrete', we have meant to convey the usual meaning of the term 'real', and not 'abstract'. Concreteness, therefore, is quite different from particularisation'.

*86. The Court in **Spokeo** went on to explain what it meant by the concept of 'concreteness'. In somewhat confusing language, it explained that 'concrete' is not, however, necessarily synonymous with 'tangible'. Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete. In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles. Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. In addition, because Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important. Thus, we said in **Lujan** that Congress may*

'elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law'. Similarly, Justice Kennedy's concurrence in that case explained that 'Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed'."

Just to stop there. That observation, perhaps of some significance, there's nothing, based on that, to prevent the United States' legislature or the federal legislature from creating cases or controversies within the framework identified by Mr. Justice Kennedy. But then the court said at paragraph 87: 11:18

"*Applying these two*" -- sorry, then Mr. Richards says at paragraph 87: 11:18

"*Applying these new principles to the case at hand, the Court held that to satisfy the constitutional minimum of standing, plaintiffs must have suffered concrete harm and not a 'bare procedural violation', which would be constitutionally insufficient to allow a remedy. As the Court explained, 'In the context of this particular case, these general principles tell us two things: On the one hand, Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk. On the other hand, Robins cannot satisfy the demands of*

Article III by alleging a bare procedural violation. A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm'."

And Mr. Richards continues: "***Spokeo*** *certainly made standing doctrine stricter in general especially in* 11:19
privacy cases, yet it was actually greeted with relief by some advocates and academics among the US privacy community. One of the great fears in the community was there was a substantial risk the Supreme Court might hold not only that Robins (the plaintiff) would lose, 11:20
but more broadly that standing doctrine might be interpreted to substantially limit the ability of Congress to authorise private rights of action to remedy privacy wrongs."

11:20

That's the point I just made a few minutes ago.

"*Because of this fear, several leading privacy law scholars (including myself) filed an amicus curiae*

*brief in the Supreme Court. Our brief did not take a position on Mr. Robins' narrow dispute with Spokeo, but addressed instead what we saw as the real threat to privacy law that the case presented, the risk that privacy causes of action might get limited through standing doctrine across the board in ways analogous to the way the Supreme Court recently read the Privacy Act 'actual damages' requirement so narrowly in **Cooper**. In our brief, we argued that the Federal Fair Credit Reporting Act's procedures were important to the integrity of the consumer credit system, and that more generally, the private rights of action in the FCRA and other statutes were an important part of protecting consumers and their information. I can recall teaching privacy law while the case was pending last year, and having to repeatedly tell my students that significant chunks of the course material might be rendered unconstitutional if the Court accepted all of Spokeo's arguments in that case. As a result, when the Supreme Court returned only a modest judgment for Spokeo, many privacy scholars were pleased that the Supreme Court had not gutted (figuratively speaking) US privacy law. But the case shows how close the Supreme Court could have come to placing even more substantial obstacles in the path of plaintiffs seeking redress for nonpecuniary privacy harms under American law. And the fact that even a further, modest tightening of standing rules for privacy plaintiffs was considered something of a victory shows how substantial an obstacle standing*

really is to plaintiffs under US law.

89. Perhaps because it did not originate in the national security context, I note that the other expert reports in this case have not really addressed ***Spokeo****. (I believe that neither the Swire nor Vladeck reports even cite the case, for example). However, because standing doctrine applies to every lawsuit brought before a federal court, the Court's tightening of standing doctrine in* ***Spokeo*** *to make the concreteness requirement stricter and to forbid Congress authorizing 'bare procedural violations' through private rights of action represents a higher obstacle for US privacy plaintiffs in general, whether they seek redress against companies, the government or both."* 11:22

He then asks at paragraph 90: "*Where do these developments in standing law leave privacy litigation in the United States? As explained previously the classic definition of injury in fact under American* 11:22 *standing doctrine is that an injury must be both (1) 'concrete and particularized' as well as (2) 'actual and imminent, not conjectural and hypothetical'. The two most recent Supreme Court privacy standing cases make each of these requirements more difficult for* 11:22 *claimants to satisfy. In* ***Clapper****, the Court tightened up the 'actual and imminent' prong in a surveillance case in which there may have been an injury to fundamental civil liberties, but the government was not*

*required to tell, while in **Spokeo**, the Court tightened up the 'concrete and particularized' prong in a data protection case involving the processing of personal data, which rejected 'procedural violations' as being adequate to support a remedy in the absence of demonstrable injury. As noted, **Spokeo** also seems to reject Congress's ability to authorize private rights of action that remedy a 'bare procedural violation' of privacy or data protection standards. From this perspective, the DPC's conclusion that standing doctrine represents a general obstacle to data protection claims brought by EU citizens seems eminently correct."*

And he then refers to the draft opinion where he continues: *"As I understand it the **Schrems 1** court seems to allow a substantially lower threshold for a remediable injury than US standing doctrine does."* 11:23

He then refers to the DPC draft opinion at 30 quoting Schrems at 87. And 87, I'll come back to it later, the court in **Schrems** said that to establish interference with the right it didn't matter if the person had suffered any adverse consequence. 11:23

He proceeds then, Judge, at paragraph 91: 11:23

*"91. The V1adeck Report acknowledges that the **Clapper** decision is substantively unsatisfying, but it suggests*

that the DPC Draft opinion 'errs' in concluding that 'US law thereby requires a claimant to demonstrate that a harm has in fact been suffered as a result of the interference alleged'."

And he quotes that: "*I do not think agree with this critique. In my opinion the DPC draft opinion correctly states this basic principle of standing law - that the Constitution requires each federal court plaintiff to demonstrate that an injury in fact (harm) has been suffered that was caused by the defendant and which can be redressed by a favourable decision of the court. Moreover, in the case of a privacy violation, the* ***Spokeo*** *decision makes clear that not all regulatory 'harms' will satisfy the constitutional minimum.* ***Spokeo*** *requires that injuries must be concrete, which in that case meant more than a 'bare procedural violation'.*

92. The Vladeck Report also cites a number of lower court cases subsequent to ***Spokeo*** *to suggest that '[g]iven how much more is publicly known today about U.S. government surveillance authorities - especially Section 702 of FISA - it seems far more likely that an EU citizen could demonstrate a 'substantial risk' that his communications will be unlawfully collected by the U.S. government today than it would have appeared to the Supreme Court in Clapper'. I sincerely hope that he is correct about this, but this conclusion is merely*

speculative. Those cases are in any event factually distinguishable, and of course are not binding on the Supreme Court.

*93. The Vladeck Report notes further on this point that some lower court cases have rejected challenges to standing, but concludes that 'As these cases illustrate, there is significant uncertainty in the lower courts over exactly when Clapper does and does not foreclose standing, and I do not mean to suggest otherwise. The critical point for present purposes is that this uncertainty is not nearly as categorically hostile to standing as suggested in the DPC Draft Decision, and instead is more reflective of the case-specific vagaries of individual lawsuits. Thus, based on the cases surveyed above, it is my view that, where EU citizens can marshal plausible grounds from which it is reasonable to believe that the U.S. government has collected, will collect, and/or is maintaining, records relating to them in a government database, they will likely have standing to sue even in light of the Supreme Court's **Clapper** decision."*

And that phrase there, you will recall Ms. Gorski referred to it on Friday, Judge, *"plausible grounds"*. 11:26

He then references that and he continues:

"*I would agree that there is great uncertainty on this*

point in the US Courts, but my reading of the DPC Draft Decision is slightly different. I understand the DPC to have concluded that standing law is a general obstacle to EU citizens bringing suit, and that '[o]n their terms, I consider that these requirements appear to be incompatible with EU law in circumstances where, as a matter of EU law, it is not necessary to demonstrate an adverse consequence as a result of an interference with Articles 7 and 8 of the Charter in order to secure redress of a violation of the said Articles'. In my opinion, the DPC is correct that standing is a general obstacle to all litigants, and particularly correct that American standing doctrine's injury in fact requirement always requires the demonstration of actual injury, particularly since Spokeo's strengthening of the concreteness requirement eliminates the possibility that 'bare procedural violations' can produce the requisite level of constitutional injury.

11:27

*94. On the subject of lower-court cases, the Gorski report notes the ACLU's litigation representing a group of human rights and educational groups (including Wikimedia, which runs the Wikipedia online encyclopedia) challenging Section 702 'Upstream' surveillance, and how that case was dismissed in district court under the Supreme Court decision in **Clapper**. I should note that I joined a brief with other First Amendment Law Professors seeking to have*

the dismissal overturned on appeal. I agree with Ms. Gorski both in the hope that this ruling will be reversed on appeal, and that (in her words) 'the district court's opinion illustrates the difficulties that plaintiffs face in establishing standing, even at the outset of a case, when a plaintiff's allegations must merely be plausible'. I would amplify this point by noting that if these difficulties are substantial for one of the world's most popular websites represented by the most famous civil liberties group in the world, they would likely be even more pronounced for ordinary EU citizens.

95. The Vladeck Report also takes issue with the Serwin Memorandum's discussion of Rule 11. As the Vladeck Report explains, Rule 11 is a requirement in all civil litigation before federal courts requiring essentially that litigants filing motions before the court are not engaged in frivolous or vexatious litigation. I do not see a material difference between the Vladeck Report and the Serwin Memorandum on this point. The DPC Draft Decision does conclude with the statement that '[t]aken with the analysis adopted by the Court in Clapper in connection with the making of 'speculative' claims regarding alleged violations of data privacy rights, the Federal Rules of Procedure would appear to preclude the bringing of precisely the kind of complaint now before me'. Professor Vladeck is correct that Rule 11 does not preclude claims, but

*rather authorizes sanctions on the abuse of process. Insofar as the statement in the DPC's Draft Decision might be interpreted in isolation as suggesting that Rule 11 would preclude bringing a speculative claim identical to the one rejected in **Clapper**, such an interpretation of US law would not be correct. However, I do not believe that this is the best way to read the DPC Draft Decision's interpretation of US law. On the contrary, when one reads paragraph 56 of the Draft Opinion in connection with the preceding 55, the DPC's conclusion seems to be different and correct as a matter of US law. Under this reading, substantive standing doctrine can operate to bar speculative claims alleging unlawful surveillance. On balance, I think that this latter reading is a more faithful reading of the DPC Draft Decision. Moreover, I could envision that a claim that is more 'speculative' than **Clapper** could not only be barred by the developments in the recent privacy law standing cases, but could also run the risk of Rule 11 sanctions as well. In any event, even if this statement by the DPC could fairly be said to be erroneous, it would be at most a misreading of Serwin that I do not see as undermining the DPC's overall US law argument.*

11:29

The Swire report - he continues at paragraph 96 - also considers the issue of standing. Professor Swire agrees with the DPC's conclusion to the extent that standing is a generally-applicable requirement for all

*litigants in federal court, but notes that **Clapper** 'should not, however, be read to create a per se ban on cases involving US foreign intelligence or counterterrorism programs' citing lower court cases that have found litigants with standing to challenge other surveillance programmes."*

Citing **ACLU -v- Clapper**.

Finding, he says, that: "*Standing existed to challenge section 215 metadata programme where the bulk collection necessarily included plaintiffs' phone records.*" 11:30

Then he refers to **Klayman -v- Obama** and **Shearson -v- Holder** which he observes: "*Holding that individual had standing to challenge her suspected placement on the terrorist watch list, even though the court found 'it is impossible for [her] to prove that her name remains on that list', but where she had proven indicia of being on the watch list. It is both correct and encouraging that lower Courts after **Clapper** have allowed civil liberties challenges to surveillance to go forward. However, as I understand both the Swire Report and the DPC Draft Opinion, there is no disagreement that standing is an obstacle to relief, particularly where there is no injury in fact. Under EU law as I understand it, particularly as the CJEU interpreted Article 47 in **Schrems I**, a stringent* 11:30

*requirement of injury in fact akin to that required by the US Supreme Court in **Clapper** and **Spokeo** is not always required. This could represent a bar to a significant chunk of such claims by EU citizens that US law would leave unredressed. This barrier seems higher, as the **Clapper** court noted, in national security cases. And it also would now have to satisfy the more stringent 'concreteness' requirement for injuries in fact after **Spokeo**. Thus, while standing doctrine is not a complete bar to relief in surveillance cases, it is still frequently a substantial and frequently unsatisfying one. I agree here with scholarly work by Professor Vladeck in which he has argued that."*

11:31

And the way he describes this I think is important, Judge: "*Perhaps the most important takeaway from **Clapper** is the extent to which the Supreme Court's Article III standing jurisprudence interposes substantial obstacles to judicial review of secret surveillance programmes (if not all secret government conduct) on the merits.*"

11:31

And that Prof. Vladeck's comment and description, substantial obstacle to judicial review of secret surveillance programmes in an article that he has published.

11:32

"*Moreover, this is also how I read (and concur with)*

the DPC Draft Decision's findings on US law - that standing doctrine is a general obstacle to relief of this sort that, while not necessarily fatal, is nevertheless substantial and jurisdictional. In conclusion regarding the potential remedies, it is my opinion that EU citizens seeking legal relief to remedy violations of their data protection and privacy rights in the US face substantial obstacles at the specific level of causes of action, and at the general levels of standing doctrine and the practical difficulties in learning about surveillance in the first place. The other four experts on US law who have filed reports in these Proceedings also take positions on this question. The Swire Report is quite optimistic about the availability of remedies in US legal proceedings. It argues that the 'fragmentation' of US remedies is not a vice but rather a virtue, and explains that there is a lot of substance to US privacy law, contrary to the belief of some foreign observers. The Swire report offers five categories of remedies for privacy violations under US law - (1) judicial remedies against the government, (2) non-judicial remedies available against US government surveillance, (3) individual remedies against US companies, (4) privacy enforcement and (5) standing. 11:33

99. I agree with the Swire Report that the US does have real privacy law, and that there is a lot of it. However, the fact that US privacy law is substantial is

not directly responsive, in my opinion, to the questions I have been asked to address in this report, such as the availability of judicial remedies to EU citizens who wish to challenge unlawful data processing by the US government once their data has been transferred to the US. From the perspective of that question, of the five categories of law described in the Swire Report, only part of category (1) and category (5) are relevant, as they are the only ones that bear on legal redress against the United States government for surveillance that violates EU fundamental rights. With respect to category (2), non-judicial remedies are by definition non-judicial. Category (3) remedies against companies are not remedies against the government. And privacy enforcement under US state law, though it has been overlooked by many until recently, does not provide redress against the national government. As for category (5), I have already explained at length above why I believe that standing doctrine is a substantial obstacle, and I will not repeat that discussion here.

100. This leaves category (1), which are 'US Civil Judicial Remedies'. In this category, the Swire Report includes some other remedies, such as those under the 'Umbrella Agreement', the Privacy Shield Ombudsperson mechanism, standard contractual clauses, and Privacy Shield alternative dispute resolution. I respectfully disagree that these are judicial remedies, though I

address the potential and limitations of the Ombudsperson mechanism in Part III, below. With respect to Privacy Shield alternative dispute resolution, which is separate from the Ombudsperson mechanism, I do not see how a civil arbitration scheme between a company and its customers could provide relief for government privacy violations. Finally, Litigation under the standard contractual clauses is a judicial remedy, but I also do not see how it could provide relief for government privacy violations. 11:34

101. The Swire Report also discusses under category (1) 'US Criminal Judicial Remedies' brought by the US Department of Justice against people (including government officials) who violate ECPA, FISA, and the Privacy Act. These criminal prosecutions could not of course be brought by EU citizens, and although they could certainly punish people who have violated federal privacy law, to my mind this is not the same as the redress of a violation of a fundamental right. The Swire Report does discuss under category (1) the Privacy Act/Judicial Redress Act, the Electronic Communications Privacy Act, and FISA. I have already discussed these causes of action and some of their specific limitations above. 11:35

102. In contrast to the Swire Report, the Gorski and Butler Reports are more pessimistic as to remedies. The Butler Report explains that 'EU citizens whose

personal data has been transferred to the U.S. have limited remedies available where their claims arise from access to, use of, or dissemination of their private communications or other personal data. None of these statutory remedies provide a means of redress for bulk surveillance'. The Gorski report goes further, concluding that 'U.. Surveillance law is extremely permissive, as the government claims broad authority to acquire the communications and data of non-U.S. persons located abroad. For the vast majority of individuals subject to Section 702 and EO 12333 surveillance, there has to date been no viable avenue to obtain meaningful redress for the rights violations resulting from this surveillance'. Indeed, earlier in her report, Ms. Gorski explains that due to the obstacles facing litigants, 'no civil lawsuit challenging Section 702 or EO 12333 surveillance has ever produced a U.S. court decision addressing the lawfulness of that surveillance'.

11:36

103. In between these positions is the Vladeck Report, which concedes some of the objections raised by the DPC Draft Report, as well as some of those raised by the Gorski Report, the Butler Report, and the Serwin Memorandum - many of which I have already discussed in this Report. At two points in his report, Professor Vladeck notes that relief is problematic, but then argues that it is not as problematic as the other opinions on this question (with the exception of Prof.

Swire) conclude. At paragraph 98 of his Report, he states that 'although there <u>are</u> shortcomings in the existing U.S. legal regime with regard to redress of unlawful government data collection, I do not believe that they are nearly as comprehensive - or that standing is as categorical an obstacle - as the DPC Draft Decision or the [Serwin] Memo suggest'. At paragraph 103 of his Report, he concludes that in his opinion the DPC Draft Decision's assessment of current U.S. remedies for unlawful collection of EU citizens' data from U.S. companies is significantly incomplete, that its analysis of the obstacles posed by 'standing' doctrine is substantially overstated.

104. It is my expert opinion that the DPC Draft Decision does not significantly overstate the specific or general difficulties faced by EU citizens seeking relief for violations of their EU fundamental privacy and data protection rights in US courts. For the reasons given in this report, I thus respectfully disagree with Professors Swire and Vladeck on this point, and agree with the ultimate conclusions to the contrary on this point reached by the Serwin Memorandum, the Gorski Report, the Butler Report, and the DPC Draft Decision." 11:37

He then proceeds, Judge, in the final section to address the Privacy Shield framework. He says at paragraph 105:

"The Privacy Shield framework is a recently-negotiated agreement designed to replace the Safe Harbour Agreement invalidated by the CJEU in ***Schrems****. After negotiations between the government of the US, the European Commission, and other interested parties, the European Commission issued a decision on 12 July 2016 providing a derogation for adequate processing of personal data pursuant to Article 25 for US companies that satisfy the 'Privacy Shield' requirements and follow its rules. Commission Implementing Decision of 12 July 2016, pursuant to Directive 95/46.*

"Under the Privacy Shield framework" - he says on the next paragraph: *"Framework, as under the predecessor Safe Harbour Agreement, US companies can self-certify online to the Department of Commerce and publicly commit to adhere to and comply with the Framework's requirements.*

107. The Privacy Shield Principles, like the predecessor Safe Harbour principles, are derived from Fair Information Practice Principles (FIPPs) common throughout international privacy law.

108. The Recourse, Enforcement and Liability Principle requires organizations under the Privacy Shield Framework to provide recourse (including an effective remedy) to the individuals whose data they hold under the framework ***in*** *cases of non-compliance with the other*

principles. The Commission Implementing Decision envisions seven different possible sources of recourse for such individuals.

First, they can pursue cases of noncompliance directly with the company that is self-certified to the Privacy Shield Framework. Second, they can bring a complaint to a company designated 'independent dispute resolution body'. Third, they can bring their complaint to their national Data Protection Authority. Fourth, they can bring complaints to the US Department of Commerce. Fifth, companies that self-certify to the Privacy Shield Framework must also be subject to the Federal Trade Commission's investigatory and enforcement powers, including the ability to obtain consent decrees in cases of alleged unfair and deceptive trade practices. Sixth, there is the availability of binding arbitration by a 'Privacy Shield Panel' of arbitrators constituted under the Framework. Seventh, there is always the possibility of individuals bringing legal claims under US state law.

Based upon the seven possible avenues of redress against Privacy Shield self-certifying companies, the European Commission found in its implementing decision that 'that the Principles issued by the U.S. Department of Commerce as such ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the substantive

*basic principles laid down in the Directive'. Nevertheless, because the adequacy of Safe Harbor was invalidated in **Schrems** on the basis of access to EU personal data held in the US by the US government, the Commission considered the state of US surveillance law in light of the reforms that have been implemented in the wake of the Snowden revelations. In negotiations with the US government, the Commission received detailed submissions from the US government about its collection programmes and limitations. It also received a commitment by the US government to create a new 'Privacy Shield Ombudsperson', to be housed in the Department of State.*

111. The role of the Ombudsperson is set out in a letter ('the Kerry Letter') from the US Secretary of State to the European Commission, which was considered by the Commission in its adequacy determinations for the Privacy Shield. In the letter, Secretary of State John Kerry designated Under Secretary of State Catherine Novelli, the Under Secretary of States for Economic Growth, Energy, and the Environment, to serve as the Ombudsperson. He also stated that 'Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me'. The Kerry Letter sets out the Ombudsperson's mechanism in a six-page Memorandum, which was attached to the Letter as Annex A. This memorandum described the Ombudsperson's role as follows:

1. The Privacy Shield Ombudsperson. The Senior Coordinator will serve as the Privacy Shield Ombudsperson and designate additional State Department officials, as appropriate to assist in her performance of the responsibilities detailed in this memorandum. The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.

2. Effective Coordination. The Privacy Shield Ombudsperson will be able to effectively use and coordinate with the oversight bodies, described below, in order to ensure that the Ombudsperson's response to requests from the submitting EU individual complaint handling body is based on the necessary information. When the request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers.

A. The Privacy Shield Ombudsperson will work closely with other United States Government officials,

including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies. In particular, the Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers.

B. The United States Government will rely on mechanisms for coordinating and overseeing national security matters across departments and agencies to help ensure that the Privacy Shield Ombudsperson is able to respond within the meaning of Section 4(e) to completed requests.

C. The Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

The Kerry Letter also provides a mechanism by which EU citizens can submit requests to the Ombudsperson via their National Data Protection Authorities, and through the DPAs to an 'EU Individual Complaint Handling Body' that will verify and standardize requests to the Ombudsperson. Notably, in a departure from the

standing requirements that apply to private litigants in US federal courts, the Kerry Letter provides that 'To be completed for purposes of further handling by the Privacy Shield Ombudsperson under this memorandum, the request need not demonstrate that the requester's data has in fact been accessed by the United States Government through signal intelligence activities'. The Kerry Letter also provides a procedure for the Ombudsperson's investigation. The Ombudsperson is required to acknowledge receipt of the request to the 'EU Individual Complaint Handling Body', and conduct an initial review to ensure completeness of the request and see if more information is needed from the 'EU Individual Complaint Handling Body', including having it contact the complaining individual.

The Kerry Letter then provides three additional requirements: Once a request has been completed as described in Section 3 of this Memorandum, 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 policies. The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives [sic] orders, presidential directives, and agency policies, providing

the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of noncompliance, such noncompliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed as provided under that statute and applicable regulations.

F. The Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of one of the underlying processes described below, then those communications will take place in accordance with existing procedures.

G. Commitments in this Memorandum will not apply to general claims that the EU-U.S. Privacy Shield is inconsistent with European Union data protection requirements. The commitments in this Memorandum are made based on the common understanding by the European Commission and the U.S. government that given the scope of commitments under this mechanism, there may be resource constraints that arise, including with respect to Freedom of Information Act (FOIA) requests. Should the carrying-out of the Privacy Shield Ombudsperson's

functions exceed reasonable resource constraints and impede the fulfillment of these commitments, the U.S. government will discuss with the European Commission any adjustments that may be appropriate to address the situation'.

116. Finally, the Privacy Shield Ombudsperson procedures outlined in the Kerry Letter provide that 'A request alleging violation of law or other misconduct will be referred to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance'. This envisions the involvement of two kinds of oversight officials: (1) 'Inspectors General'. US agency officials whose job it is to conduct internal investigations, audits, and review, and also to recommend 'corrective action' and (2) Privacy and Civil Liberties officers and oversight boards.

Based upon its review of the procedures and commitments outlined in the Kerry Letter, the European Commission determined that 'the US 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'. It also determined that the objection of the CJEU in ***Schrems I*** *regarding effective remedies under Article 47 of the*

European Charter. It determined that this objection had been satisfied, based upon a combination of both the current remedies available under US law to EU citizens and the new Ombudsperson mechanism, which it deemed to provide 'for independent oversight with investigatory powers'.

118. The European Commission proceeded from these determinations to conclude that the Privacy Shield provided an adequate level of legal protection under Article 25.

*119. I have been asked to consider 'The nature and extent of the remedy (or remedies) that an EU citizen may access in the US in the particular context at hand in the light of the adoption of the Privacy Shield mechanism'. Before I do this, I must make three initial caveats. First, while the privacy principles and redress mechanisms against private companies seem stronger under Privacy Shield than under Safe Harbour, I offer no firm opinion on this point because it seems largely irrelevant to the question that produced the judgment in **Schrems I**, law enforcement and intelligence services access to EU personal data transferred to the US.*

Second, consistent with my instructions in this case and my own expertise in US rather than EU privacy law, I offer no determination about the correctness or not

of the European Commission's determination of Privacy Shield's legal adequacy under the Directive. Third, since the Ombudsperson mechanism is new and the Privacy Shield Framework is still being built up, it is difficult to draw any firm conclusions about how useful the mechanism will be in practice. Any analysis at this stage by anyone with knowledge of the mechanism will be speculative by its very nature.

120. In my opinion, the Privacy Shield Ombudsperson mechanism offers a potential opportunity for relief for EU citizens who are concerned that their data protection rights are not being observed through the Privacy Shield enabled transfers of their data to the US. The mechanism offers an opportunity to have a government official investigate claims, and that official seems to have access to a number of internal investigators and civil liberties lawyers and professionals within the US government intelligence bureaucracies. By providing that a complaint can be investigated without the complainant proving that their data has been accessed by the US government, the mechanism potentially side-steps the obstacle of 'injury in fact' that makes a litigation remedy in federal court so difficult to achieve for many privacy plaintiffs. The Ombudsperson is also, by reporting to the Secretary of State, nominally independent from the US intelligence apparatus. I note that both the Gorski Report and the Robertson Report disagree with this

assertion on the grounds that the Department of State is entangled in the US intelligence community.

121. Nevertheless, there are several features about the Ombudsperson mechanism that strike me as very different from a judicial remedy. First, the Ombudsperson is not a disinterested judge, but a political appointee who appears to serve at the pleasure of another very senior political appointee, the US Secretary of State. Second, even in cases in which the Ombudsperson's investigation discovers a violation, she has no formal power to order it to be fixed. Third, even when a violation is discovered and fixed internally, the Ombudsperson cannot tell the EU citizen complainant whether or not they were a target of unlawful surveillance or what if any problems were fixed. Fourth, the Ombudsperson does not tell an EU citizen complainant anything, as her role is insulated from the complainant by two levels of DPA bureaucracy at the European and national levels. And fifth, any response given to the 'EU Individual Complaint Handling Body' appears to be qualified both by being an 'appropriate response' and by remaining 'subject to the continuing obligation to protect information under applicable laws and policies'. These would seem to be bureaucratic refuges that could be used to do very little.

122. The Swire Report expresses optimism that the

Privacy Ombudsperson mechanism envisioned by the Privacy Shield Framework could represent an alternative form of relief to EU citizens. The Swire Report makes reference to the Ombudsperson mechanism in Chapter 7, but I do not see anything in this report that causes me to decide that the Ombudsperson mechanism solves the difficulties faced by EU citizens who might desire a legal remedy for privacy violations.

123. In connection with this debate about the effectiveness of Ombuds mechanisms, I note that the Robertson Report."

I'm going to pass from that, Judge, as you know, Judge, there is an issue around the admissibility of that report. 11:50

Paragraph 124: "*In sum, while I believe that the Privacy Ombudsperson mechanism has the potential to be a useful reform, it looks to me far more like a complaint resolution scheme than something approaching a judicial remedy, at least as that notion is understood within the US system with which I am expert. This is not to denigrate the mechanism, which I see as both a reform and an improvement, but the Privacy Shield, in my mind, does not substantially change the legal remedies available to EU citizens, at least not in the way that legal remedies are typically understood in the United States. I note that the Gorski report is*

substantially in agreement with that interpretation.

125. In sum, it is my opinion that there is not only substantial evidence to support the conclusions of the DPC Draft Decision and the Serwin Memorandum that EU citizens lack meaningful avenues of legal relief to remedy violations of their data protection and privacy rights in the US, but that I believe these conclusions are correct interpretations of the state of US law at present. US privacy remedies are indeed fragmentary and suffer from individual deficiencies, as well as having to surmount the general obstacle of standing doctrine, which appears to be becoming more stringent, especially in privacy cases. In addition, having reviewed the Privacy Shield framework, particularly the new Privacy Ombudsperson mechanism, I do not find that this program provides a legal remedy that changes my conclusion."

So, Judge, what I'm going to do now, and I hope I can do it relatively briefly, is try to gather together some of the comments that were made by Mr. Collins last week while he was opening the material and to relate them to the evidence that you have seen in the legal authorities. You are aware that we have delivered written legal submissions, as of course have all of the parties, and I'm going to refer to aspects of those. 11:51 11:51

But I am, Judge, going to ask you in the first

instance - sorry, Judge, I seem to have mislaid my note - I'm going to ask you in the first instance to look at the **Schrems** case. Again I know this was opened to you by Mr. Collins and you'll find it.

MS. JUSTICE COSTELLO: Which book is it in again? 11:52

MR. MURRAY: Yes, it's in Book 3.

MS. JUSTICE COSTELLO: Now is this of the trial books or the authorities?

MR. MURRAY: Book 3 of the agreed authorities.

MS. JUSTICE COSTELLO: Thank you. 11:52

MR. MURRAY: And you'll find it at Tab 36A.

MS. JUSTICE COSTELLO: Yes, thank you.

MR. MURRAY: Just a number of aspects of this which I would like to relate back to what you now see in the material before the court. 11:53

If I can ask you first to turn to paragraph 63, page 20, and here we come back to just, I have mentioned this a number of times so I'll pass from it, I hope, briefly, but here we come back to how it is you, Judge, 11:53 are hearing this application and what is the standard that you are to bring to bear on the request by the Commissioner for a reference. At paragraph 63 the court said this, he said:

11:53

"63. Where a person whose personal data has been or could be transferred to a third country which has been the subject of Commission decision pursuant to Article 25(6) lodges with the national supervisory authority a

claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing that claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental 11:54
rights and freedoms of individuals, it is incumbent on the national supervisory authority - that's the Commission of course - to examine the claim with all due diligence.

11:54

64. In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded - that it's not invalid - and therefore rejects it, the person who lodged the claim must, as is apparent from 11:54
the second subparagraph Article 28(3) of the Directive, read in the light of Article 47, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in 11:54
paragraphs 61 and 62 of the present of the present judgment, those courts must stay proceedings and make a reference to the Court of Justice for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, 11:55
as the case may be, raised by them of their own motion are well founded."

So if the national supervisory authority rejects the

claim of invalidity, you have an entitlement to go for a judicial remedy in accordance with Article 47. And the court then, if it decides that the grounds for invalidity are well founded, the Commissioner having founded that they are not, then it must proceed to make a reference. And it can do that of its own motion, and I'll come back to that in a moment. 11:55

"In the converse situation", at paragraph 65: "*Where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded - which is the situation here - that authority must, in accordance with the third indent in the first subparagraph of Article 28(3), be able to engage in legal proceedings. It is incumbent on the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, make a reference.*" 11:55 11:56

Now it seems to us, you could read that perhaps one of two ways. I can submit the correct way is that it reflects a deference to the view of the national supervisory authority. If it has come to or formed the opinion that the objection is well founded, then the 11:56

court, if it shares that doubt, then proceeds to refer. And slightly different language is used, the court itself must be satisfied that the complaint is well founded where the national supervisory authority has rejected it. It may be a distinction without a difference. 11:57

In this case in our respectful submission, whether you look for a doubt or seek to have the complaint identified or ascertained that it is well founded, that burden is met. 11:57

Just to, I suppose, re-emphasise some points that we make in our written submission. The manner in which those paragraphs are framed of course reflects the role of the Court of Justice in determining and being best positioned to rule on the validity of Union acts. The court should not apply an unduly stringent test before deciding whether the court should be called upon to determine an issue of validity where a matter comes before it in the way envisaged in those paragraphs. 11:57

Secondly, the plaintiff is the national supervisory authority, given the functions that she has under the legislation and indeed in European law, in our respectful submission the court should afford some deference to the view that she has formulated. 11:58

And, thirdly, in making your decision as to whether the

evidence discloses a basis for a reference having regard to the applicable legal principles, you should in our respectful submission have regard to the overriding objective of the Directive, which of course is to ensure a high level of protection for privacy rights with respect to the processing of personal data. And you should exercise that power bearing in mind and guided by the principles of effectiveness and the obligation to ensure sufficient remedies to give effect to those legal rights. 11:58 11:59

And just while on that, there is a point that's made by Mr. Schrems where he suggests that he hasn't actually made a complaint that the SCCs are invalid. I think Mr. Collins referred to this in our submission when the court looks to the complaint that was in fact made by him. We find it difficult to see how he can say that he wasn't attacking the validity of the SCCs in substance if not in form. In fact in his own submissions to this court, paragraph 9, he accepts that one of his complaints was that Facebook could not rely on the SCCs due to the inadequacy of protections afforded to him under US surveillance law. So he himself prayed in aid the underlying or the objection that underlies the Commissioner's concern. 11:59 11:59 12:00

But whether he did or didn't in our respectful submission is neither here nor there. The Commissioner must have the power of her own motion, as the court

acknowledges the court has the power of its own motion, that if she feels, in the course of determining the complaint, that this issue has presented itself as to the validity of the SCCs and that she has a well-founded concern as to their validity she must have the entitlement to proceed to court, as she has done here, whether or not a complaint in those terms was made. And I don't believe there is anything in the judgment that would displace that entitlement, Judge. 12:00

MS. JUSTICE COSTELLO: Well you are not saying she could do it for a moot? 12:00

MR. MURRAY: No, absolutely not. But clearly in circumstances where Mr. Schrems himself, as I said he acknowledges in paragraph 9, was complaining or one of the complaints he made was that Facebook couldn't rely on the SCCs due to the inadequacy of protections afforded under US surveillance law, given that that was part, as it were, of the matrix that the Commissioner had to deal with, then it certainly was not a moot. 12:00

12:01

So the, I suppose, first point of relevance of the decision is insofar as it defines and identifies the nature of the court's jurisdiction and what it is the court, as it were, is going to have to determine in deciding whether to make a reference. 12:01

The second point, if I could ask you to go forward to paragraph 73, where, dealing with the word "adequate" in Article 25(6), the court said the following:

"*The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection* identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of *Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.*"

Judge, this is an important paragraph. Obviously it confirms that the third country - in this case, obviously, the United States - doesn't have to have protections that are identical, but the manner in which the court frames what it is the third country must have is significant. First of all, the test is of essential equivalence. But secondly, what it has to be

12:03

equivalent to is *not* the individual protections that particular Member States have in fact implemented in their domestic laws. The standard is *not* defined by looking through the laws of Poland or France or the UK and saying 'Well, aha, the US law actually provides *more* protection'. It is something quite different, and deliberately so. What it is is essentially equivalent to that guaranteed within the European Union, but by virtue of the Directive, viewed -- sorry, read in the light of the Charter. 12:04

This is the standard that is defined by the Charter as interpreted by the court. And it is for that reason that what you, Judge, are concerned with is the proper meaning of Article 47, in this case as interpreted by the court, not with what individual Member States may or may not or should or should not have done in their own laws. 12:05

And it is for that reason that we say that a large amount of the evidence - and this is a central part of the Facebook case, that no, we really should be looking at the laws of the individual states and because we can show that the laws of the individual states are in some respect different or do not have the same level of protection, as some of the evidence suggests, as the US, well therefore, there is and can be no difficulty with the SCCs. 12:05

And in that regard, Judge, we just think it's perhaps important to observe this: The fact of the matter is that for this reason, the laws of the Member States do, in some respects, lag behind the law as defined by the Court of Justice as the law evolves. This all began when a Directive addressing data retention, which was implemented, given effect to in all of the Member States and then in the **Digital Rights** case the Court of Justice declared the Directive to be invalid, resulting in a situation where many Member States had implemented laws which corresponded with the Directive which was now invalid. 12:06 12:06

You'll see a dramatic example of that in **Watson**, the decision of the Court of Justice of 21st December, where many, I don't know if all, but certainly many Member States had mandatory data retention laws as a result of the Directive - which had been struck down in **Digital Rights** - and they were indiscriminate retention laws, effectively requiring telecommunications companies and internet service providers to maintain data for an identified period of time, irrespective. And many states had such laws. But in **Watson**, the Court of Justice declared those laws to be inconsistent with the Charter because they were indiscriminate and didn't distinguish between, or were not -- retention didn't occur based on targeting, as it were. 12:06 12:07 12:07

So the focus, as it were, under that paragraph,

paragraph 73, is clearly, and deliberately so, that of the Charter. And perhaps suggests that it would be very strange were the position otherwise, because it is the interpretation of the Charter by the court, not the practice of Member States in how they go about implementing their obligations or their perception of it that is critical to the ultimate protection of the rights in question. 12:08

MS. JUSTICE COSTELLO: When you say "by the court", do you mean a national court or the CJEU? 12:08

MR. MURRAY: No, I mean the Court of Justice. Now, if you continue, Judge, just to go through paragraph 74:

"*It is clear*", the court continues, "*from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the* [legal order]."

And that latter part of that sentence defines part of your inquiry; do the US laws prove in practice effective to ensure protection that is essentially equivalent to that guaranteed within the Union? And here we are, as I've said, concerned specifically with Article 47. 12:09

"*75. Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2)... take account of all the circumstances surrounding a transfer of personal data to a third country.*"

If you then turn, Judge, to paragraph 84, the difficulties which presented themselves with safe harbour, with which the court was obviously concerned, were considered, or at least some of them were addressed: 12:10

"*In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create*

conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests...

85. In this connection, Decision 2000/520 states... with regard to the limits to which the safe harbour principles' applicability is subject, that, '[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'.

86. Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them."

They then say this:

"*In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest*

requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference."

And refers then to the **Digital Rights** case. And that paragraph, I think, is referred to in a number of the reports in the context of the definitions under EU law for the purposes of the Charter of when there is an interference with rights. And I think Mr. Collins alluded to this; **Digital Rights**, of course, was a case that came on a reference from the High Court here and McKechnie J. made the reference. And there, Digital Rights' standing to challenge the data regime operated at the time the case was initiated and subsequently changed was based on the fact that it was the owner of a mobile telephone. The State challenged that as a basis for locus standi and McKechnie J. held that no, that indeed was sufficient in the context of the type of alleged interferences which were being complained of, that was sufficient to justify, or to grant locus standi.

12:11

12:12

12:12

Now, if you move forward then, Judge, to paragraph 95, the critical function of remedies is addressed by the court. And what it says at the bottom of page 24, paragraph 95, is this:

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

Again that very short statement of principle disposes of another aspect on which Facebook has adduced a very large volume of evidence, which is the plethora of *non-judicial* remedies upon which it relies by way of context. I think Prof. Swire appears to have believed himself or been instructed to prepare a record effectively for the Court of Justice, in the event that this case goes there, and his report addresses the

12:14

remedies afforded by Congressional Oversight Committees, by the free press, by the availability of a plethora of non-governmental organisations and so forth. But while interesting, in our respectful submission, none of that is in fact germane to the specific question presented by the Commissioner's concerns here and as referred to in this paragraph of the ruling, which are directed exclusively to judicial remedies. 12:15

MS. JUSTICE COSTELLO: So you're saying "tribunal" must mean a court of some sense? 12:15

MR. MURRAY: Of some sense. And I will come back in relation to that to just address you briefly on the legal authorities regarding what that means. But certainly we are talking about *judicial review*, not necessarily a court as the Constitution of *this* jurisdiction might prescribe it, but certainly judicial review, not a Congressional Oversight Committee. 12:15

But it also, Judge, brings into focus again the point arising from the earlier paragraphs I've opened to you - the essence of the fundamental right to effective judicial protection. Because certainly as one reads this, the court is envisaging that the right to judicial protection arising from Article 47 has an essence and that essence cannot be derogated from and in particular the essence is not respected by legislation that doesn't provide for any possibility for an individual to pursue legal remedies in order to 12:15 12:16

have access to personal data related to him or to obtain rectification of the data. And that obviously is where the operation and effect of US standing laws comes into play - obviously there are judicial remedies and they are addressed at some length in the various reports.

But the question which concerns the Commissioner and the critical issue presented by the reference is whether the consequence of the restriction on those various remedies, which I'll come back to shortly, is in effect to mean that for EU residency, EU citizens whose data is exported to the United States, where it is liable to be accessed in accordance with the legal regime that you've seen described, whether those persons have, or have been deprived of, a possibility to pursue legal remedies to have access to the various reliefs that are envisaged and, we say, required by European law.

12:17

Some of those themes are repeated in the **Watson** case that I referred to, which is perhaps useful simply because it is such a recent restatement of the law. And I've explained to you a few moments ago how this arose; it was a challenge to the retention regimes in two jurisdictions, the UK and Sweden - there were two references made. And I just want to draw your attention to one paragraph in the Advocate General's ruling --

12:18

MS. JUSTICE COSTELLO: Sorry, where do I find this decision?

MR. MURRAY: I'm terribly sorry, Judge, it's the next tab, tab 37(a). Sorry, it's not actually the next tab, it's tab 37(a) 12:18

MS. JUSTICE COSTELLO: Thank you.

MR. MURRAY: If you turn to paragraph 132.

MS. JUSTICE COSTELLO: Now, the first one, is that the Advocate General?

MR. MURRAY: That is the Advocate General's. 12:18

MS. JUSTICE COSTELLO: And 132?

MR. MURRAY: Yes, Judge.

MS. JUSTICE COSTELLO: Yes?

MR. MURRAY: I just want to draw your attention to this paragraph, because it does summarise 12:19 the method of analysis which the court uses. In paragraph 132 it says:

"*Together, these two provisions*" - and it's referring to particular provisions in the directives in question 12:19 - "*establish six requirements that must be satisfied in order for the interference caused by a general data retention obligation to be justified:*

- the retention obligation must have a legal basis;

- it must observe the essence of the rights enshrined in the Charter;

- it must pursue an objective of general interest;

- it must be appropriate...;

- it must be necessary...;

- it must be proportionate..."

And unsurprisingly and indeed as in Irish constitutional law, what that envisages is that of course you can have limitations and restrictions on fundamental rights where those limitations and restrictions are justified by a legitimate object of protecting the rights of others or public order or whatever, that restriction must be proportionate in, bear a reasonable relationship to and go no further than necessary to obtain that objective. But - *but* - there is an essence of the right which *cannot* be impaired. And that again reflects the analysis in domestic constitutional law; the circumstances in which people are precluded outright, for example, from ever bringing a case in court are, if nothing, exceptional. 12:19 12:20 12:20

So that essence is part of the focus of the Commissioner's application to the extent that, going back to the comments that I've just opened to you in **Digital Rights**, she contends that you are concerned with whether there is, in the United States, a protection of the essence of the Article 47 right - and the various limitations in the remedies which she has identified, in our submission, suggest not - but that actually, issues of national security or other exigencies of the public interest - the general agreement on tariffs and trade or economic considerations - are really not relevant insofar as the 12:21 12:21

court will be looking at this very narrow issue of whether the essence of the right has been impaired.

So that it may well be the Court of Justice believes the various and very considerable evidence that has been adduced as to justifications for constraints on judicial remedy are well placed or justify negating the right, but certainly it's not apparent to us, on the basis of the law, that that is so. And for that reason, the Commissioner has not engaged in that debate. 12:22 12:22

Can I ask you then to move to --

MS. JUSTICE COSTELLO: So you're saying I'm not concerned with the justification -- 12:22

MR. MURRAY: Precisely.

MS. JUSTICE COSTELLO: -- for the laws in the United States, I'm only concerned with the effect of the laws?

MR. MURRAY: If it is the case, if it *be* the case that under United States law EU citizens whose data is exported to the United States have no effective legal remedy as envisaged by Article 47 in respect of that interference with their data privacy rights, if they have *no* effective remedy, then in our respectful submission, those various issues of justification, the, to use a very general term, public interest considerations which Facebook say and their experts say would justify never telling you that your data has been accessed, not having delayed notification, having a 12:22 12:23

standing requirement which presents the significant obstacles that it does, having a rule whereby the Fourth Amendment and its freestanding claim for damages relief is not available to EU citizens, having a rule whereby the NSA or the CIA are exempted from obligations imposed under the Privacy Act or the Judicial -- sorry, more accurately, the Judicial Redress Act, having those rules, if it is the case that alone or in combination they mean that EU citizens do not have an effective remedy as envisaged by Article 47, then yes, in our respectful submission, the court is not concerned with those issues. 12:23 12:24

But again, what you are in fact being asked to do is to accept, based on our evidence and submission, that our concern that there is no such remedy is well founded or that there is a doubt and to ask the Court of Justice then, if it wishes to engage in this proportionality analysis, to do so. 12:24

But **Watson** again is very interesting in that regard. The decision in **Watson** went *beyond* the case that had been argued by any of the parties before the court. Because the parties before the court accepted that there could be *general* retention regimes in particular circumstances - the idea, as you'll be aware, that if the police know that all telecommunications service providers, all internet companies are mandatorily retaining their data for a year or two years, well 12:25

then, if a situation presents itself where they have to, for the purpose of a criminal investigation, track somebody, see what their movements were, they will be able to go and obtain that information.

12:25

And what the Court of Justice said was that no, retention itself is an impairment of the privacy right because - and I suppose this touches on another issue which presents itself here - because, as it were, that the possibility exists that someone can find out matters such as your movements or who you've been speaking to and that, therefore, there should only be retention of persons who the State can establish are persons of, to use the phrase, of interest or particular areas or location where a crime may be about to be committed.

12:25

12:26

If I can ask you to turn to paragraph 120 -- sorry, of the court decision, which you'll find at tab (b). The court addressed this issue of remedy. And at paragraph 120 it said this:

12:26

"*In order to ensure, in practice, that those conditions*" - and after its consideration of the various authorities on data privacy - "*are fully respected, it is essential that access of the competent national authorities to retained data*" --

12:26

So it's dealing here now, you know, on the assumption

that data is retained, when can it be accessed? And I should say that it's my understanding that in the United States, certainly I don't believe there's any federal law that has mandatory retention. So you're not concerned with retention. But here the court moves on to *access* by the relevant authorities. 12:27

"*In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.*"

Then in the next paragraph they say this: 12:27

"*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.*"

And --

MS. JUSTICE COSTELLO: So it could be two months or it could be 20 years?

MR. MURRAY: A delayed notification. But there must be a mandatory notification. Because clearly there will be circumstances in which, I don't think anyone would dispute, that contemporaneous notification could prejudice the purposes of access in the first place. 12:28

Now, can I suggest, Judge, just a number of conclusions that, in our respectful submission, the court should draw from that very short consideration of the cases: First, the court should, in our respectful submission, refer if it shares the Commissioner's doubts as to the validity of the SCCs; secondly, in making the decision as to validity, the key question, in our respectful submission, is whether US law provides protections that are essentially equivalent to those provided under the Charter; thirdly, essential equivalence mandates an effective remedy within the meaning of Article 47; fourthly, in considering that question - effective remedy - the issue is the protection afforded by the Charter, not by the law of individual Member States; fifth, the concern is with a remedy that is judicial, not an extrajudicial remedy; sixth, in making that assessment, the question is whether there's been an interference with the essence of the right under

Article 47 - matters of proportionality arise only if that essence is protected; seventhly, European law mandates a remedy which arises where there has been an interference; and eight, as you've seen, it requires notification on the conditions that you've just identified, Judge.

So that is the context in which, in our respectful submission, you will now come to address the US law. And there are a number of issues that present themselves in that regard. I've already referred earlier this morning while looking at Prof. Richards' report to the question of standing. The United States Supreme Court has clearly and indisputably held that lawyers, journalists, human rights activists who speak to non-US clients about sensitive topics with people the government considered suspicious do not have standing to challenge Section 702; even though they reasonably believed their communications were being monitored, the court held there was no standing because the claim that their communications would be targeted was speculative. And in our respectful submission, that sets a bar which is beyond that which is permissible under Article 47.

12:30 12:31 12:31 12:32

Judge, if I can ask you just to take out our written submission. And the written submissions of the parties are in book 12. And if I can ask you to go please to paragraphs 85 and 86.

MS. JUSTICE COSTELLO: Sorry, you're at tab...

MR. MURRAY: It is tab three, Judge, yes.

MS. JUSTICE COSTELLO: Three. And 85 and 86?

MR. MURRAY: Yes.

MS. JUSTICE COSTELLO: Thank you, I have it. 12:32

MR. MURRAY: What we have done here, it's just perhaps easier than going back through the cases, is, in relation to standing, we explain in paragraph 85 the general position under EU law:

"*National rules of procedure must grant standing to persons who fall within the scope ratione personae of a directly effective provision of EU law... Where compliance with the principle of effective judicial protection militates in favour of giving access to the court to persons having an interest in the correct application of an EU provision, those persons must enjoy locus standi.*"

And in the particular context of data protection then, 12:33
we observe the entitlement to institute proceedings as being broad: All forms of processing may give rise to an interference, including a retention obligation, provision for the processing of data and access to data, no adverse consequences are required. And we 12:33
quote from **Schrems**:

"*To establish the existence of an interference with the fundamental right to respect for private life, it does*

not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference."

Thirdly, there's no requirement for the individual to have been inconvenienced in any way. And we reference authority in relation to that at footnote 105. And indeed, even the creation of a feeling will suffice to give rise to an interference in **Digital Rights**. 12:34

"*CJEU endorsed view of Advocate General that the fact that data retained and subsequently without subscriber or registered user being informed was likely to generate in minds of persons concerned the feeling,* 12:34 *that their private lives were the subject of constant surveillance.*"

The standing issue goes beyond the specific concern arising from the **Clapper** case, where the belief of the 12:34 plaintiffs that their communications may have been intercepted was speculative, there's the second issue arising from the decision in **Spokeo** which Prof. Richards has identified or emphasised - the holding that procedural violations don't constitute concrete 12:35 and particularised harm and the difficulty, or the particular difficulty that that presents in the context of privacy, of data protection violation claims.

I've referred already to the issue of notification; the evidence given by Ms. Gorski that most people whose data is accessed in the United States - she was referring, I should say, to FISA - have never been told of that fact. There are some provisions in US law, notably under the ECPA, which provide for notification in certain circumstances, but not all do so. And indeed the **Microsoft** case, which was the subject of a decision from the Federal District Court in Washington State on, I think, 6th or 8th February this year, was one in which it was in fact being argued by Microsoft, although they weren't ultimately permitted to make this argument, that the Fourth Amendment entailed an obligation to notify after there had been a search of or access to information in the cloud. But those remain certainly not -- sorry, the practical situation, as expressed by Ms. Gorski and indeed as referred to in her report was not challenged. 12:35 12:35 12:36

Then there's a number, Judge, of particular issues with particular remedies provided for under the Constitution or under legislation that are perhaps difficult to piece together because of the, admittedly fragmentary, nature of US privacy law. But we have gathered together some of the principal questions in our submission. If I ask you to look at paragraph 99, it might be perhaps easier just to direct you to where they're gathered together here. 12:36 12:36

So what we explain at paragraph 99 is that - this is on page 34 of our submission - the legal remedies that *are* available, we say, are not complete and, first of all, that even where a remedial scheme *is* available in principle, there may be broad exemptions. For example, 12:37
the Privacy Act's general rule of nondisclosure is subject to 12 statutory exceptions, with the routine use exemption in particular having the potential to be the proverbial exception that swallows the rule. And that was a comment made by Mr. Richards in the context 12:37
of those, I don't think it's denied, very, *very* broadly drawn exceptions in the legislation.

The Judicial Redress Act is likely to have limited impact, given that many of the records potentially at 12:38
interest in the proceedings have been exempted by administrative process from its coverage, while the protection in the legislation extends to EU citizens will depend on how the terms "covered record" and "covered country" are interpreted. 12:38

Moreover - and contrary to the criticism made of the fact that the draft decision did not consider the Administrative Procedure Act - the APA is a remedy of limited availability, it only arises in circumstances 12:38
in which there's no alternative available framework. And indeed, as I think I said yesterday and I think is correct, I don't believe it's referred to at all by even Prof. Swire. And in addition then, we observe

that the EU data subjects without substantial connections are most likely unable to bring a Fourth Amendment **Bivens** challenge. And that, as I understand it, certainly from Prof. Vladeck's report, is not disputed. 12:39

Then we deal with certain immunities. Sovereign immunity operates as an impediment at a number of levels. The FISA provides the possibility for individuals to sue US government officials for damages 12:39 where there's been unauthorised electronic surveillance or where information obtained by unauthorised electronic surveillance has been disclosed. The Ninth Circuit has held that Section 1810 does *not* operate as waiver of sovereign immunity to the effect that the US 12:39 cannot be held liable. Some US courts have held that federal government agencies and officials are immune from suit under the Computer Fraud Abuse Act. In addition, under the Wire Tap Act, there's uncertainty in the statutory language that the government entities 12:39 can be held liable for violations because the definition of "person" doesn't include governmental entities.

Then, Judge, over the page we deal with the collection 12:39 of remedies which impose what we describe as an excessively difficult burden. In paragraph 106:

"*A number of remedies are limited by reference to*

intentionality and wilfulness, rendering the remedies excessively difficult, if not practically impossible, to secure:

(1) FISA provides the possibility for individuals to bring a civil cause of action for money damages pursuant to FISA against the US when information about them has been unlawfully and wilfully used or disclosed. However, this creates substantial 'procedural disadvantages' - requiring proof not only that use or disclosure of information was unlawful, but that it was also 'wilful' in the sense that it was knowing or reckless.

(2) Similarly, the Electronic Communications Privacy Act - which, as you know, includes the Wiretap Act and the SCA - "*but the provisions of these Acts are focussed on intentional unauthorised access to electronic communications, with the Wiretap Act applying to communications that are intercepted while in transmission, and the SCA applying to the unauthorised access of stored communications.*

(3) The Judicial Redress Act also uses concepts of intention and wilfulness, with for example, a remedy being created by 552a(g)(1)(D) in respect of disclosures, but only 'with respect to disclosures intentionally or wilfully made'...

107. Case law applying the Privacy Act in the US suggests that 'pecuniary harm' - rather than dignitary harm as will more likely arise in this context - must be shown in order to for damages relief to be ordered."

And that's a reference to the **Cooper** case. Then there's a heading which we direct the proposition you will have seen in some of the Defendant's evidence that, well, there *is* a remedy if you're prosecuted, because you may be able to rely upon an illegality of a search as a basis for excluding evidence. And we just make the, I suppose, unsurprising comment there in paragraph 108 that the fact that you have those rights is not an effective remedy - a classic example that operates by requiring individuals to "*test the law by breaking it.*"

12:41

12:41

We then observe that there'll be no guarantee of access to an independent authority even after implementation of the Privacy Shield.

12:41

"... *even if Facebook is correct that Article 47 - as distinct from Article 6... does not require access to a court, it fails to recognise that access to an independent authority is a pre-requisite to the definition of a 'court or tribunal' in Union law.*"

And we refer there to a case of **Denuit**.

"*This requirement is not fulfilled by the Privacy Ombudsperson, who, as Professor Richards puts it, is 'not a disinterested person, but a political appointee who appears to serve at the pleasure of another very senior political appointee, the US Secretary of State*."

Heading eight, I deal with notification. I've mentioned that already. And then we address the question of standing, which I've outlined to you. And we urge, Judge, at heading nine, paragraph 120 on page 39 the Commissioner's provisional view as set out in the draft decision that that host of frailties is such that the law, US law, impairs the essence of Article 47 and even if the Commissioner is wrong and the essence of Article 47 remains intact, such is the extent of the encroachment on Article 47 rights, that it cannot be justified by reference to the countervailing factors. 12:42 12:42

Just on two other perhaps significant constraints, Judge, which are not listed in that summary. FISA, Section 1806(a) and 1825 -- 12:43

MS. JUSTICE COSTELLO: Just a moment. 1806, little a, isn't it?

MR. MURRAY: Yes.

MS. JUSTICE COSTELLO: And then one-eight? 12:43

MR. MURRAY: Then 1825. Provide that information acquired under FISA may only be used and disclosed in accordance with minimisation procedures. Those procedures only apply to information relating to

a US person. EU citizens are not able to bring a claim under Section 2712 -- Title 18, Section 2712, for noncompliance. Mr. Serwin will explain that when he gives evidence.

12:44

And the Judicial Redress Act does not authorise a civil action for violation of Title 5, Section 552a(d)(1)(c). In other words, you can't bring a civil action where the agency fails to adequately maintain records concerning an individual as is necessary to ensure fairness in the determination.

12:44

So there are, I suppose, reflecting the fragmented nature of the remedies, an equally fragmented, but nonetheless -- an equally fragmented set of difficulties with them, but they do come together to create, in our respectful submission, for the reasons we've identified, a significant impairment of Article 47, to the extent that the very basis of the entitlement is not effective.

12:44

12:45

So that, Judge, is the essence of the argument that we present under the heading of why it is that we claim that the inadequacies in US law are such as to generate a doubt or create a well founded concern, however you express it, of the kind envisaged by paragraphs 65 and 66 of **Schrems**. But there are a series of, I describe them as technical objections, and I don't mean by that to diminish them, but there are a series of legal

12:45

objections that are raised by the parties, but in particular to Facebook -- in particular *by* Facebook that I want to address just briefly so that the court, as it were, has a complete account of what we're saying. Many of these have been already discussed by Mr. Collins, but it's just, as it were, to gather them together. 12:45

The first issue is this - and this *was* addressed by Mr. Collins - and it relates to the relationship between Article 25 and Article 26. And if you go back to our submission at page 18, you will see the -- I'm sorry, Judge, I've given you the wrong reference. Yes, sorry, if you go back to page 11, paragraph 34, you'll see how this issue arises. Essentially, Judge, Facebook says the Commissioner erred in determining as she did that in looking at the validity of the SCCs, the first question, she said, is whether the US ensured adequate protections. And the second then is to move to look and see if the SCCs did so. And her reasoning was that you couldn't look at the second of those, the effect of the SCCs, without first considering and identifying what the inadequacy of the third country was and what the inadequacy in its legal protection was. 12:46 12:46 12:47 12:47

Facebook criticise that and what they say is that Article 26 enabling the SCCs is a derogation from Article 25 and the stipulation of adequacy that's there

and that because it's a derogation, effectively the adequacy test shouldn't have arisen at all. And if you look at paragraph 34 - Mr. Collins opened the text of the articles to you, but I will, Judge, just refer to our summary of the relevant provisions at page 11, paragraph 34: 12:48

"*(1) Article 25(1) of the Directive establishes a general rule prohibiting the transfer of personal data outside the European Economic Area unless the country to which the data is transferred 'ensures an adequate level of protection' for the data protection rights of those data subjects to whom the transferred data relates.*

(2) Article 25(2) identifies the criteria by reference to which the adequacy of the level of protection available in a third country is to be assessed.

(3) *Schrems* [identified or defined] *'adequate level of protection'*."

I've already, obviously, opened that to you. And Articles 25 and 26 then provide methods by which transfers can occur, notwithstanding an *inadequate* level of protection or *absence* of essential equivalence. The Article 25 method of facilitating transfers involves the adoption of an adequacy decision by the Commission. Meanwhile, Article 26 sets out six 12:48

specific circumstances in which data transfers to a third country may be permissible, even though the third country in question doesn't ensure an adequate level of protection. Then Article 26(2) provides that:

"*Without prejudice to Article 26(1), a Member State may authorise a transfer or a set of transfers of personal data to a third country which does* not *ensure an adequate level of protection... 'where the controller adduces adequate safeguards with respect to the protection... '.*"

Then Article 26(4) says that, in accordance with the with procedure in Article 31, the Commission may decide that certain contractual clauses offer sufficient safeguards. 12:49

Then, Judge, at paragraph 35 we outline how the Commissioner analysed these. She said:

"*(1) It is not disputed that data transfers made pursuant to Article 26 - including the SCC Decisions adopted pursuant to Article 26(4) - are made on the assumption that the third country does not provide 'an adequate level of protection'.*"

That's fully recognised in the draft decision. That does *not* mean that the question of whether the third country offers an adequate level of protection falls

away. Rather, where a data transfer is made pursuant to the SCC decisions, it's based on the premise that the SCCs provide sufficient safeguards within the meaning of Article 26(4). The safeguards provided by the SCCs must be, in turn, be such as to enable the 12:50
controller to adduce adequate safeguards within the meaning of Article 26(1). So if adequate protection *cannot* be provided by the third country, it will *have* to be supplied by the controller, including by way of adherence to the SCCs. The underlying premise is, 12:50
therefore, unequivocal; if the third country does *not* provide adequate protection, the SCC has to match -- sorry, remedy the inadequacy.

Just to stop there. And that's why, in the 12:50
Commissioner's submission, you have to begin by identifying what the inadequacy is, because it's only when you have done that that you can proceed to consider the extent to which it is addressed by the SCC -- 12:51

MS. JUSTICE COSTELLO: If there's a gap and it says 'Plug the gap'.

MR. MURRAY: Exactly. Otherwise you're looking at the SCC divorced from its actual purpose and intention. 12:51

Logically, therefore, she says at seven, there's no way of knowing whether the SCC provides sufficient safeguards to enable the controller to adduce adequate

safeguards without understanding the extent and nature of any inadequacy in the level of protection offered by the third country. In other words, it's *not* possible to ascertain whether the SCCs provide sufficient safeguards without examining the extent to which, the way in which the relevant third country fails to provide an adequate level of protection. 12:51

So the conclusion being that the adequate level of protection, which of course has been the focus of our submission and the evidence to you, remains, in our submission, central and integral to Article 26 and, accordingly, the validity of the SCCs. 12:51

So there you see the two questions the Commissioner directed herself to: Does the US ensure adequate protection? And if so -- sorry, if not, do the SCC decisions *in fact* offer adequate safeguards? 12:52

Now, we outline, Judge, over the next few pages *why* we say that's the correct interpretation. And at paragraph 40 we say that this is the purpose of Article 25 and 26 is usefully illustrated by the **Schrems** ruling: 12:52

"(1) *The CJEU observed that 'Chapter IV of the Directive, in which articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries',*

with the national supervisory authority 'vested with the power to check whether a transfer of personal data from its own member state to a third country complies with the requirements' of the Directive.

(2) Advocate General Bot noted that, 'transfers of personal data to third countries should not be given a lower level of protection than processing within the European Union'.

(3) He also noted that 'the fact that the Commission has adopted an adequacy Decision cannot have the effect of reducing the protection of citizens of the EU with regard to the processing of their data when that data is transferred to a third country by comparison with the level of protection which those persons would enjoy if their data were processed within the European Union'.

(4) For the Advocate General, it followed from this that national supervisory authorities must be in a position to intervene notwithstanding a European Commission decision, as '[w]ere that not so, citizens of the European Union would be less well protected than they would be if their data were processed within the European Union.

(5) He also observed of Article 25 that while the CJEU had previously described this provision as setting up a

'special regime', 'that does not mean... that such a regime must afford less protection'.

(6) He added that 'the point is not the creation of a special system of exceptions that offers less protection for citizens of the European Union by comparison with the general system provided for in that Directive for the processing of data within the European Union'."

So we say that the interpretation doesn't just follow from the text of the provisions and their intended effect, but is supported by those observations. At paragraph 43 and over the page, the Facebook interpretation is summarised. What they say is that, in paragraph 44, the decision *wrongly* applies the adequacy test contained in Article 25 to a measure adopted under Article 26 and repeatedly suggests Article 26 is a derogation from the general rule. So they're saying that once transfers are -- sorry, the transfers under Article 26 are *premised* on the country not providing an adequate level, therefore that simply falls away from the analysis. And we summarise there, and I've said it really already, why, in our submission, that's a mistaken proposition. 12:54 12:54 12:54

And this issue, Judge, becomes relevant for a second, related reason. The Commissioner conducts the analysis of identifying the inadequacy issue, as she perceives

it, and then comes to see, well, does the SCC remedy that - is that inadequacy addressed sufficiently in the SCC? And that presents another, what is another important aspect of the Facebook case. Because - and you will have seen in the evidence which I opened yesterday, and indeed Mr. Collins referred to this in the course of his opening - Facebook places a great deal of reliance on the safeguards within the SCCs themselves and in particular the obligations imposed on the data importer and exporter and the availability of a damages remedy against the exporter, and in default, in certain circumstances, the importer of the information in breach of the SCCs. And Facebook's case is 'Well, the SCCs themselves provide an adequate or sufficient remedy in all of those circumstances'. 12:55 12:55 12:56

Now, that was addressed and it was addressed with some brevity and, we submit, correctly so by the Commissioner. And that brevity itself is criticised by Facebook. But it's addressed by the Commissioner in her decision. If I can ask you to turn to it, it's in book one, tab 18. 12:56

MS. JUSTICE COSTELLO: That's trial book one, isn't it?

MR. MURRAY: Trial book one, yes. If you go, Judge, to page 29, at paragraph 60 she, having identified the difficulties that we have been considering with the US system, she says: 12:57

"*For all of the reasons outlined above, therefore, I*

have formed the view, subject to consideration of such submissions as may be submitted in due course by the Complainant and FB-I that, at least on the question of redress, the objections raised by the CJEU in its judgment in Schrems have not yet been answered."

So that's the inadequacy that she has identified as part, or as the first part of her analysis. And she then says:

"*It is also my view that the safeguards purportedly constituted by the standard contract clauses set out in the Annexes to the SCC Decisions do not address the CJEU's objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in Schrems.*"

Now, just perhaps to stop there, Judge. I mean, there will, of course, be inadequacies that are or that may present themselves in third countries that can be 12:58
resolved by appropriate provision in an SCC - the making available of claims and perhaps compensation is one of them - which may not be available within the State, or other deficiencies in entitlements to notification or rectification. You can perhaps 12:58
envisage circumstances in which they would occur.

But here the problem which was identified by the Commission - namely, the inadequacy defined by the US

law's failure to provide the essentials of a legal remedy under Article 47 - is not something that *could* be remedied by the SCC; it is a deficiency in the remedial system in the United States itself. And that's why the Commissioner said in the next sentence: 12:59

"... *concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in Schrems. Nor could they. On their terms, the standard contract clauses in question do no more than establish a right in contract, in favour of data subjects, to a remedy against either or both of the data exporter and importer. Importantly for current purposes, there is no question but that the SCC Decisions are not binding on any US government agency or other US public body; nor do they purport to be so binding. It follows that they make no provision whatsoever for a right in favour of data subjects to access an effective remedy in the event that their data is (or may be) the subject of interference by a US public authority, whether acting on national security grounds, or otherwise. On this basis, I have formed the view, subject to consideration of such further submissions as may be filed... that the protections purportedly provided by the standard contract clauses contained in the Annexes... are limited in their extent and in their application. So far as the question of access to an effective remedy is concerned, it is my view that they cannot be said to ensure adequate*

safeguards for the protection of the privacy and fundamental rights and freedoms of EU citizens whose data is transferred to the US".

MS. JUSTICE COSTELLO: Perhaps we'll take it up then at two o'clock. 13:00

MR. MURRAY: Certainly, Judge.

(LUNCHEON ADJOURNMENT)

13:00

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

MS. JUSTICE COSTELLO: Good afternoon.

MR. GALLAGHER: Afternoon, Judge. 14:06

REGISTRAR: Matter of Data Protection Commissioner -v- Facebook Ireland Ltd. and another.

MR. MURRAY: Judge, I was just referring to or I had finished referring to the Commissioner's Draft Decision at paragraph 61 and I think had recorded her comment 14:06 that the nature of the inadequacy which she had identified with US law was such, as she said herself, that the SCCs simply could not remedy. And that's correct, in my respectful submission it is self-evidently so, how could they? The SCCs don't bind 14:06 the US government, they don't create any cause of action against the US government, they don't resolve the difficulty as to how a Facebook customer, who doesn't know if their data has been accessed, can bring any claim against anyone for damages. They don't 14:07 resolve the difficulties arising from establishing standing in proceedings against the US government in which a EU citizen seeks to assert their data protection rights of rectification, rights of access.

14:07

So the SCCs, insofar as they confer or provide for a claim for damages for breach of contract, and that's what it is, against the data exporter in the first instance I suppose, that does not in fact address the

fundamental difficulty identified by the Commissioner, and for that reason the second stage of the analysis which she undertook does not provide an answer that allows the validity to stand, if it is the case, for them to stand as valid if it is the case that she is correct in the inadequacy that she identified. 14:07

One does wonder how the SCCs in this situation and having regard to this inadequacy can function properly at all. I mean I have referred already to the difficulty arising from the customer who doesn't know whether their information has been accessed. I would just draw your attention to the fact, I won't open it, but it's in Clause 5(d)(i). 14:08

MS. JUSTICE COSTELLO: Is that a big D or a small D. 14:08

MR. MURRAY: It's a small D because this is, not the US legislation, but the actual decision itself with the standard contractual terms. It states, unsurprisingly, that the data exporter won't be required to tell the data importer of requests for access to information if it is the case that the -- 14:08

MS. JUSTICE COSTELLO: Did you say exporter or importer.

MR. MURRAY: The data - I am terribly sorry, you are quite correct - the data importer will not be required to advise the *exporter* if the third party law prevents it from doing so. 14:09

And just to make this observation. One also wonders

what sort of damages can be claimed in this action for breach of contract. Normally, as you know, damages for distress or inconvenience, and indeed the violation of a right of the nature in issue, here would not fit within a claim for breach of contract. They wouldn't be known. The Supreme Court here decided only a couple of weeks ago you can't get damages for breach of contract for distress or inconvenience. That's a minor point, but the more fundamental one is the Commissioner's conclusion, which we say is correct, that the inadequacy which she had identified was one which simply could not be corrected, as it were, by the standard contractual clauses. 14:09 14:09

Now, there are three other issues that I want to address briefly. One -- and the first is the question of national security which, as you know, Facebook say operates in this case to oust EU law entirely and the Charter. What they say, and there's a summary of it, I won't open it, but just quote it to you. There's a summary at paragraph 5 of their submission where they say: 14:10 14:10

"*The EU Treaties expressly provide that EU law, including the Charter, does not apply to what they describe as national security activities.*" 14:10

That contention is as surprising as it is misconceived, surprising because if it's correct it means that both

the CJEU and the Advocate General in **Schrems**, and indeed the court in **Watson** but particularly the CJEU in **Schrems**, overlooked a fundamental jurisdictional issue. It's misconceived because in fact the data is not transferred for a national security objective. It's undertaken, it's transferred for commercial purposes and for that reason the national security exemption, for the want of a better term, upon which Facebook rely is simply inapplicable.

14:11

We address this, Judge, in our submission at paragraph 142, page 46. At paragraph 142 we introduce the issue and at paragraph 144 we explain that:

"*What is in issue here is the transfer of data from the EU to the US. The data is not transferred for a national security objective as the submissions of Facebook and BSA in particular seem to emphasise. The transfer is undertaken for commercial purposes.*"

14:12

And that's correct and in the undisputed evidence it is correct. The commercial transfer clearly falls within European law for the purpose of the Directive, as we say at paragraph 145, and indeed for the purposes of the Charter. It is well established, we say, that once the matter falls within the scope of Union law, even if a Member State subsequently seeks to derogate, it is bound by the fundamental rights standards.

14:13

Then if you turn over the page there are some quotations from the Advocate General and the court in **Schrems** which in our respectful submission clearly support the position adopted by the Commission in relation to jurisdiction. The Advocate General observed that:

"*There is nothing to suggest that arrangements for the transfer of personal data to third countries are excluded from the substantive scope of Article 8(3) of the Charter, which enshrines at the highest level of the hierarchy of rules in EU law the importance of control by an independent authority of compliance with the rules on the protection of personal data.*" 14:13

And then he added: "*The access enjoyed by the US intelligence services.*"

So it's not as if the Advocate General was not aware that this was a matter related to US intelligence service activity: "*The access enjoyed by the United States intelligence services to the transferred data therefore also constitutes an interference with the fundamental right to protection of personal data guaranteed in Article 8, since such access constitutes processing.*" 14:14

And the CJEU then we quote on the next paragraph:

"*The operation consisting of having the personal data transferred from a Member State to a third country constitutes in itself processing of personal data within the meaning of Articles 2(b) of the Directive.*"

14:14

We similarly say, Judge, at the following paragraph how that is supported by the position adopted by the Article 29 Working Party: "*Which has observed that the fact that the national security activities of the Member States are excluded from the scope of application of EU law does not mean that EU law ceases to apply where data subject to EU data protection law is accessed by third countries in the name of the national security.*"

14:14

14:15

And Article 29 Working Group observed that Article 4 TEU: "*Attempt to define the competences of the Union vis-à-vis the Member States. This, however, is different from the obligation to comply with EU data protection law weighing on controllers even where they are subject to national security legislation of a third country.*"

14:15

So we have addressed that issue -- sorry, just perhaps also to ask the following question: That if this is ousted from EU law in the manner alleged, it does beg the question as to how the Privacy Shield could have come into being at all. Because the same logic would appear to apply to the data, and it is almost a

14:15

collateral attack on the Privacy Shield inherent in that argument because, if it's correct, it's outside the competence of EU law entirely. But it isn't correct for that reason.

14:16

Judge, our submission deals with that issue very briefly. One could analyse the question a lot more, and we're not entirely certain to what extent this is being pressed by Facebook. But what we have done, on reviewing our own submission and perhaps thinking it could be dealt with in more detail, is that we prepared a very, well it's not a short, we prepared a speaking note which, unusual amongst speaking notes, I'm not going to speak to, but I am going to hand into the court and to Mr. Gallagher. So that, rather than spend further time on the issue, he will be aware of the arguments we're advancing in a little bit more detail so that when he or Ms. Hyland next week or whenever they get to make their full submissions, if they consider that they wish to address the Privacy Shield argument they will have our case outlined in considerable detail there and I can reply as appropriate. But the essence of it, Judge, is outlined in our original submission.

14:16

14:16

14:16

MR. GALLAGHER: This is a very surprising --

14:17

MS. JUSTICE COSTELLO: This is a nearly the length of your own original written submission.

MR. GALLAGHER: It is. And there was strict word limits to it and it is entirely unsatisfactory that day

seven of the trial that this is handed to us - day six I think, is it - that this is handed to us and I'm going to be on my feet shortly responding and setting out our case. It is entirely unsatisfactory, Judge. I can't stop Mr. Murray making whatever submission he wants in relation to the matter, but I do think this is wholly unfair. And, if I am to address it, I'm going to need a little bit longer than the court has allocated me in terms of the opening because I can't deal with this issue on the blind without knowing what the case is. The whole idea was that I would respond to the case and to get it now, now at 14:17. 14:17 14:17

MS. JUSTICE COSTELLO: Well the whole idea - there is two points there, Mr. Gallagher. The whole idea was that you were allowed to put up what your case is. 14:17

MR. GALLAGHER: Exactly.

MS. JUSTICE COSTELLO: He is putting in his defence to your case.

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: It is not quite the same thing as you responding to his case. You will, when you, if you like, get your full -- 14:18

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: -- go as opposed to your truncated go obviously be able to deal with it. Where is the difficulty in dealing with *your* position if you are unaware of what his answer to your position is? 14:18

MR. GALLAGHER: Because they have asserted a jurisdiction, I am responding and saying there is *no*

jurisdiction in respect of the matter.

MS. JUSTICE COSTELLO: Okay.

MR. GALLAGHER: So I am responding and setting out and the whole idea was that it would be helpful to you to know what our position is. 14:18

MS. JUSTICE COSTELLO: I understand that.

MR. GALLAGHER: This is entirely new as part of, they dismissed it, they dealt with it and they have dealt with it, so that's part of what I will be responding to, the national security contention. They had a 14:18 significant advantage in this case, they put in their submissions after all of ours for procedural reasons, the oddity of this procedure. They put it in and, as part of my response, I was going to, I have outlined to you what the position was, and will still do obviously, 14:19 in terms of national security. I am just saying it is highly unsatisfactory to get it now.

MS. JUSTICE COSTELLO: Hmm.

MR. GALLAGHER: They have had our submissions before they had their own submissions. They've been opening 14:19 the case for six days and we now get it. I'm not going to deprive you of any material that you ultimately find helpful, but I do make the point this is a most unfair way. The first notice we had was literally when it was handed in to you now. 14:19

MR. MURRAY: Judge, it is another play by Mr. Gallagher to get a longer opening. He will have an opportunity to respond to this, it will be the end of next week or the following week. He knows what our case is on

national security, it's in our submissions, that's the primary document I opened.

Now we can do this one of two ways. I can go through the document I have just handed you up, I will ask you to take it back, take it back from Mr. Gallagher and I will go through everything in it now or I can do, as I have done, which is an attempt to try and save everybody's time dealing with matters at a level of detail that may not be necessary. Mr. Gallagher does not need to address this argument in his short opening provided as a matter of concession in a context where his full opening will be in a week or ten days time. 14:19 14:20

MS. JUSTICE COSTELLO: In relation to these documents, can you give me a rough outline of what's in it? In sense of what are we talking about, are there new arguments are there more authorities, what's in it. 14:20

MR. MURRAY: Well there are some more authorities but it is an elaboration in far more detail, on what we have set out there and it also responds to some of the arguments that are in the case, Judge. But in my respectful submission the objection is misconceived. Mr. Gallagher will have a long, long time to consider it in detail. The essence of our argument is in our submission and that's what I have primarily relied upon for the purpose of my opening. 14:20 14:20

MR. GALLAGHER: Well when we refers to response to our document, I assume he is talking about the submissions which have already been responded to, I assume.

MR. MURRAY: Yes. Our response to Mr. Gallagher's 20,000 word submissions, which we did in considerably less space in an attempt to try and provide the court with a succinct summary of the issues. Judge, I'm in the court's hands as to how you would like me to progress the issue, but, as I said, the essential argument is as outlined in the submission which Mr. Gallagher has had for some time. 14:21

MS. JUSTICE COSTELLO: Refresh my memory, is it Mr. Schrems who is going to be speaking before Facebook or Facebook before Mr. Schrems. 14:21

MR. GALLAGHER: Mr. Schrems.

MR. MURRAY: Mr. Schrems is first.

MS. JUSTICE COSTELLO: So it seems to me that we are going to have a position anyway where this isn't going to be concluded today. 14:21

MR. GALLAGHER: No, that is correct, Judge.

MS. JUSTICE COSTELLO: We can both have a little look at this overnight and see where we are going and I will defer any ruling in relation to that, I'll take it in de bene esse at the moment and look at it overnight. 14:21

MR. GALLAGHER: That's fine, Judge.

MS. JUSTICE COSTELLO: Because I'm just looking at the time.

MR. MURRAY: Thank you, Judge. Judge, in relation to the Privacy Shield, which is the second last issue I want to address, again I'll be very brief on this. Everything we have to say is, everything we have to say on this has been outlined in the course of the evidence 14:21

that you have seen.

But the Privacy Shield itself, insofar as it intrudes into the SCCs, and of course Facebook rely primarily upon the SCCs for their data transfers. But the Ombudsman issue, the Ombudsman is not established by law in the sense in which that term is used in Article 47, he doesn't have compulsory jurisdiction, he doesn't make or she doesn't make decisions of a judicial nature, doesn't give reasons, but most critically of all is not independent of the administration. That is a key indicia of a court or tribunal for the purpose of Article 47. As with any court or tribunal Article 6, or indeed for the purposes of the provisions dealing with references. This is not an independent body and it is not a judicial remedy and in our respectful submission the matter doesn't have to be put any further than that. 14:22 14:22 14:22

The last issue is not an issue raised by Facebook, it's an issue raised by Mr. Schrems and an issue which in our respectful submission does not in truth arise from these proceedings but I do just want to address it very briefly and it relates to Article 4. 14:23

Perhaps the best way of looking at this, Judge, if I ask you to go back to the Book of Pleadings Tab 24 where you will see the second affidavit of Mr. O'Dwyer. I don't believe this was opened to you, Judge, by 14:23

Mr. Collins.

MS. JUSTICE COSTELLO: No, I don't think any of Mr. O'Dwyer's affidavit was opened.

MR. MURRAY: And if I can ask you to go to Tab 24 and paragraph 19 where he just notes this question over a number of pages. 14:24

He is picking up a point made by Mr. Schrems in his affidavit where: *"At paragraphs 17 and 19 of his affidavit, Mr. Schrems suggest the Commissioner did not have any or any adequate regard to the provisions of Article 4 of the Decision, which confers on the Commissioner the power to prohibit or suspend data flows to third countries (such as the US) in order to protect individuals in regard to the processing of their personal data."* 14:24 14:24

I say that this doesn't arise in these proceedings because it's not apparent to us how, whether the Commissioner should or should not have exercised that discretionary power under Article 4, how that affects in any way the entitlement of the Commissioner to seek the relief which is being sought here. It seems to be an entirely extraneous consideration insofar as the exercise of your power is concerned. 14:24 14:25

But just to address and explain the Commissioner's position on it, Judge. In paragraph 20:

"*The prohibition or suspension of data flows contemplated by Article 4(1)(a) of each of the SCC Decisions is called for where two decisions are fulfilled: Firstly where it is established 'that the law to which the data importer is subject imposes on him requirements to derogate from the relevant data protection rules which go beyond the restrictions necessary in a democratic society'; second 'where those requirements are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses'.*" 14:25 14:25

And the suggestion seems to have been that the Commissioner ought to have exercised this discretionary power vis-à-vis Facebook so as to prevent data transfers. 14:25

And in paragraph 22, he says: "*The Commissioner did not refer to Article 4 in the Draft Decision and it is not relevant to the within application. Mr. Schrems' attempt to invoke it involves an attempt on his part to expand the scope of the proceedings.* 14:25

23. The Commissioner does not agree with Mr. Schrems' belief that the Commissioner has concluded that the circumstances contemplated by Article 4(1) are met. 14:26

24. Contrary to the premise of Mr. Schrems' averments, Article 4(1) is not expressed in mandatory terms. A

decision on whether or not to avail of the mechanism is a matter for the discretion of the national supervisory authority."

And he then refers to provisions and recitals which he says supports that. 14:26

He then explains that Article 4 is not engaged at paragraph 25. I don't think I need open those paragraphs because they explain what you already well know in terms of what it was the Commission was concerned with. 14:26

In paragraph 28 he says: *"At least insofar as the question of access to an effective remedy is concerned, there is no guarantee contained in the SCC Decisions that can be said to be the subject of a 'substantial adverse effect' as a result of the requirements of any US law that is incompatible with Articles 7, 8 or 47 of the Charter. On this basis, Article 4 of the SCC Decisions is not engaged in the current context.*

29. In addition, the inadequacies the Commissioner identified on a preliminary basis revealed a problem that is systemic in nature, such as to render inappropriate resort to Article 4. It follows that any solution to such inadequacies must likewise target the underlying systemic problem, namely, the fact that a 14:27

legal remedy compatible with Article 47 is not available in the US to EU citizens whose data is transferred to that jurisdiction where it may be at risk of being accessed and processed.

30. In that regard, by analogy with the analysis set out in Hogan J Request for a Preliminary Ruling, the complaint here concerns the terms of the SCC Decision and not the manner of their application."

14:27

"In its decision", he notes at paragraph 31: "*In the CJEU ruling in **Schrems**, the CJEU identified systemic deficiencies in the US legal order in relation to the protection of EU citizens' data protection rights, and concluded that, as a matter of EU law, the Safe Harbour* 14:27 *Decision did not provide safeguards sufficient to address such deficiencies. I say it is necessary and appropriate that the sec Decisions likewise be examined by the CJEU on a systemic basis to determine whether those decisions are capable. Pending such an examination by this Honourable Court and by the CJEU, it would not have been appropriate to single out data flows between individual data exporters and importers and prohibit or suspend those flows in isolation."*

14:28

In other words obviously --

MS. JUSTICE COSTELLO: Facebook but not.

MR. MURRAY: Exactly, and that's, in our respectful submission in the context of a discretionary power, a

legitimate and proper consideration for the Commissioner to take into account in deciding whether to exercise or not to exercise the powers. But we just don't see whether she did or did not do that properly is a matter that arises before you in any event, but that, as it were, is the reason that the Commissioner adopted the position that she did. 14:28

We also just note over the page, and I think that this came in developments since this affidavit was sworn. Yes. She just notes that there was an issue as to the validity of Article 4(1) of the decision in any event after the Schrems ruling because in **Schrems** the CJEU had concluded that: "*The particular form of suspension mechanism provided --*" 14:28 14:29

MS. JUSTICE COSTELLO: Sorry, which paragraph are you reading from.

MR. MURRAY: Paragraph 35, Judge, excuse me. She just observes that: "*Paragraphs 99 to 106 of the ruling in **Schrems** actually cast a question mark over the validity of Article 4(1) because the CJEU had concluded that the particular form of suspension mechanism provided for in the Safe Harbour Decision had the effect of imposing restrictions on the exercise by national supervisory authorities of the powers they had under Article 28 of the Directive to suspend. In circumstances in which the Commission lacked the power to impose any such restriction, the Court concluded that the Commission had acted in excess of its powers.*" 14:29 14:29

Now I just draw that to your attention because it's a useful introduction to this, that in December last year, I think it was 16th December, the Commission took out Article 4(1) of the decision as it originally stood and replaced it with a new Article 4 and they express in their --

MS. JUSTICE COSTELLO: Article 4(1) is in which decision now, are we talking about the Privacy Shield decision or the one of the SCC.

MR. MURRAY: This is in the SCC, yes. 14:30

MS. JUSTICE COSTELLO: SCC decision, because there is three of them. But it's the 2010 decision.

MR. MURRAY: Yes.

MS. JUSTICE COSTELLO: Thank you.

MR. MURRAY: Yes, exactly. I think it's in each of them in fact. So certainly it mightn't have been called Article 4 in all of them -- it is, yes. In the event that has now been replaced because the Commission shared that concern as to validity, there may not have been an Article 4 in place at all at the relevant time. 14:30 So you will see, Judge, there, I think we address that again briefly in the concluding paragraphs of our submissions, but I don't propose to open those to you.

So, Judge, subject to the court, those are our submissions in the opening. Thank you. 14:30

MS. JUSTICE COSTELLO: Well thank you. So, Mr. McCullough, Mr. Doherty had estimated that you would take half an hour, I'm not quite sure if you

agree with his estimate.

MR. McCULLOUGH: I will try and do that, Judge.

Judge, we agree with the DPC on the issues that you have heard agitated over the last five days. So we agree on the necessity for effective equivalence; we agree on the requirement as a matter of EU law that an effective judicial remedy should be provided; and we agree that US law imposes requirements that don't permit that EU law standard to be met. We agree that that is so both because of the US laws relating to standing and because such remedies as do exist in US law are subject to the wide exceptions, immunities and barriers that have been explained to you. 14:31 14:31

I don't intend - we have some material, Judge, and in due course we will add to that, but I don't intend to use the exceptional opportunity that you have given to me today to advance a case with which I fundamentally agree. I don't think that would be a useful use of this time. What would be useful I think, Judge, is to explain to the court the respect in which our case differs from that of the DPC. 14:32

It differs in this respect, Judge: That we say that it is not appropriate to make a reference. The starting point, Judge, is to look at the basis upon which a reference can be made by a court. The text of Article 267 itself, Judge, is clear on that. The court 14:32

will find that at Book 1 of the authorities, Tab 2.

MS. JUSTICE COSTELLO: 267; is that right?

MR. McCULLOUGH: 267, Judge, yes.

MS. JUSTICE COSTELLO: Yes, I have it. Thank you.

MR. McCULLOUGH: Thank you, Judge. You will see, Judge, Article 267 provides: 14:33

"*The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning the interpretation of the Treaties; and the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union; where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the Court to give a ruling thereon.*" 14:33 14:33

So the question must be properly raised before the national court and it must be a question whose resolution is necessary to allow the national court to give judgment in relation to the issue raised before it. 14:34

There's a number of authorities dealing with that, Judge. I'm not sure at this stage the extent to which what I say on this matter will be a subject matter of controversy, so I will just refer to court to one at this stage, the well known decision of **CILFIT** which the 14:34

court will find at Book 2 of the authorities, I hope, Tab 21. If the court could move to paragraphs 9 to 11 of that judgment the court will see the relevant text.

MS. JUSTICE COSTELLO: That's Book 2 of authorities and it's tab? 14:35

MR. McCULLOUGH: 21, I hope, Judge.

MS. JUSTICE COSTELLO: Thank you. Paragraph 9.

MR. McCULLOUGH: Paragraphs 9 to 11, Judge, are the relevant paragraphs.

MS. JUSTICE COSTELLO: Yes. 14:35

MR. McCULLOUGH: The court said: *"In this regard it must in the first place be pointed out that Article 177 does not constitute a means of redress available to the parties to a case pending before a national court or tribunal. Therefore the mere fact a party contends a* 14:35 *dispute gives rise to a question concerning the interpretation of Community law does not mean that a court or tribunal concerned is compelled to consider has been raised within the meaning of Article 177. On the other hand, a national court or tribunal may, in an* 14:35 *appropriate case, refer a matter to the Court of Justice of its own motion.*

10. Secondly, it follows from the relationship between the third and third paragraphs of Article 177 that the 14:35 *court or tribunal as referred to in the third paragraph have the same discretion as any other national court or tribunal to ascertain whether a decision on a question of community law is necessary to enable them to give*

judgment."

And that's the important point, Judge: "*Accordingly, those courts or tribunals are not obliged to refer to the court of justice a question concerning the interpretation of community law raised before them if that question is not relevant, that is to say, if the answer to that question, regardless of what it may be, can in no way affect the outcome of the case.* 14:36

11. If, however, those courts or tribunals consider that recourse to community law is necessary to enable them to decide a case, Article 177 imposes an obligation on them to refer to the court of justice any question of interpretation that may arise." 14:36

Now as the court is aware there's a difference between the rules that apply to a Court of First Instance and a final court in this respect. But in either event, Judge, the requirement is that the reference must be necessary. 14:36

And it's important just to reflect on that for a moment, Judge. The question of necessity doesn't arise to be determined in the context just of the proceedings before *this* court. The DPC can't, if you like, simply by bringing this question only before the court then make it necessary for this court to refer the question that the DPC has brought before this court to the Court 14:36

of Justice. The lis between the parties arises from Mr. Schrems' complaint, that's the matter that the DPC is investigating.

This matter comes before this court only because the DPC has found an issue in that case that she wants to refer to the court. But the question of necessity falls to be determined in the context of Mr. Schrems' complaint and the investigation into it, and that's a crucial point, Judge. 14:37

MS. JUSTICE COSTELLO: Can you just explain to me -- how that arises. Because obviously the complaint has to be dealt with by the Commission. 14:37

MR. McCULLOUGH: Yes.

MS. JUSTICE COSTELLO: I don't have a function at all in relation to the merits of that complaint.

MR. McCULLOUGH: No.

MS. JUSTICE COSTELLO: That's for the national authority, in this case the Commissioner. 14:37

MR. McCULLOUGH: To put it in practical terms, Judge.

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: If it is not necessary for the Commissioner in order to resolve the complaint made by Mr. Schrems to refer this court, to refer this question to the Court of Justice, well then the reference is not necessary. To put it in the positive sense, Judge, if the DPC can resolve Mr. Schrems' complaint without a 14:38

reference to the Court of Justice then the reference isn't necessary.

MS. JUSTICE COSTELLO: Well I understand what you are saying in relation to your complaint before the DPC.

MR. McCULLOUGH: Yes. 14:38

MS. JUSTICE COSTELLO: But what about these proceedings, I mean the two reliefs sought in these proceedings.

MR. McCULLOUGH: There are, Judge, but it would be entirely self-fulfilling of the necessity requirement 14:38 if necessity fell to be determined in these proceedings only. The DPC could create that necessity by saying well these are the only questions that I am bringing before the court and therefore, because these are the only questions before the court, it's necessary for 14:38 this court to refer those questions to the Court of Justice.

Whereas in fact the proper perspective --

MS. JUSTICE COSTELLO: You are saying you can't 14:39 artificially create necessity.

MR. McCULLOUGH: Exactly, Judge. You can't artificially create necessity. The DPC can't hive off one question and say 'now having hived off this one question it's now necessary for the court to refer this 14:39 question to the Court of Justice'. The issue is whether, in order to resolve Mr. Schrems' complaint and the investigation that follows into it, it is necessary that there should be a reference.

The starting point, Judge, is the decision itself, the decision 2010. I would ask the court to look at that. We were looking at it just a moment ago with Mr. Murray. You'll find that, Judge, at book --

MS. JUSTICE COSTELLO: This is the third of the Commission's decision in relation to the SCCs. 14:39

MR. McCULLOUGH: Yes, exactly, Judge.

MS. JUSTICE COSTELLO: It is just there are so many decisions around the place I have to make sure which one we're talking about. 14:40

MR. McCULLOUGH: There are. I suppose there are really two on one level, Judge. There is one amended decision and this is the second decision, the 2010 decision.

MS. JUSTICE COSTELLO: And where do I find that now again. 14:40

MR. McCULLOUGH: You'll find that in Book 1, Judge, of the authorities Tab 10.

MS. JUSTICE COSTELLO: Thank you.

MR. McCULLOUGH: (Short pause) If you look, Judge, at Article 1: 14:40

"*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* 14:41 *regards the exercise of the corresponding rights as required by [Article] 26(2) of Directive 95/46.*"

So the court will recall Article 26 of the Directive

sets up certain permitted derogations from the overall principle, and this decision provides that the standard contractual clauses offer adequate safeguards in order to overcome the difficulty that would otherwise be created by the lack of adequate safeguards in US law. 14:41

MS. JUSTICE COSTELLO: By failing the Article 25 test?

MR. McCULLOUGH: Exactly, Judge, yes. And indeed you don't come within Article 26 at all unless you fail the Article 25 test, so the premise of being within Article 26 at all is if you fail the Article 25 test. 14:41 And, as Mr. Murray has explained, the point of the SCCs is to bring you back into compliance with the test that you have failed under Article 25.

If the court then just looks at one definition in Article 3. 14:42

MS. JUSTICE COSTELLO: Yes.

MR. McCULLOUGH: It is *"applicable data protection law"* means: *"The legislation protecting the fundamental rights and freedoms of individuals and in particular their right to privacy with respect to the processing of personal data."* 14:42

MS. JUSTICE COSTELLO: Sorry, yes.

MR. McCULLOUGH: It's (f), Judge.

MS. JUSTICE COSTELLO: Yes. 14:42

MR. McCULLOUGH: *"And in particular their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the exporter is established."*

And Article 4, Judge, is the most important part of this: "*Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to various chapters of Directive 95/46, the competent authority in the Member State they may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where.*" 14:42

14:42

And then three possibilities are set out, it's the first we're looking at here:

"*It is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses.*" 14:42

And there's a notification obligation, Judge, at 5(3). 14:43

So if I can sum up, Judge, what the short decision states. First it states that one isn't entitled to a derogation under Article 26 unless your agreement is in

compliance with the SCC decision. That's what Article 1 provides.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: If you are in compliance with the SCC decisions, if the contract pursuant to which you transfer material is in compliance with the SCC decision, you are entitled to obtained the benefit of the derogation for which this decision provides. Of course the corollary of that is if your contract is not in compliance with the SCC decisions well then you're not entitled to rely on this decision at all, you don't have a derogation. 14:43 14:43

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: Then Article 4 provides for what is to happen if the DPC ascertains that the law in the country to which the data is being transferred imposes requirements to derogate from applicable data protection law which go beyond the restrictions necessary in a democratic society. 14:44

14:44

And in essence, Judge, that means that Article 4 kicks in where US law, in this case, imposes requirements to derogate from EU data protection law that go beyond those that could be justified to safeguard national security as a matter of EU law interpretation, and I'll come back, Judge, to Article 13 of 95/46 in due course. 14:44

So Article 4 kicks in, Judge, when US law, or the law of the country to which the material is being

transferred, imposes additional requirements that go beyond what would be justified in EU law.

And then the second condition in Article 4 is that those requirements, in this case the requirements of US law, are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law or the standard contractual clauses. 14:45

So the second question is do the requirements in this case of US law have a substantial adverse effect on the guarantees that are provided by EU data protection law and the SCCs? 14:45

And the structure of the decision is as follows, Judge: That if the DPC or the national commissioner, in this case the DPC, come to the view that the conditions in Article 4 are not met well then it's her obligation to suspend data flows to that country. The conditions, Judge, that are set out in Article 4 are for practical purposes, the same as the adequate level of protection or effective equivalence requirements that you find between Article 25 and 26. They are not expressed in exactly the same way, Judge, but in practical terms they are the same. 14:45 14:46 14:46

To put it, Judge, at colloquial level: If US law doesn't provide for effective protection, if it imposes requirements that mean that you can't abide by the

safeguards that are otherwise provided by the SCCs, such that those requirements of foreign law have a substantial adverse effect on the guarantees that the SCCs are meant to provide, well then the DPC has a job to do. 14:47

MS. JUSTICE COSTELLO: They sort of nullify the SCCs in effect.

MR. McCULLOUGH: I beg your pardon?

MS. JUSTICE COSTELLO: You are saying, if you like they nullify the SCCs role of filling in the otherwise inadequacy. 14:47

MR. McCULLOUGH: Insofar as that country is concerned.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: Of course the SCC decision applies worldwide. 14:47

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: And the discovery that the laws of a particular country have the effect as described in Article 4 won't apply across the world, it will apply only to the country in which one ascertains that about the loss. So that's the job that is provided for the DPC under Article 4. 14:47

The court can see the internal structure then of the decision. It says you can't transfer unless you are in compliance with the SCCs. And then it says, if the DPC ascertains that US law for practical purposes has the effect that the guarantees provided by the data protection laws in the SCCs cannot be met, well then 14:47

she must suspend data flows. That is one of the fundamental points made by Mr. Schrems here, Judge, that that's what the DPC should be doing if she comes to the view that the conditions of Article 4 are met, that there is a remedy provided in Article 4 to meet precisely the circumstances that are said to arise in this case before you and that it is wrong to ask that the SCC decision should be nullified as a whole. Rather, it would be it would be correct to use the remedy for which the decision itself provides, that is to suspend data flows. 14:48 14:48

Can I move then, Judge -- and Mr. Murray says correctly that Article 4 has subsequently been altered, Judge, and you will find the altered version, I think, in the 2016 decision at Tab 14 of the same book. I just bring it to your attention, Judge, instead of opening it now, but I don't think I need to open it at this stage. 14:48

Can I move then, Judge, to the reformulated complaint in order to see what are the issues that Mr. Schrems raised and therefore what are the issues that the DPC should be investigating. You'll find that, Judge, at Book 1, not of the authorities, Book 1 of the -- 14:49

MS. JUSTICE COSTELLO: Trial book. 14:49

MR. McCULLOUGH: -- the trial book, Judge, exactly, at Tab 17, I think, Judge. Mr. Schrems's complaint can be described compendiously in the following way, Judge.

He complained that his data was being transferred in breach of his rights as an EU citizen, but he broke that down into a number of different complaints, different issues that he raised. First, Judge, as is clear from the text when I take you to it that he didn't limit his complaint to the SCCs. He said that he knew about the SCCs because Facebook had given him a redacted version of their data transfer agreement, but he made it clear that his complaint wasn't limited to those and that there may well be other means by which Facebook Ireland transfers its data to the US and those two should be the subject matter of the investigation, that's the first point. 14:50 14:50

The second point that he raised was this, Judge: In respect of the SCCs specifically, he raised a particular complaint. He said that the Facebook Data Transfer and Processing Agreement, that's the phrase that's used, the Data Transfer and Processing Agreement, doesn't comply with and isn't in the form permitted by the SCCs. The court will recall Article 1 of the SCCs; unless you are in accordance with the format set out in the annex, you're not entitled to use the derogation at all. And that was Mr. Schrems' basic complaint in relation to the SCCs. He says well they are not in compliance with Article 1 and therefore they are not entitled to use the derogation at all. 14:51 14:51 14:51

Then, thirdly, he said, Judge, as a subsidiary point,

that if there is compliance on the part of Facebook with Article 1 of the decision, it was nevertheless the case that the transfer by Facebook to the US was in breach of the principles of EU law but that the appropriate remedy under those circumstances was to apply Article 4. And he raises it very specifically. 14:52

Mr. Schrems, Judge, did not ask the DPC to pursue the invalidity of the decisions, rather he raised these specific points. He said it's only one of the issues, it's one of the means by which there may be transfer, you should investigate the others; secondly, in particular he said about the SCC decisions they are just not in compliance with them; and then, thirdly, he said, if I'm wrong about that, it's not that I am asking you to invalidate the SCCs, rather I am asking you to operate Article 4, making the point that that's precisely what the decision provides for. It provides internally for a method to enforce its provision.. 14:53 14:53

Now if we just take a moment, Judge, to look through some of the content of the reformulated complaint, Judge. I think it's at Tab 16, Judge - sorry, Tab 17, Judge. It's not the first --

MS. JUSTICE COSTELLO: No, I'm in it. I am just trying to work where into it. 14:54

MR. McCULLOUGH: It's a few pages into it, Judge. There's a couple of letters.

MS. JUSTICE COSTELLO: Yes, complaint, I have it.

I have the complaint, yes.

MR. McCULLOUGH: It's dated 1st December 2015.

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: I'll just bring the court to parts of it. In the second paragraph on page 1, Judge, he refers to the discussions that he's been having with Facebook and he says: 14:54

"*As a preliminary point my solicitors wrote to Facebook Ireland Limited on 12th October 2015 requesting details of all legal basis that they were relying on to transfer my data to the US. Furthermore, I requested a copy of any contract that they purported to rely on. Unfortunately, Facebook Ireland Ltd has only responded to my request on Friday, 27th November 2015 at the end of the business day. The response from Facebook Ireland Limited's solicitors attached an Agreement dated 20th November 2015 between 'Facebook Ireland Ltd' and 'Facebook Inc'.*" 14:54

And you'll find that, Judge, at Tab 23 at this book, you'll find the data transfer agreement itself.

You'll find it there in redacted version, Judge.

MS. JUSTICE COSTELLO: Mm hmm. 14:55

MR. McCULLOUGH: You actually had it opened to you yesterday, an unredacted version, in the affidavit of Ms. Cunnane and you'll find it at Book 5 Tab 29 as well. I'll come to it in just a moment.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: *"The request to identify any other legal basis for transfers between Ireland and the United States of America has not been comprehensively answered by Facebook Ireland Ltd. Instead, they state 'in addition to the agreement, Facebook Ireland relies on a number of additional legal means to transfer user data to the US'."* 14:55

That's I suppose the first of the points I raise, Judge. Mr. Schrems is saying well I know about the SCCs but it's not just that that I am concerned about. I have asked what else they rely on, they won't give me the details of it, but they have said that they rely on *"additional legal means to transfer data to the US"*. 14:55

Can I ask you, Judge, to turn forward to, he sets out the facts, Judge, then on pages 2 through to 6 and we'll just pause on page 6 for a moment.

MS. JUSTICE COSTELLO: Mm hmm. 14:56

MR. McCULLOUGH: You see he returns to this point about other legal grounds at item 8 on that page.

MS. JUSTICE COSTELLO: Yes.

MR. McCULLOUGH: He says: *"Facebook Ireland does not identify other legal grounds for a data transfer. My solicitors wrote to Facebook Ireland on 12th October 2015 and requested the following:* 14:56

'Therefore, we require you to identify, by close of

business on Friday 16th October 2015, all legal basis that you are relying to transfer our client's data to the US. When replying, we call upon you to forward us a copy of any contract relied on by you'.

In their reply dated 27th November 2015 'Facebook Ireland Ltd' has refused to identify all legal bases that it uses to transfer data to the US. This fact is especially relevant given the duties to inform data subjects (actively, but at least upon request) about these grounds under the law. The fact that 'Facebook Ireland Ltd' has refused such information upon request may render any of these grounds invalid in any event."

The important point, Judge, is that he is not confining his point to the SCCs. As I say that's the one he knows about.

Then over the page, Judge, on page 7 he engages on his legal analysis. Most of that I don't need to look at, Judge. At paragraph 1 he deals with the definition of processing and he makes the point, Judge, that Mr. Collins and Mr. Murray have included at the third paragraph that: "*Processing includes making available",* that goes to the substance of the matter, Judge, but it's an important point. 14:57 14:57

Then at 2 he deals with the Charter of Fundamental

Rights, 3 Irish Constitutional law. At 4 he makes some general remarks on the transfer to a third country under the Directive. And then if I can ask you to look, Judge, at item 5 on the next page.

MS. JUSTICE COSTELLO: Mm hmm. 14:57

MR. McCULLOUGH: Under the heading: "*Specific justifications under Directive 95/46/EC.*

In the letter of 27th November 2015 Facebook Ireland Limited has denied any comment on the methods used to 14:58 *transfer data to the US other than an 'Agreement' based on decision 2010/87 and a 'number of other additional legal means' that they apparently intend to address 'as part of the now ongoing investigation'."*

14:58

It's the same point again: "*Given this clearly defensive and unhelpful response by 'Facebook Ireland Ltd' I am unfortunately not in a position to make any final comment on the legal basis 'Facebook Ireland Ltd' may argue in the course of these proceedings, which could have led to a fast decision. However, there are a number of options 'Facebook Ireland Ltd' will likely try to argue. In the interest of a swift procedure I would therefore comment on the following options in advance.*" 14:58

And the court is familiar, that there are a number of organisations, different derogations in particular under Article 26, not just the SCCs, but he deals in

particular with the SCCs. He deals with that at (a):

"*According to the letter from 27th November 2015 Facebook claims to rely on standard contractual clauses, in the version of Commission decisions 2010/87/EU.*" 14:58

And then he makes his specific complaint about that:

"*Validity of the arrangement provided. Application of SCCs significantly limited by undisclosed additional agreements.* 14:58

The clauses used by Facebook Ireland Limited and Facebook Inc. significantly differ from the ANNEX to Decision 2010/87/EU, most notably:

** The contract provided is giving priority to some blacked out arrangement named in Clause 2.3 over the ANNEX to Decision 2010/87/EU. Unless this legal basis is disclosed, 'Facebook Ireland Ltd' cannot possibly rely on Decision 2010/87/EU if the ANNEX is altered in a way that it is overruled by some non-disclosed element.*"

I'll bring the court to the Facebook agreement in a moment, Judge. He had only a redacted version, but he is making the point that the Facebook data transfer agreement appears on its face to be subject to some other agreement and he is saying that means that it's 14:59

not in compliance with article - with the 2010 decision.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: He may be right or he may be wrong about that, Judge, of course, but that's the complaint that he is making. 14:59

Then he continues: "*The contract provided is giving priority to some blacked out arrangement named in Clause 2.3 over the ANNEX to Decision 2010/87/EU. Unless this legal basis is disclosed, "Facebook Ireland Ltd" cannot possibly rely on Decision 2010/87/EU if the ANNEX is altered in a way that it is overruled by some non-disclosed 'intragroup agreements'.*

As Commission Decision 2010/87 only applies to 'standard contractual clauses set out the Annex' according to Article 1 of the Decision, 'Facebook Ireland Ltd' cannot claim the benefits of Decision 2010/87 when using an altered contract that allows other undisclosed elements to overrule the agreement. The nature of 'Standard Contractual Clauses' is that a controller cannot independently overrule these standards. Accordingly Clause 10 of the ANNEX to Decision 2010/87/EU states that:

'The parties undertake <u>not to vary or modify the</u>

Clauses. *This does not preclude the parties from adding clauses on business related issues when required as long as they do not contradict the clauses."*

And that, as I say, Judge, is the fundamental point that he makes. I will just pause for a moment, Judge, to change. 15:00

Then, Judge, in the next heading he continues:

"*Contracts covering Sub-Processors missing*
As known to your office, 'Facebook Ireland Ltd' and/or 'Facebook Inc' use a large number of sub-processors to provide its services... The relevant contracts have to be disclosed under Clause 4(h) of the Agreement, which 'Facebook Ireland Ltd' has failed to do. It is therefore not possible to assess the legal protection of my personal data if my data is processed by the various sub-processors."

Then he makes a number of other different complaints, Judge, but they're all related to the same point; he says that they all have the same effect, to a greater or lesser degree, that the Facebook Data Transfer Agreement is not in accordance with the 2010 decision. 15:01

If we turn over the page, Judge, to where he summarises his views on the validity of the SCCs used. He says:

"*In summary, 'Facebook Ireland Ltd' cannot possibly rely on Decision 2010/87 on the basis that it does not even fulfil the most basic formal requirements: It does not cover all processing operations by 'Facebook Inc', it does not include the necessary arrangements with sub-processors, it is not even signed in a verifiable way and obviously only applies to transfers within the last week.*

Most notably 'Facebook Ireland Ltd' has chosen to depart from the text in the ANNEX to the decision. Accordingly, the DPC is not at all 'bound' (let alone 'absolutely bound') by Decision 2010/87, Article 26(4) of Directive 95/46 and/or 11(2) of the Irish Data Protection Act. At the same time the DPC is *bound by the judgments of the CJEU... and the High Court in Schrems... and the CFR as well as the Irish Constitution, which clearly prohibit a transfer in this situation, as set out above*".

MS. JUSTICE COSTELLO: CFR, what's that a short for again? 15:02

MR. McCULLOUGH: The Fundamental Rights Charter, Judge.

MS. JUSTICE COSTELLO: The Charter.

MR. McCULLOUGH: The Charter. So as I say, Judge, it's clear that's the fundamental point. He says 'Just not in accordance with the SCCs. 15:02

The next paragraph, Judge, and the paragraph after that

are the two paragraphs that are selected by the DPC to use in the draft determination and they're repeated indeed in the pleadings. And it's said, if you like, either stated expressly, or at least inferred, that the next two paragraphs are, if you like, at the heart of the complaint. I'll just read them out, Judge. He certainly *makes* those complaints, Judge, but in fact you have to see them in context. 15:03

He says: 15:03

"*'Facebook Ireland Ltd' has not proven that the alternative agreement was authorised by the DPC under Section 10(4)(ix) DPA. Even if it would be, such an authorization would be invalid (and void in the light of the judgements... Schrems... and therefore irrelevant in this procedure.*"

Then the next paragraph, Judge: "*Even if the current*" -- and the next paragraph is also quoted by the DPC in the draft determination. 15:03

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

7, 8 and 47 of the CFR (as the CJEU has held) and the Irish Constitution (as the Irish High Court has held)."

So he's moving on to a second point, Judge. He's saying 'Well, even if there's no problem about compliance with the SCCs, they still can't rely on them', for the reasons that he states here - their failure to comply with the Directive and the Charter. 15:04

The next paragraph, Judge, though is what he says follows from that. And this paragraph, Judge, isn't in the draft determination. He says: 15:04

"*Article 4(1) of Decision 2010/87 (as all other relevant Decisions) takes account of a situation where national laws of a third country override these clauses, and allows DPAs to suspend data flows in these situations.*"

Then he quotes Article 4(1)(a) and its then text 15:04

"*This section is taken from Art 4(1)(a) of Decision 2010/87, but all other decisions that 'Facebook Ireland Ltd' may claim in these procedures have similar exceptions.*"

And they do, Judge.

"*The fact that the 'PRISM program' violates the essence*

of Art 7 and 47 CFR was clearly established by the CJEU and is binding on the DPC."

Now, just leave that for a moment, Judge, and look at the foot of the page. He raises consent under b. Now, consent, Judge, is a reference back to one of the permitted derogations under Article 26. It's another possibility. It's -- 15:05

MS. JUSTICE COSTELLO: If 6(2) wasn't one of the six points? 15:05

MR. McCULLOUGH: It is, Judge, exactly. So this is another possible derogation on which Facebook may be relying and Mr. Schrems is saying 'Well, of course' --

MS. JUSTICE COSTELLO: He's speculating as to what the -- 15:05

MR. McCULLOUGH: He's speculating and saying 'I don't know, but this is something you have to investigate'.

"*Consent* 15:05
It is very much disputed that the rights under Art 7 and 47 CFR can be 'waived' through consent. In addition 'consent' to be freely given requires that a user has the free choice between different options. Given that 'Facebook Ireland Ltd' has basically become a utility and users cannot choose between having their data transferred to the United States or not, the user is not in any situation that would allow for a 'freely given consent'. I therefore submit that consent is

not *a legal basis for any data usage that violates fundamental rights...*"

Then he says, Judge, even if they can be waived, he says consent has to be freely given. Then, Judge, under c, at the foot of page, he says "Any Other Legal Basis". 15:06

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: "*Any other derogation under Article 26(1) of Directive... that 'Facebook Ireland Ltd' may argue must again fail on the basis that the CJEU has been very clear that transfers that lead to the use of such data for 'mass surveillance' are a violation of Art 7, 8 and 47.*"

So he's making it clear, Judge, as I say, that he's not limiting himself to the SCCs.

Then finally, Judge, if I can turn to page 15 of the complaint, where he sets out his requests. He says this is what he wants. He wants the DPC -- 15:06

"*Suspension of all data transfers*
Based on the facts and legal arguments above - and any other legal or factual basis - I therefore request that the DPC issues a prohibition notice under Section 11(7) to (15) DPA, an enforcement notice under Section 10(2) to (9) DPA and/or any other appropriate step to suspend all data flows from 'Facebook Ireland Ltd' to 'Facebook

Inc'."

I'll come to Section 11 in just a moment, Judge, but it provides the means in Irish law whereby orders such as those for which Article IV of the decision can be made. 15:07

So as I say, Judge, you'll find the unredacted version of the Facebook agreement, Judge, in a number of places, but the version I think that you were looking at yesterday is in book five, tab 29. 15:07

MS. JUSTICE COSTELLO: 29?

MR. McCULLOUGH: Yes, Judge. And if you'd just look at clause 2. It's really a very short extract. These are the two paragraphs to which Mr. Schrems was referring in particular, although as I say, he had them 15:07 in redacted version. So it's clause 2, subclauses 2 and 3 to which he was referring.

"*2. For the avoidance of doubt, nothing in this clause 2 shall impact on or affect other intragroup agreements in the Facebook group of companies save for those which have, as their primary object or effect the international transfer and processing of data.*

3. In particular, and without prejudice to the generality of the foregoing, this Agreement shall not impact upon the Data Hosting Services Agreement between the parties dated September 15, 2010."

And he makes the complaint on that basis, but on the other basis set out in the reformulated complaint that this agreement isn't in compliance with the SCCs. As I say, Judge, he may be right or he may be wrong, but that's what the complaint was. 15:08

So, Judge, having seen the complaint, I think one can summarise it in the following way. The primary focus is on the contention that the contract didn't comply. Secondly, Judge, it's pointed out that the SCC decisions are only one of numerous different types of entitlements upon which Facebook may rely - he was making it clear that they all require to be investigated as part of his overall complaint. And then thirdly, Judge, he's saying, as a contingent issue only arising from his first complaint in relation to the SCCs, he's saying that *even if* this agreement is in compliance with the SCCs, Facebook can't rely on it anyway due to the inadequacy of protection, but he's making it clear that the correct course and the course that he's asking the DPC to follow is to use the powers under Article IV. 15:08 15:09 15:09

I said, Judge, that I'd bring you to Section 11 of the Act and I'll do that very briefly just to show the Irish... 15:09

MS. JUSTICE COSTELLO: I'll do it on the tablet thing here.

MR. McCULLOUGH: Yes, Judge. You'll find that,

Judge, in book two, tab 17. And it's Section 11, Judge. Perhaps I'll just bring your attention to it, Judge, in the interests of saving time.

MS. JUSTICE COSTELLO: Where is it? On the books, book seven? 15:10

MR. McCULLOUGH: It's book...

MS. JUSTICE COSTELLO: I'm just, I'm in your pad and there's...

MR. McCULLOUGH: Book two, Judge, tab -- no, sorry, on the pad. Let me find it in a different way then. 15:10

MS. JUSTICE COSTELLO: Maybe the pages.

MR. McCULLOUGH: Yes, certainly, Judge. A13, Judge, tab 17. On the tablet, Judge, it's --

MS. JUSTICE COSTELLO: Yes, thank you. Agreed EU/Irish authorities and it's... 15:10

MR. McCULLOUGH: Tab 17, Judge.

MS. JUSTICE COSTELLO: Do you have a page? This isn't speeding me up at all.

MR. McCULLOUGH: It's page 48, Judge. 15:11

MS. JUSTICE COSTELLO: Oh, God. No, it's eight of three thousand and something. We'll go back the old way.

MR. McCULLOUGH: It may be easier to go back the old way, Judge, I'm sorry. 15:11

MS. JUSTICE COSTELLO: What was it again? Okay, I did try. Where were you in old money, Mr. McCullough?

MR. McCULLOUGH: Book B2, Judge, tab 17.

MS. JUSTICE COSTELLO: Yes, thank you.

MR. McCULLOUGH: And Section 11, Judge. I hope that *is* the Act, Judge, that you're...

MS. JUSTICE COSTELLO: This is in the prohibition on and transfer of personal data outside the State?

MR. McCULLOUGH: Yes, Judge, exactly. 15:12

MS. JUSTICE COSTELLO: It's F32 then, is that --

MR. McCULLOUGH: F32, Judge, yes. That's just a footnote I think. And then Section 11. So it provides:

"*The transfer of personal data to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer and, in particular, but without prejudice to the generality of the foregoing.*"

Then it sets out a number of criteria, Judge, that the DPC should consider, including the nature of the data, the purpose for which, the period the data is intended to be transferred and so on.

15:12

Then over the page at subsection 3, Judge, it mirrors, I suppose, the requirement of the decision, that the Commissioner shall inform the Commission and the supervisory authorities of the Member States in any

case in which he or she considers a country outside the EEA does not ensure the adequate level of protection referred to in subsection 1 of this section.

There is a similar provision, Judge, in the Directive itself that I'll bring you to in book one, tab four, Judge. 15:13

MS. JUSTICE COSTELLO: I'm assuming that's authorities, not trial book?

MR. McCULLOUGH: It *is* authorities, Judge, yes. 15:13

MS. JUSTICE COSTELLO: I'm sorry, you did tell me the tab.

MR. McCULLOUGH: Tab four, Judge.

MS. JUSTICE COSTELLO: Thank you.

MR. McCULLOUGH: And Article 28, Judge, sub-article 3. 15:14

MS. JUSTICE COSTELLO: Yes, I think Mr. Collins opened it.

MR. McCULLOUGH: Yes. Very good, Judge. Well, then I won't open it again, Judge -- 15:14

MS. JUSTICE COSTELLO: No, no, it's all right. Do, yes.

MR. McCULLOUGH: It's the second indent, Judge:

"*Each authority shall in particular be endowed with:*

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out... ensuring appropriate

publication of such opinions" - and then this is the important bit - "*of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller.*"

And so on, Judge. So that ties in with Section 11. So those are the three issues, Judge, that he raised. Then can I bring you very briefly, Judge, to the draft decision itself and just show you, Judge, how they were addressed. You'll find that, Judge, at book one, tab 18. And the, if you like, Judge, the fundamental difficulty that we have with the draft determination is that it doesn't really address the points to which I've been bringing the court's attention, and those are all points that need to be addressed before it can be said that a reference on *this* point, which is not really a point raised by Mr. Schrems at all, can be said to be necessary. 15:15 15:15

So I'll open just very short parts of this, Judge. If you look at paragraph 36. 15:16

MS. JUSTICE COSTELLO: "*Strand 1 of the Investigation*"?

MR. McCULLOUGH: Sorry, Judge, maybe paragraph 33 onwards at page 15 of the draft determination. The Commissioner sets out her post-litigation investigation of the complainant's complaint. At paragraph 33 she says - she's talking about what happened immediately after the **Schrems** decision came back from Europe and 15:16

Judge Hogan's decision was made - she says:

"*Immediately thereafter, my office opened its investigation into the Complainant's complaint. In circumstances where there was by now no question but that EU/US transfers of Facebook subscriber data could no longer be undertaken under the safe harbour arrangements, the investigation has sought to establish whether, following the demise of the Safe Harbour Decision, the transfer of personal data relating to its European subscribers by FB-I to Facebook Inc. is lawful.*"

And that in itself, Judge, is a perfectly reasonable description of what she should've been doing. If I can continue then, Judge, to paragraph 34: 15:17

"*In practical terms, my investigation has proceeded in two distinct strands, running in parallel. Strand 1 has comprised a factual investigation focused on establishing whether FB-I has continued to transfer subscribers' personal data to the US subsequent to the CJEU Judgment of 6 October 2015. If and to the extent that it does, my investigation has also sought to examine the legal bases on which such transfers are effected.*"

And that in itself, Judge, again, if you like, is not -- none of that is unreasonable. Then at paragraph

35, Judge, she refers to the fact that her office notified the FBI of the commencement of the investigation, it invited Mr. Schrems to reformulate his complaint and it says that Mr. Schrems duly submitted his reformulated complaint on 1st December. And the court has seen all that. I'll just continue, Judge, after the words "1st December". 15:18

MS. JUSTICE COSTELLO: Yes.

MR. McCULLOUGH: *"Having secured access in the interim to one or more of the data processing agreements to which FB-I and Facebook Inc. are party, that complaint referred to the nature and extent of those parties' reliance on the SCC Decisions. (A copy of the complaint is contained at Annex 1...). In particular, Mr Schrems made the following complaints."*

Then, Judge, there are two paragraphs quoted. And I suppose, Judge, taken in isolation, they *do* look as if Mr. Schrems has, as his fundamental problem, a complaint about the validity of the SCC decisions. But in fact the court has seen that wasn't the point of the reformulated complaint at all. 15:18

Then having set out those two paragraphs, Judge, from Mr. Schrems' reformulated complaint, the DPC continues under "Strand 1", paragraph 36: 15:18

"*In the course of exchanges between FB-I and this Office in relation to Strand 1, FB-I has acknowledged*

that it continues to transfer personal data relating to Facebook subscribers resident in the European Union to its US-established parent and, further, that it does so, in large part" - I'd ask the court to note "in large part" - "*on the basis of its contention that - by means of the deployment of the form of standard contractual clauses set out in the Annexes to the SCC Decisions - the company ensures adequate safeguards for the purposes of Article 26(2) of the Directive with respect to the protection of the privacy and fundamental rights and freedoms of EU-resident subscribers to the Facebook platform and as regards the exercise by such subscribers of their corresponding rights.*"

And you'll see, Judge, when we go through this, there is in fact no investigation of two matters: One, the SCCs are the *only* derogation that are investigated in the draft decision, the determination, there is in fact no investigation of the other derogations of the; and 15:19
secondly, Judge, there is in fact no investigation, certainly no determination of Mr. Schrems' fundamental point, which is to question whether the Facebook agreement was in compliance with the 2010 decision.

15:20

So at Strand 2, Judge, she sets out what she embarks upon on that. The court has already seen that, Judge, I won't open that. Then, Judge, the DPC goes on to set out in some detail her findings as to the defects -- or

I should say as to the absence of sufficient protection in US law. The court has seen those, Judge, and I don't think I need to open them again in detail. I should say, Judge, we agree with the *entire* of it. Everything she says about US law, Judge, we're in entire agreement with. We agree with her both about the requirements of EU law and the differences between what can be supplied, or what should be supplied under European Union law on the one hand and what *is* available pursuant to the requirements of US law on the other hand. 15:21 15:21

Judge, if you turn then just to paragraph 60, you'll see her conclusions on all of these matters.

MS. JUSTICE COSTELLO: Yes. 15:21

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

61. It is also my view that the safeguards purportedly constituted by the standard contract clauses set out in the Annexes to the SCC Decisions do not address the CJEU's objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in Schrems."

Now, the point is this, Judge: If the DPC relies on this material as material upon which she brings this application before the court asking this court to refer a question as to the validity of the SCCs, we say, 15:22
Judge, that this same material leads inexorably to a decision that Article IV is engaged and, therefore, according to the proper scheme of the decision, ought to lead to a suspension of data transfers pursuant to Article IV of the 2010 decision. 15:22

That's perhaps more evident, Judge, at paragraph 62, where she says:

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

And of course, he *did* say, Judge, that they can't be

relied upon, but he made it clear that that does *not* lead to the conclusion that the SCCs are invalid, rather it leads to the conclusion that data transfers should be suspended pursuant to Article IV.

15:23

Then, Judge, at paragraph 64 she sets out her overall conclusions, conclusions which, in my respectful submission, Judge, are apt to engage Article IV.

So, Judge, in my respectful submission, the consequence of all of that, if you look at the Strand 1 comments, which are very short, the Strand 1 comments demonstrate that there *is* no investigation of the other methods of transfer. It's certainly said in large part that Facebook relies on the SCCs, but that in itself as a phrase necessarily means that it has other means by which it achieves transfers. And there is simply no investigation of the primary issue, that's to say the issue that I said was Mr. Schrems' major complaint, the question of compliance with the decisions. Those points, Judge, aren't addressed.

15:23

15:23

15:24

And in my respectful submission, Judge, the consequence of that is that this reference is not necessary, or at least is premature. Because the primary complaint needs to be investigated first. If that complaint is resolved in favour of Mr. Schrems, well, then it follows that there can be no need to seek to invalidate the SCCs. Facebook's particular transfer mechanism

15:24

would have been struck down or prohibited by the DPC, but there can be no question under those circumstances of seeking to invalidate the decisions themselves. That's why I say, Judge, it's unnecessary, or at least premature. 15:24

The same thing applies, Judge, to the failure to investigate the other methods of transfer, the other derogations. Those haven't been examined yet. And it is undesirable, Judge, and I say premature and 15:25 unnecessary that there should be a reference to the CJEU on *this* point when it may well be that there will be other issues lying behind this which in turn may lead to further references to the CJEU. From Mr. Schrems' point view of, Judge, he's already been 15:25 there once. It's now proposed he will go there twice. It follows from what Facebook are saying that there may be other methods which will lead to yet a third reference. And in my respectful submission, Judge, that renders *this* reference, this proposed reference, 15:25 of necessity, at least premature.

The same thing applies, Judge, to the Strand 2 comments. You can see, Judge, that there is simply, on the DPC's part, a conclusion - with which we *don't* 15:25 disagree if it comes to it - that the decisions are invalid. But we say that it couldn't and shouldn't come to it, because we say that Article IV is engaged and that the appropriate response here is to make the

order pursuant to Article IV.

The court was brought to the DPC's affidavit, Judge, and a number of points are made in that as to why that's wrong. In the interests of time, Judge, I'm not 15:26
going to go over the various reasons why Mr. Schrems says that *that's* wrong. But you'll see those reasons analysed, Judge, in our submissions. And you'll find that material, Judge, at book 12, tab one. And at paragraph 54 of those submissions, Judge, each of 15:26
Mr. O'Dwyer's reasons are analysed. He says in his affidavit that there are various reasons why it *wouldn't* be appropriate to rely on Article IV, and each of those is answered there.

15:27

Could I just, I suppose, look very briefly at three of the major points that are raised, both here and in their submissions? It's said first of all, Judge, that the DPC doesn't accept that Article IV is engaged. And I say, Judge, that's wrong, because a close analysis of 15:27
the draft determination makes it clear that the DPC has formed the view that there are requirements of US law that have the effect for which Article IV provides. I can return to this in more detail in due course, Judge, and I don't think I need to do it now. But I say, 15:28
Judge, that the net effect of the findings of the DPC in her draft determination are such as to make it clear that the conditions for Article IV are met.

Secondly, Judge, it's said that, well, it would be disproportionate to make an order under Article IV. And I say, Judge, that's wrong as well. Article IV is there, it should be used, the scheme of the decision is precisely to provide *for* its use. Judge, if you reflect on relative proportionality here, an order made by the DPC under Article IV might have an effect on the transfer of data between the EU and the US - only, of course, insofar as that data is transferred in reliance on the SCCs. But that's the maximum effect that it would have. But the issue that the court is being asked to refer to the CJEU and the preliminary view reached by the DPC will lead to the invalidation of the entire decision, which has a worldwide impact, because the decisions, of course, don't relate to the US only. Unlike Safe Harbour, say, or Privacy Shield, which are specifically EU/US, it's proposed that the *entire* of the SCCs would be struck down. So if you look at relative proportionality, Judge - the SCCs decisions would be struck down - relative proportionality, Judge, in my respectful submission, the proper approach is to do what Mr. Schrems asked the DPC to do.

15:28 15:29 15:29 15:29

Then finally, Judge, it's said that the point *can't* be raised, because it doesn't arise from the draft determination itself. It's said in particular that the Article IV point doesn't arise from the draft determination itself. Well, that's, if you like, circular and self-probative, Judge. It doesn't arise

15:30

from the draft determination only because the DPC didn't put it in, only because the DPC didn't reach a determination on it and didn't put it in as an issue into those in respect of which proceedings were issued before this court. It *cannot* be said, Judge, that it doesn't arise as an issue in the complaint. It quite clearly does. And as I've suggested to the court, the questions of necessity must be determined in the context of the complaint as a whole. 15:30

15:31

You'll have seen in our submissions, Judge, that we say that in fact, on the basis of Article IV, but on that narrow basis only, the SCC decisions *aren't* invalid - I'll just spend one second on that, Judge - precisely because Article IV provides for this safety valve, precisely because Article IV allows for the suspension of data flows under circumstances where the Article IV conditions are met and there are inadequate safeguards. 15:31

MS. JUSTICE COSTELLO: In other words, if you comply with the regime correctly, it's fine. But if you breach it then you'll have to be suspended, is that what -- 15:31

MR. McCULLOUGH: You have to be suspended, Judge, yes. And that is what Article IV provides for. And on that narrow basis, Judge, if we're correct about that, well then we say there's no invalidity in the decisions, precisely because they contemplate exactly the sort of circumstance that is now said to arise. And it can't be correct, Judge, we say, to rely upon 15:31

arguments that could lead validly and should lead validly to the suspension of data flow pursuant to the decision and rely upon those same points to seek to invalidate the decision as a whole.

15:32

If one contemplates an Act, Judge, an Act of the Oireachtas which permitted a judge to make an injunction to restrain a breach of privacy, how could it be said that the Act was invalid because it, if you like, inevitably infringed upon privacy? And that's the essence, Judge, of what has happened here. 15:32

So that's why, Judge, in my respectful submission, we say, Judge, that it's *not* appropriate to make the complaint, it's premature and unnecessary in accordance with the way in which that matter is approached in the European decision. 15:32

I do emphasise, Judge, that notwithstanding that, we agree with everything that the DPC says as to the essential inadequacy of the safeguards that are in place. We say that should lead to Article IV activation. Of course, if I'm wrong about that and it doesn't lead to Article IV activation, well then of course it should lead to the invalidity of the SCCs, and that's the very final position, Judge, that I advocate. But it is, if you like, after each of the other positions that I put forward to the court. And I'm sorry I've taken somewhat more than my half an 15:32 15:33

hour, Judge. May it please the court.

MS. JUSTICE COSTELLO: Thank you.

MR. GALLAGHER: May it please you, Judge. I've a, I think, more structured idea of time than Mr. McCullough -- 15:33

MR. McCULLOUGH: We shall see.

MR. GALLAGHER: -- so I'll try and keep to the time allowed, with maybe just a little bit of latitude.

MR. McCULLOUGH: I see.

MR. GALLAGHER: I've looked at the speaking note, so-called, handed in by Mr. Murphy at twenty five past two on the sixth day of, I think, as long as his original submissions. I can deal with it, but I would ask that we have an opportunity of just putting our response in writing. It should've been part of their submissions. They elected to keep their submissions to initially 10,000, they got an extra thousand. As we were putting them in first and had to set out the position in US law, clearly our submissions were going to take somewhat longer. But I'll move on from that, because whatever assists the court --

MS. JUSTICE COSTELLO: Certainly you can respond to that as you see fit.

MR. GALLAGHER: Thank you, Judge.

MS. JUSTICE COSTELLO: In terms of your timing, to some extent I'll leave it to yourself, but obviously before the -- they have to reply.

MR. GALLAGHER: Oh, yes. And we'll get it in, I'm sure we *won't* leave it to the last minute.

MS. JUSTICE COSTELLO: We don't want too much pressure on Mr. Kieran.

MR. GALLAGHER: No. Thank you, Judge. I'm sure he'll be very grateful for that.

15:34

I suppose just to put this in context, Judge, I'm going to focus on what Mr. Murray, on behalf of the DPC, says and not on what Mr. McCullough says. That's not because I agree with what he says, but I think the time is best utilised in going to the substance. I mean, 15:35
Mr. McCullough's client has made it clear he doesn't want data transferred to the US. It's, of course, his legal entitlement to argue that. The consequences of what he is seeking are quite extraordinary.

15:35

The uncontested evidence before the court in Prof. Meltzer's report, a portion not referred to by Mr. Murray - I make no criticism of it - but if data which he describes as being an *integral* part of trade - it happens to be Facebook that's before the court - but 15:35
he has described the range of entities within the EU that transfer data as an integral part of their trade, including small enterprises transferring to the cloud, people in all sorts of transactions, and Prof. Meltzer says that to prohibit the transfer from the EU would 15:35
lead to an annual reduction in the GDP of the European Union of 0.8 to 1.3% and EU services exports could decline by 4.6 to 6.7. So there are very serious issues involved in this case.

My client is in the position that it is the entity against whom the complaint was made, but the ramifications extend to all of those other entities and many of whom that perhaps don't have different and alternative legal bases to make a transfer, as my client would have. 15:36

The oddity about the claim put forward by the DPC is that her decision ignores some very important issues. And let it be said that Facebook respects the tremendous work that's done by the DPC in protecting the rights of data subjects. Facebook itself, as you will have seen from the affidavits, is an organisation that is fiercely protective of the data which it holds. And that's not only a matter of public record, but outlined in detail in the affidavits. Nevertheless, it finds itself here, unfortunately, disagreeing with the DPC and it does so because the DPC's provisional decision, as it's called, is fundamentally defective in a number of significant respects. 15:37 15:37 15:37

You will have noticed a number of oddities, as I say, about the decision, some of which Mr. Murray has manfully tried to cure retrospectively, including with now addressing really for the first time the issue of national security and its exclusion from the scope of EU law, not in a satisfactory way or in an answer to what we say. But these are matters on which the 15:38

decision is entirely silent. He also sought to address briefly today the interaction between Articles 25 and 26. And you won't find any mention of 26 in the decision, the analysis is based on the Article 25 test.

Perhaps the most significant matter that is expressly omitted from the decision is any consideration of the Privacy Shield. In footnote 22 of the decision, the Data Protection Commissioner says that she has not considered the Privacy Shield because its implementation postdated the decision, the decision being 24th May 2016 and the Privacy Shield being finally introduced in July of 2016, but it was initially announced and circulated in draft form in *February* of 2016. 15:38 15:39 15:39

Mr. Collins, with consummate skill, skirted through the privacy decision and Mr. Murray, with equal skill today, touched on it very briefly. But of course, the one thing that the privacy decision -- or the Privacy Shield, I should say, and more particularly the Adequacy Decision, which forms part of it, says that is of the utmost relevant to this court is that US law does provide adequate protection. And in the second day of the opening, you were treated to a day's analysis of US law and it's alleged deficiencies, supplemented by Mr. Murray's arguments today. But *no* consideration has been given by the DPC to what is the authoritative and actually binding assessment of the 15:39 15:40

adequacy of the protections provided by US law and this court is asked to come to a contrary conclusion.

The Commission began its interaction with the US authorities in early 2014, having previously, in 2013, in its communication to the Parliament identified itself its concerns with the then position under US law. Over a period of two years at the highest level, it engaged in the most detailed interaction with the US authorities and arrived at a very carefully considered conclusion, published in draft form, considered comments on it and then set out in great detail the reason why US law is to be regarded as providing adequate protection. 15:40 15:40

MS. JUSTICE COSTELLO: Can you address me when you come to it as to the distinction that could be made, or if there's no distinction, between the Commission decision in relation to Privacy Shield and the Commission decision in relation to safe harbour? I mean, I understand that they're both binding on national authorities, be it a data protection investigator or a national court, but obviously in **Schrems 1** the Court of Justice says you've got to look at these things anyway. 15:41 15:41

MR. GALLAGHER: Absolutely.

MS. JUSTICE COSTELLO: So I'd like some help in that regard. 15:41

MR. GALLAGHER: Absolutely. And that's a critical decision. You focussed on a very important point and the answer is simply this, Judge: In **Schrems**,

the issue before the Commissioner was the adequacy -- or was the validity of the safe harbour; that's what the court said - just because the safe harbour is there, if a complaint is raised that raises an issue with regard to it then there is a procedure because the Commissioner, or the DPC cannot declare this Commission decision to be invalid, can refer it to Europe. 15:42

But the obvious difference that will have occurred to you and is obvious from the decision is there is no *challenge* here to the Privacy Shield - not by the DPC, not by Mr. Schrems. There is no *complaint* before the DPC which involves any such challenge. And in those circumstances, it's quite clear as a matter of law, and in particular Section 11 of the Data Protection Act as amended, in the context of Article 31 of the directive, that there is a decision that is binding on everybody. 15:42 15:42

But of course, what is even more remarkable in the six days of submissions and in all of the consideration given by the DPC to this matter is that, as I said, the analysis has been done by reference to Article 25 when we're concerned with Article 26, which in its express terms is a derogation; it says "where the adequate protection does not exist", it provides an alternative. And you're treated to an analysis of why there is not adequate protection, which is the Article 25 standard, but nobody on behalf of the DPC says 'Well, actually, the position has changed since we considered this in 15:43 15:43

May 2016, there is now a decision which, even if we are correct with regard to the *standard* that is applicable' - which we say they're not - 'actually is not only relevant, but is decisive'.

15:44

And that leads to just one fundamental matter you raised yourself this morning; there's no necessity to make a reference if something is a moot. And the proper course in this case -- there was no requirement that the decision be issued by 24th May 2015. There was no surprise about the Commission's position with regard to the position under US law. And what should've been done if adequacy of protection was the correct standard was that should've been considered. But what we have instead is a moot; it is asking you to make a reference on the basis of assumed facts, which is the one thing you *cannot* do. And the Supreme Court authority in the **Löffingen** case establishes that, and I'll be opening that to you.

15:44

15:45

15:45

You can't assume facts that are not the case. And this decision does *not* take into account the Adequacy Decision of the Commission in its analysis of the Privacy Shield. And you're being asked to second-guess that.

15:45

The other remarkable feature - and I'll come back to expand on that in a moment - that you'll have noticed is that this is all about the SCC decisions. And they

are actually not dealt with in the decision, they are sidelined on what seems like intuitively at the beginning might seem to be like a valid point that the contracts don't bind the State and, therefore, they're irrelevant. Well, on closer examination, one might ask the question: How does Article 26 of the Directive, which is not challenged, envisage that adequate safeguards - which is the wording of Article 26 - can be provided through contracts? And Article 26(2) and 26(4) *expressly* understand that. The European legislature, in introducing the Directive, didn't think that Facebook or the small/medium sized enterprise or anybody else who is using it is going to ring up the US Government and say 'Enter into a contract so that I can transfer this data'. It was never envisaged as *doing* that. So to say, when an issue arises in relation to it, that you won't consider it because the contract doesn't bind the State raises a very fundamental question. 15:46 15:46 15:47 15:47 15:48

And of course, the answer at its most basic is that this is relevant, this is very important and how could you have a well founded concern about the protections that are available without having looked at it, taken it into account and seen its significance - something that has not been done in the last six days; brief references to it, as if it was of no significance? And it's of the *utmost* significance and provides remedies of a very important type that in some ways go further

than the remedies considered as part of the Privacy Shield in terms of the arbitration model and other models.

Then, of course, as I say, you have, instead of that, what purports to be a conclusion that US law doesn't provide adequate protection - again done by, I say, Article 25. But they don't carry out that exercise by reference to the criteria specified in Article 25(2), or indeed in **Schrems**, as to how you go about that exercise. What they do is they look at the remedies, which is a *novel* methodology - a methodology not adopted by the Commission in the Privacy Shield, not adopted anywhere - but you just look at the remedies, you ignore the substantive law, you ignore practice. Indeed, in **Schrems**, as I will be showing you, the court says the effective means don't have to be the same as the means that exist in Europe, but they have to provide a remedy in practice.

15:48 15:49 15:49 15:49

But the whole practice here has been *completely* dismissed. And you have been told repeatedly that you shouldn't even *look at* the elaborate oversight mechanisms and other protections that exist, even though that's something that the Commission did and is something that is clearly relevant.

15:50

So in short, we say there should be no reference, because the DPC's decision has been overtaken by

events. I say it with sympathy for the position of the DPC, but the decision is deeply flawed as a matter of law and as a matter of methodology and it doesn't *at all* provide a basis on which this court could share any doubt. As you identified, this process is one that is set out in the statute involving the DPC in the first instance taking the particular assessment, or making the particular assessment of the complaint. That's what the statute provides for. 15:50

15:51

And it's important, I think, to remember the context, that this is a complaint made to the DPC on which she has arrived at a provisional conclusion and she asks the court to share that conclusion when her assessment is wrong and it's one that the court should not share. She seeks deference in respect of it. With the greatest of respect, the deference doesn't arise. These are all matters of law and to seek deference with regard to the position under US law, when she acknowledges she has no competence in the area, is a surprising proposition. 15:51 15:51

But really the significance of what the court is being asked to do, under a presentation that presents it as, in a sense, the attractive solution to this; the DPC is defending rights, the court doesn't really have to worry about the difficult issues and doesn't have to really resolve issues of US law, because all you have to do, as Mr. Collins said and Mr. Murray in his eight 15:52

point collusion this morning, having reviewed the materials, all you have to do is share the Commissioner's doubts.

But in fact the consequences of a reference are quite portentous and have enormous implications, casting doubt collaterally on the Privacy Shield, which is to be reviewed *in any event* this July. So that if the alleged deficiencies exist, the Commission, with all its expertise, the input from the working party, input from Parliament, input from everybody will be able to arrive that conclusion. But there is *no way* in which you can make a reference without collaterally animadverting on the Privacy Shield. And that is something this court should *not* engage in. The Privacy Shield is not part of this application. There is no challenge to it. It *cannot* be the subject of a reference. But yet *you're* being asked to make a reference on the basis of doubts as to the adequacy of protection, which of course underlie the Privacy Shield.

And you perceptively asked Mr. Collins last Friday when he was opening Prof. Swire's evidence when Prof. Swire just said there could be implications for other means of data transfer, mentioned the Privacy Shield and other factors. Because while this is an Article 26 case and should've been treated by the DPC as an Article 26 case, she in fact has treated it as an

Article 25 case. The standard she has posited is the adequacy of protection, which is the Article 25 standard and that standard does have implications for other methods of data transfer, including the Privacy Shield.

The other matter that you will have noticed that is missing from the analysis - and it's of considerable significance - is the whole issue of the extent to which national security is within the scope of EU law. And that's important, because Article 4(2) of the TEU expressly excludes it from the scope of EU law. And a number of attempts have been made to answer that point by mischaracterising our submission on it. We do not say that EU law cannot prohibit the transfer of data. That's clear from Articles 25 and 26; you can *only* transfer the data if you're not prohibited, and you're not prohibited if you comply with either or one or the other. So that's *not* the point.

But the point is that when looking at the issues that have been raised by the DPC of the adequacy of protection and the remedies, you cannot leave out of the assessment the fact that what is occurring in the US - and which is objected to - is processing in the context of national security. Article III of the Directive excludes Member States processing for the purpose of national security. So you have an exclusion in the Treaty, which of course is definitive *and* an

exclusion in the Directive. And really what is said is you leave out national security from your analysis entirely. That can't be done and I'll explain and elaborate why.

15:56

And of course, it leads to the fairly absurd position that you cannot transfer data because there is inadequate protection in the US, not because of any inadequate protection in the private sphere - this decision is all about national security - we're not 15:56 told on what basis the national security is *actually* being evaluated by the DPC, but it seems to be evaluated on the basis that somehow the protections in the Data Protection Directive applies - that's unclear - even though those protections don't apply to Member 15:57 States. So in the case of Ireland, in the case of each of the other 27 Member States, the protections in the Data Protection Directive just don't apply to national security processing.

15:57

So Mr. Murray says it's entirely irrelevant what Member States does. Well, it's not and it's a misunderstanding of our point. Firstly, the relevant law that is referred to in the SCC decisions is the applicable data protection law. The applicable data 15:57 protection law is the Member State law. But leave that aside. Is it seriously to be said that you omit entirely from any evaluation of the adequacy of the protection, from any consideration of whether

objectives are well founded that the processing to which objection is made is processing for national security purposes on the basis that sending the data to the US will result in less protection than in Europe and you *ignore* the fact that in Europe there *is* no equivalent protection in *any* of the Member States? 15:58

So you leave it in Europe because of concerns about processing for national security, when the FRA report to which Mr. Robertson refers, but which as you know is a report from -- 15:58

MS. JUSTICE COSTELLO: I haven't read his affidavit.

MR. GALLAGHER: Oh, no, I appreciate that. And I'm only looking at the report at the moment, I'm not commenting on what he says. The report is part of the institutional structure. The FRA fundamental rights agency is a European agency, specifically set up to guide the institutions with regard to fundamental rights. And a consideration of that report would show that actually the level of transparency, the level of legal basis and the variety of protections both under the law and of an oversight nature match anything in Europe and, it's apparent, exceed anything in Europe, but certainly match anything in Europe. 15:58 15:59

So all of that is left out of the consideration. Intuitively, it seems to be wrong and I hope to demonstrate why, legally, it is absolutely and utterly wrong. 15:59

Judge, then it is put that really if you've *any* doubts, you should refer it. That, of course, is not the test; you've to share the well founded concerns, that you consider the concerns are well founded. In fact, 16:00
Advocate General Bot, on whom they rely for so many matters, in the **Schrems** decision referred to having serious doubts. But we would respectfully say that there is *no* basis for having serious doubts or believing that the DPC's concerns are well founded, in 16:00
circumstances where an examination of the decision demonstrates very significant failures on the part of the DPC.

Tomorrow morning I'm going to address the issues to 16:00
assist you and to perhaps put focus on where the disputes between the parties are under the following headings: It *will* be necessary to look at the Directive in a little bit more detail than it's been looked at; the interaction between Articles 25 and 26 are very 16:00
important; the SCC decisions, which as I say, have been largely ignored, ignored by the DPC and largely ignored here; the Privacy Shield itself, to which you have been taken through to a large extent by Mr. Collins, but there are some very important aspects of it; the 16:01
incorrect comparator in terms of apparently assessing it not clearly, but assessing it, it would appear, by reference to rights under the Data Protection Directive; a contention not made by the DPC, but made

in submission that the essence of the right, the data protection rights, have been infringed, so there's no room for anybody to consider a balancing of rights or the necessity of the measures that exist - not something that the DPC concluded and they cannot now, in their submissions, seek to support her decision by recasting her findings and putting them on a different basis.

16:01

And we will take you through then an analysis of the national security exception. As we say, it's not that EU law has no say on this matter, as I say, in relation to the transfer, but it is relevant. And we'll look very briefly at the adequacy of protection under US law - briefly, obviously, because I want to manage my time, but secondly, because in a sense we say you *don't* have to go there because of the Privacy Shield. But not briefly because we accept that there are, even on the DPC's characterisation of the limits to US law, that there is something which, in effect, undermines Article 47 or indeed Articles 7 and 8 when properly understood in context.

16:02

16:02

16:02

So that's the framework and I'll continue with that tomorrow if I may, Judge?

16:03

MS. JUSTICE COSTELLO: Thank you.

MR. O'DWYER: Judge, perhaps just before you rise, can I just ask you about -- you may remember that at the beginning of the case you had indicated that you

might consider whether or not the affidavits submitted by various amici will be admitted. And the reason I mention it is because in our particular case there is not so much an objection, but an application to cross-examine the man, Mr. Butler, or Prof. Butler, who was the deponent in the affidavit, and that would naturally follow, obviously, the expert witnesses. So I'm just wondering could the court indicate, because obviously certainly from our point of view we need to know whether he will in fact be cross-examined -- 16:03

MS. JUSTICE COSTELLO: Well, perhaps after Mr. Gallagher -- I thought we'd agreed there was going to be -- maybe I hadn't --

MR. GALLAGHER: You did.

MR. O'DWYER: I think it was after the openings. 16:03

MS. JUSTICE COSTELLO: After Mr. Gallagher has made his opening remark, then I'll hear the parties' submissions in relation to that matter.

MR. GALLAGHER: Exactly. But I want to make clear one thing. It was made *quite* clear that our position is we object to any evidence from the amici. What we did, because we had to do it to preserve our position pending a resolution of that, is served a notice of cross-examination *entirely* without prejudice to that contention, because, of course, we had to do that. 16:03 16:04

MR. O'DWYER: Of course, yeah, I accept that, Judge. But that will probably be tomorrow, I suppose,

is the --

MS. JUSTICE COSTELLO: I'm hoping Mr. Gallagher will be finished by lunchtime.

MR. GALLAGHER: I will, Judge. I'll certainly do that. 16:04

MS. JUSTICE COSTELLO: So we'll probably start on that point at that stage.

MR. O'DWYER: I'll notify my colleagues that are for the other amici.

MS. JUSTICE COSTELLO: Thank you. 16:04

MR. O'DWYER: Thank you.

THE HEARING WAS THEN ADJOURNED UNTIL FRIDAY, 17TH FEBRUARY AT 11:00

B

C

D

E

F

G

H

J

K

L

N

O

P

Q

R

S

T

U

V

W

Y

Z