THE HIGH COURT - COURT 29

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 TUESDAY, 14th MARCH 2017 - DAY 20

20

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:	MR. RICHARD WOULFE 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:	**FREE LEGAL ADVICE CENTRE** **13 DORSET STREET LOWER** **DUBLIN 1**

INDEX

WITNESS **PAGE**

THE HEARING RESUMED AS FOLLOWS ON TUESDAY, 14TH MARCH 2017

MS. JUSTICE COSTELLO: Good morning.

REGISTRAR: At hearing, Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 11:00

MR. MURRAY: May it please the court.

MS. JUSTICE COSTELLO: Mr. Murray, before you take up where you were on the last day I have a series of questions that I was going to sort put to you, you don't have to answer them now, but if you might get a chance to address them before you finish. 11:00

MR. MURRAY: Certainly, Judge.

MS. JUSTICE COSTELLO: They are not necessarily in any particular order. You were addressing the point that the essence of the right to privacy involved the possibility of notice, knowledge that there could be some limitations if the requirements of national security were still ongoing, but that you said that the possibility at least of notice at some stage was at the essence of it. 11:00 11:01

The US government and all its agencies and laws employ a *"neither confirm nor deny"* approach for the reasons they have outlined and the justification they have in relation to that, the hostile actor, all that sort of stuff; so I am just wondering is it possible then ever to transfer data from the EU to the US, is there an irreconcilable conflict between the principles? 11:01

Then another question was, does the, and it's not a criticism, it's sort of non-loaded question, it may be the implication: Does the DPC's case involve applying a standard to the protection of data in a third country that is higher than that which it enjoys within the European Union because in the European Union you have the exemptions for financial security. 11:02

Then what relevance does the data petitioner attach to the scope of the issues canvassed by the Commission in the Privacy Shield when considering US law. You will have seen that, I think it's paragraphs, recital 65 to 124, deal with all of the various oversight and all sorts of matters. While I understand your point that the Privacy Shield is a limited decision, what exactly would be the status of recital 90 in particular where there seems to be something approaching a conclusion there. And, if it is not binding, is it in some way sort of persuasive in the way that common law courts might understand that term. 11:02 11:02 11:03

And then, sort of a second matter, different matter, when are the limitations or the principles, or what are the principles applicable when a data protection authority is exercising powers under Article 28(3) or are there any principles in relation to that as such or is it wider Charter points? 11:03

I am just wondering, I was trying to tease things out:

When does the Data Protection Commissioner say that the data protections for EU citizens' data is either breached or potentially breached? Because obviously we were focussing on the act of transfer to the US, there's reference to the fact that the data is *accessible* to being surveilled and then a lot of the US evidence has been directed towards protections once it has been surveilled, minimising collection, minimising analysts' approach, minimising dissemination and all that sort of thing and is that relevant to the assessment. 11:04 11:04

(Short pause) I think that's probably sufficient to be going on with.

11:04

SUBMISSION BY MR. MURRAY:

MR. MURRAY: Judge, I'm going to answer all of those now except for question 4, which is the one relating to Article 28, which I think is perhaps best addressed in the context of Article 4 of the SCC decisions because there's an obvious overlap between the two. 11:05

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: In relation to the others, I think I can deal with them relatively briefly but in the course of the today as I come through each of these issues I think I'll be able to elaborate upon them, but can I just give you a headline response now. 11:05

You referred, Judge, to the provision of notice in the context of the essence of the right to privacy. And, while that is not incorrect, it is actually the essence of the right to a judicial remedy under Article 47 which is the one that is engaged by the provision as to notice. Now, that is not just a semantic distinction, because it does go to the focus of the Commissioner's decision. 11:05

And insofar as you say 'well in the US they don't give notice, they neither confirm nor deny', does that mean that there has been a breach of the right, and the answer to that lies in what I have just said. If you frame it in terms of Article 47, I believe the answer is *not necessarily*. Because if you have a standing rule which accommodates the person who does not know, then that mitigates the absence of notice. But what is, in our respectful submission, absolutely and clearly contrary to the scheme envisaged by the Charter is what the US has which is a rule of *never* notifying. 11:06 11:06

You will recall that even Prof. Swire in his 2004 paper at page 98 recommended a reconsideration of the absolute rule of non-notification; in other words, what the court in **Watson** said was that you've a right to be notified at the point where the investigation is no longer prejudiced by notification. 11:07

MS. JUSTICE COSTELLO: Hmm.

MR. MURRAY: The formulation of that is significant

because it is actually, it's not a test that's subject to proportionality, it is a test that has proportionality built into it, but in the US there's an absolute blanket rule. And that is, in our respectful submission, inconsistent with the requirements of the Charter. 11:07

So it can be mitigated in one of two ways: Either not the absolute rule, and it is an absolute rule, or a relaxation of the standards such as standing. And can I just make one point because this picks up on something that was suggested but not, I think, developed by Ms. Barrington which was that there was some constitutional preclusion under Article 3 of the federal constitution, some constitutional rule that would prevent Congress from broadening standing. And I would just remind you that Prof. Vladeck in his writings and in his evidence had explained why that, in his opinion, is not correct. 11:08 11:08

Judge, the second issue which you raised was the standard to apply to data in a third country in a context where the domestic rules have a preclusion for national security.

MS. JUSTICE COSTELLO: But what I meant was in here, within the EU -- 11:09

MR. MURRAY: Hmm.

MS. JUSTICE COSTELLO: -- obviously national security is an exception to the Directive, so you can have national

security, it's supervised to an extent by the CJEU, but you have that exception for national security.

MR. MURRAY: Yes. But in our respectful submission, and this was the point in the two extracts at pages 10 and 11 from the FRA Report which I opened to you on Friday, page 10 their own view by reference to the **ZZ** decision and page 11 quoting Mr. Anderson in his report, there is and there remains a review power, deriving we would say from the Charter, for the use of data in the context of national security within the Union. Both of those statements were clear and unequivocal. 11:09 11:09

So you can't produce the trump card, and you are absolutely right when you refer to the derogation under the Directive, Article 3(2), but you cannot produce the trump card of national security and say 'sorry, this is the end, we don't have to comply now with Article 47, we don't have to comply with the basic principles derived by the court from the Charter'. 11:10 11:10

And, in any event, that in our respectful submission, and this is a theme that we develop somewhat in the speaking note which I handed in at the conclusion of my own opening; the fact of the matter is, if that is what the position is, well that is what the position is. 11:10

MS. JUSTICE COSTELLO: Hmm.

MR. MURRAY: The Member States are members of the Union, they are bound by the European Convention of

Human Rights, they have their own set of supervision and controls and if the position is that the United States is held in this context to a different standard so be it, that appears to be the corollary of the case law. But, for the reason I have just alluded to, I don't believe that that is correct. 11:11

MS. JUSTICE COSTELLO: It's not as stark as might have been posited?

MR. MURRAY: I don't know. Well, it is certainly not. I mean Facebook rely upon the FRA Report for *everything* -- 11:11

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: -- but it seems disagree with this conclusion, the one on pages 10 and 11 which I opened to you yesterday. They rely on Prof. Brown's report as the standard in terms of its analysis of the law of the Member States, but don't appear to rely upon his conclusion that notification is a mandatory aspect of the European Convention of Human Rights or his conclusion, immediately after the sentence that you would recall Prof. Swire quoted 12 times in his report, that the US falls below the standard set by the Convention. 11:11

You finally, I think, asked me, Judge, in reference to the status of the Commission's observations in the course of Privacy Shield regarding, I suppose, extraneous matters, and you referred to paragraph 90. And I am actually just going to come to Privacy Shield 11:11

now so it occurs to me that may be a useful point at which to examine that and can I ask you to look, Judge, at Tab 13.

Your question, I think, is in part answered by the second of two aspects of Privacy Shield which I am going to emphasise as I go through the decision. The first, to which you alluded, Judge, a few moments ago is of course: *"Privacy Shield is not a decision that the US law is adequate, Privacy Shield is a decision that Privacy Shield is adequate"*. 11:12 11:12

And the second, Judge, is that, I think when you look and consider very carefully what the Commission said about Privacy Shield, that it becomes apparent that US law, and in particular the remedial deficiencies in US law, were saved by the Ombudsman. And we will see this in particular in that sequence of paragraphs in the recital running from 115 to 124 where it, I think, is obvious that the Commission identifies a number of significant deficiencies in the remedial régime in the United States, very similar as it happens to those which feature in the Commissioner's report, Draft Decision, and then proceeds to immediately address the Ombudsman in a context which I think makes it clear that the Ombudsman is being introduced to address those deficiencies. And of course that's key because the Ombudsman comes out, then it means that the finding of adequacy, well it's not a finding of adequacy of US law 11:13 11:13

at all.

Just then, Judge, to go very quickly through it. I referred you but I don't think opened the title --

MS. JUSTICE COSTELLO: Hmm. 11:14

MR. MURRAY: -- of the decision. But it is of course a decision on the adequacy of the protection provided by the Privacy Shield. Nothing else. And if you turn then, Judge, to recital 12 where, and this is on page L2073. 11:14

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: *"In 2014 the Commission entered into talks with the US authorities to discuss the strengthening of the Safe Harbour scheme in line with the 13 recommendations contained in Communication 847. After* 11:14 *the judgment of the Court of Justice of the European Union in the Schrems case, these talks were intensified, with a view to a possible new adequacy decision which would meet the requirements of Article 25."* 11:15

But this is important: "*The documents which are annexed to this decision and which will also be published in the US Federal Register are the result of these discussions. The privacy principles, together* 11:15 *with the official representations and the commitments by various US authorities contained in the documents in annexes I and III to VII constitute the Privacy Shield."*

So that is what is being found to be adequate. And it really is a source of some surprise, to put it mildly, that such emphasis is placed on this and it is presented to you as it has been as a decision of *adequacy* of US law, but this is only adequate in a finding of adequacy in relation to the shield and it only applies to data which is transferred under the shield.

11:15

We'll see this again when we look at the actual decision where the decision makes it clear that there's data that's transferred under the shield and data that isn't and Facebook, as we know, transfers two categories of data under the shield but for at least some other purposes relies upon the SCCs.

11:15

11:16

If you look then, Judge, at recital 13:

"*The Commission carefully analysed US law and practice, including these official representations. Based on the finds developed in recitals 136 to 140, the Commission concludes the US ensures an adequate level of protection for personal data transferred under the shield.*"

11:16

11:16

So again you see that phrase. What the finding relates to is information transferred under the shield *"from the Union to self-certified organisations in the United States"*. And, Judge, and we'll see this later, just

again to emphasise: When the bodies certify, they certify the data which they are going to be transferring under the shield. It is, as it were, data specific.

11:17

If you look then, Judge, to recital 16: "*The protection afforded to personal data by the Privacy Shield applies to any EU data subject whose personal data have been transferred from the Union to organisations in the US that have [self] certified their adherence to the principles with the Department of Commerce.*" 11:17

And then from paragraphs 19, and I won't open them but just to flag them, to 29, the principles are outlined. You can see what they are and they are an inherent part of the shield and, therefore, an inherent part of what has been found to be adequate. Paragraphs 30 to 37 deal with oversight and can I just draw your attention in passing, as it were, to recital 33, just to pick up on a point that I'm going to be coming back to later, it will save me opening it. There are three references to the SCCs in the entirety of the Privacy Shield and one of them is recital 33. 11:17

11:18

"*Organisations that have persistently failed to comply with the principles will be removed from the shield and must return or delete the personal data received under the shield. In other cases of removal, such as*

voluntary withdrawal from participation or failure to recertify, the organisation may retain such data if it affirms to the Department of Commerce on an annual basis its commitment to continue to apply the Principles or provides adequate protection for the personal data by another authorised means, (for example by using a contract that fully reflects the requirement of the relevant standard contractual clauses)."

And I'm going to gather together the three references when I look at this aspect of it later but just to observe that's one of the three references to the SCCs. 11:18

Then, Judge, at paragraphs 38 - sorry, recitals 38 to 63, deal with redress and can I ask you to turn to recital 64. I will just emphasise these three paragraphs because they underscore an arresting incongruity in Facebook's case. Because on the one hand they tell you national security is off limits, national security in Article 4(2) includes the national security of the United States and, even if it doesn't, there's no comparator and so forth. But of course, if that were correct, what business has the Commission involving itself in a consideration of US national security at all, but it is absolutely clear from these paragraphs that that is exactly what it is doing. 11:18 11:19 11:19

Paragraphs 64: "*As follows from Annex II, adherence to the Principle is limited to the extent necessary to*

meet national security, public interest or law enforcement requirements.

65. The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its ODNI has provided the Commission with detailed representations and commitments contained in the Appendix VI. By letter signed by the Secretary of State, Annex III, the US government has committed to create a new oversight mechanism for national security interference, the Ombudsman, who is independent from the intelligence community." 11:20 11:20

And then a representation from the Department of Justice is contained in Annex VII. And at recital 66 it records: 11:20

"*The findings of the Commission on the limitations on access and use of personal data transferred from the EU to the United States by US public authorities and the existence of effective legal protection are further elaborated below."* 11:20

Then, Judge, in those following paragraphs there is a consideration of various aspects of the substantive

law. And it proceeds at paragraph 90, and maybe I should refer you to paragraph 88 first or recital 88, it says:

"*On the basis of all of the above, the Commission concludes that there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of persons whose personal data are transferred from the Union to the United States under the US EU Privacy Shield.*" 11:21 11:21

So this, as with all of these paragraphs, is not proposing a general clean, well a general finding of adequacy on US law, it is concerned with what US law plus the various protections provided for under the Privacy Shield achieve. 11:21

And that I think, Judge, is the context in which the paragraph that you observed, which is paragraph 90, falls to be seen. Because paragraph 89 says: 11:21

"*As the above analysis has shown, US law ensures surveillance measures will only be employed to obtain foreign intelligence information – which is a legitimate policy objective – and be tailored as much as possible. In particular, bulk collection will only be authorised exceptionally where targeted collection is not feasible, and will be accompanied by additional* 11:22

safeguards."

And then in 90: "*In the Commission's assessment this confirms that the standard set out by the Court of Justice in* ***Schrems****, according to which legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must impose 'minimum safeguards' and 'is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all of the personal data of all of the persons whose data has been transferred from the EU to the US without differentiation, limitation or exemption being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference with both access to that data and its use entail'."* 11:22

And that's a reference to paragraph 93 in **Schrems**:

"*Neither will there be unlimited collection and storage of data of all persons without any limitations, nor unlimited access. Moreover, the representations provided to the Commission, including the assurance that U.S. signals intelligence activities touch only a fraction of the communications traversing the internet,*

exclude that there would be access 'on a generalised basis' to the content of the electronic communications."

Then, Judge, and this in my respectful submission is what is critical for the purposes of the findings by the DPC, we have this build-up, as it were, through the recitals and the consideration of US law and the consideration of the representations made by the government and the consideration of the privacy principles. There is consideration of oversight in the following paragraphs and then at paragraph 115 the Commission turns to the *specific* issue with which the court is concerned and the specific issue with which the Commissioner was concerned, namely remedies. 11:23 11:23 11:24

You have seen its consideration of the substantive law and the protections but now, and that is the context in which paragraph 90 to which you referred falls to be considered, but now you move to remedies. And what the Commission says about that, in our respectful submission, is significant, both as to the content of its comments and how it believed they could be resolved. 11:24 11:24

So there's reference made, Judge, up to paragraph 115 in the various pieces of legislation to which you have seen reference already made, including the Administrative Procedure Act. And then at paragraph

115 they say this:

"*While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been subject of unlawful electronic surveillance for national security purposes, it is equally clear that at least some legal bases that US intelligence authorities may use are not covered.*" 11:24

This is the first problem and this is 12333: 11:25

"*Moreover, even where judicial redress possibilities in principle do exist for non-US persons, such as for surveillance under FISA, the available causes of action are limited and claims brought by individuals (including US persons) will be declared inadmissible where they cannot show 'standing', which restricts access to the ordinary courts.*" 11:25

So if you just take that paragraph and I'm going to ask you to look at the footnotes which are attached to it because they identify what the Commission obviously sees as significant limitations on the remedial scheme provided for in US law. 11:25

And the footnotes then refer you, actually footnote 168 which is referable to the preceding paragraph is of interest because it kind of records that: 11:25

"*The individual will normally only receive a standard reply by which the agency declines to either confirm or deny the existence of records.*"

Referring to ACLU. Then in footnote 169, the ODNI representations are recorded in appendix or Annex VI: "*According to the explanations provided, the available causes of action either require the existence of damage.*" 11:26

So this is one limitation, and this is derived from what the US authorities have told them: "*Or a showing that the government intends to use or disclose information obtained or derived from electronic surveillance of the person concerned against that person in judicial or administrative proceedings in the US.*" 11:26

So essentially you either have to prove damage, and we know from **FAA -v- Cooper** what that means, or you have to be in a situation where this evidence is being adduced against you. Now those complaints or concerns will be familiar with you, Judge, from the evidence. 11:26

And the Commission goes further because it identifies how that does *not* align with the protections provided under EU law because it says: 11:27

"*As the Court of Justice has repeatedly stressed, to*

establish the existence of an interference with the fundamental right to privacy, it does not matter whether the person concerned has suffered any adverse consequences on account of that interference."

11:27

And this is paragraph 89 of **Schrems** which of course has been referred to you on many occasions.

So there is one significant remedial deficiency in EU law identified - sorry, in US law when compared with EU law identified by the Commission. And then, Judge, they explain in paragraph 171 that the admissibility criterion stems from the case or --

11:27

MS. JUSTICE COSTELLO: You mean footnote.

MR. MURRAY: I am sorry, footnote 170.

11:27

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: So the admissibility criterion, that is standing, derives from Article III.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: Case or controversy and we have seen Prof. Vladeck's view that Congress can expand that. And then 171, Judge, is **Clapper**:

11:28

"*As regards the use of NSLs, the USA Freedom Act provides that non-disclosure requirements must be periodically reviewed, and that recipients of NSLs be notified when the facts no longer support a non-disclosure requirement. However, this does not ensure that the EU data subject will be informed that*

11:28

he or she has been the target of an investigation."

So in this short paragraph the Commission identifies many of the deficiencies which the Data Protection Commissioner is concerned about and which prompt her to bring this application which she identifies in her decision and have been elaborated upon in particular by Mr. Serwin. 11:28

Then you see how the Ombudsman comes in, and it is obvious that the Ombudsman is introduced to address *those* deficiencies; in other words, without the Ombudsman those remedial deficiencies would stand. So what it says at paragraph, footnote, recital 116: "*In order to provide for an additional redress avenue*", and sorry, we are out of the footnotes, Judge -- 11:29 11:29

MS. JUSTICE COSTELLO: The recitals, yes.

MR. MURRAY: -- into the recitals: "*In order to provide for an additional redress avenue accessible for all EU data subjects, the US government has decided to create a new Ombudsperson mechanism as set out in the letter from the US Secretary of State to the Commission contained in Annex III to this decision. This mechanism builds on the designation under PD28 of a senior coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond this the original concept.* 11:29 11:29

117. In particular, according to the commitments from the US government, the Ombudsperson mechanism will ensure that individual complaints are properly investigated and addressed."

11:30

And when you ask the question why is this Ombudsperson being put in place, what is the reason for it and why is the Commission elaborating upon it, in context it is absolutely clear it is being put in place to identify the constraints arising from the combination of the standing rule and the rules regarding the necessity for the proof of damage to sue.

11:30

"*Will ensure that individual complaints are properly investigated and addressed, and that individuals receive independent confirmation that US laws have been complied with or, in the case of a violation of such laws, the non-compliance has been remedied. The mechanism includes the 'Privacy Shield Ombudsman', the Under-Secretary and further staff as well as oversight bodies competent to oversee the different elements of the Intelligence Community on whose cooperation the Privacy Shield Ombudsperson will rely in dealing with complaints. In particular, where an individual's request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to rely on independent oversight bodies with investigatory powers, (such as the Inspector-Generals or the PCLOB). In each case the Secretary of State*

11:30

ensures that the Ombudsperson will have the means to ensure that its response to individual requests is based on all the necessary information.

118. Through this 'composite structure', the Ombudsperson Mechanism guarantees independent oversight and individual redress." 11:31

So it is this individual redress provided by the Ombudsman which addresses the concerns previously identified by the Commission: *"Moreover, the cooperation with other oversight bodies ensures access to the necessary expertise. Finally, by imposing an obligation on the Privacy Shield Ombudsperson to confirm compliance or remediation of any non-compliance, the mechanism reflects a commitment from the US government as a whole to address and resolve complaints from EU individuals."* 11:31 11:31

So it proceeds, Judge, to address aspects of the Ombudsman, it records that he will be independent from the intelligence community, and these have been opened to me and I won't repeat them, but I do want to take you to recital 122 -- 11:31

MS. JUSTICE COSTELLO: Mm hmm. 11:32

MR. MURRAY: -- as the conclusion reached by the Commission regarding the Ombudsperson:

"*Overall this mechanism ensures that individual*

complaints will be thoroughly investigated and resolved, and that at least in the field of surveillance this will involve independent oversight bodies with the necessary expertise and investigatory powers and an Ombudsperson that will be able to carry out its functions free from improper, in particular political influence. Moreover, individuals will be able to bring complaints without having to demonstrate, or just to provide indications, that they have been the object of surveillance." 11:32

So just stop there. That sentence tells you exactly what it is the Commission was concerned about, that the problem that we have been discussing arising from US standing rules and the combination of those and the absence of any obligation to notify is now being, in the commission's view, addressed: "*In the light of those features, the Commission is satisfied there are adequate and effective guarantees against abuse.*" 11:32 11:33

And then the decision, Judge, recitals 123 and 124:

"*On the basis of all of the above - and that obviously includes the Ombudsman - the Commission concludes 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 shield.* 11:33

*124. In this respect, the Commission takes note of the Court of Justice's judgment in the **Schrems** case according to which 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection as enshrined in Article 47'."*

11:33

11:34

So the Commission now has identified the very point which the DPC has been concerned about and its conclusion is this: *"The Commission's assessment has confirmed that such legal remedies are provided for in the US, including through the introduction of the Ombudsperson mechanism. The Ombudsperson mechanism provides for independent oversight with investigatory powers. In the framework of the Commission's continuous monitoring of the Privacy Shield, including through the annual joint review which shall also involve the Ombudsperson, the effectiveness of this mechanism will be reassessed."*

11:34

11:34

Now, Judge, what that means is the following: It means that the Commission has made a finding that the Privacy Shield is adequate and, if you are transferring your information under the Privacy Shield, fine. It would appear, and again I'm at pains to emphasise that my client's position is that, although the matter is not

11:34

entirely clear, that the SCCs have the Ombudsperson superimposed upon them and I will show in a moment where that comes from.

So, what there is is a finding that the whole of the Privacy Shield provides an adequate remedial basis, only the Ombudsperson is transferred over to SCCs, but if the Ombudsperson is *not* an adequate remedy, if the Commission is wrong in concluding that it is an Article 47 compliant remedy that meets the requirements of **Schrems**, well then there is, and I would respectfully submit the Commission decision supports the proposition that there is, no adequate remedy for the purpose of Article 47 in the United States. 11:35 11:35 11:36

And, for the reasons that I alluded to on Friday and to which I will return later, there are legitimate concerns and issues around the Ombudsperson.

MS. JUSTICE COSTELLO: Hmm.

MR. MURRAY: So, if anything, Judge, when one looks closely and carefully at the analysis of the Commission, insofar as the issues that we have brought to the court are concerned, if anything they support the concerns which we agitate, in my submission. 11:36 11:36

Judge, can I ask you to go to the decision itself because, as has been pointed out, the decision gets lost in the undergrowth of the recitals, it's at page 35, L207-35.

MS. JUSTICE COSTELLO: I have it, thank you.
MR. MURRAY: So this just emphasises this concept of transferring data under the Privacy Shield. So do you see Article 1: "*For the purpose of Article 25(2), the United States ensures an adequate level of protection of personal data transferred from the Union to organisations in the United States under the EU Privacy Shield.*" 11:37

So there it is in the clearest terms in the decision itself, the finding of adequacy is only to information transferred under the shield. 11:37

2. The EU-US Privacy Shield is constituted by the principles issued by the US Department of Commerce on 7th and the official representations and commitments contained in the documents listed in Annexes I, III to VII." 11:37

So that's what the shield is. 11:37
MS. JUSTICE COSTELLO: Mm hmm.
MR. MURRAY: And I'm going to just look at some extracts of that in a moment and then, thirdly:

"*For the purposes of paragraph 1, personal data are transferred under the shield where they are transferred from the Union to organisations in the United States that are included in the 'Privacy Shield list', maintained and made publically available by the* 11:37

Department of Commerce, in accordance with sections I and III of the principles."

And what that means is that, insofar as you have signed up to the shield and self-certified for the purposes of particular data, then the transfer of that data enjoys the benefit of his Adequacy Decision. And just to show you where you find that in terms of categories of information, if you turn to page 41. 11:38

MS. JUSTICE COSTELLO: Yes. 11:38

MR. MURRAY: You'll see, and this is dealing with the certification, page 41:

"*Verify self-certification requirements - prior to finalising an organisation's self-certification (or annual re-certification) and placing an organisation on the Privacy Shield List, verify that the organisation has: Provided required organisational contact information; described the activities of the organisation with respect to personal information; and indicated what personal information is covered by its self-certification.*" 11:38 11:39

So you actually identify the categories of data so certified. 11:39

And if you go forward to page 49, paragraph 6, you'll see:

"*Organisations are obligated to apply the principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. An organisation that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of employment relationship must indicate this when it self-certifies.*"

And, if you just go over the page, again you'll see it is data specific at the top of the page, an organisation has to inform individuals about and No. iii: "*Its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield.*" 11:39 11:40

And if you go forward to page 56, again you see this phrase an organisation in (f), I am terribly sorry.

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: Page 56(f): "*An organisation must subject to the Privacy Shield principles all personal data received by the EU in reliance on the Privacy Shield. The undertaking to adhere to the Privacy Shield principles is not time limited in respect of personal data received during the period in which the organization enjoys the benefits of the Privacy Shield. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it* 11:40

subsequently leaves the Privacy Shield for any reason. An organization that withdraws from the Privacy Shield but wants to retain such data must affirm to the Department on an annual basis its commitment to continue to apply the Principles or provide 'adequate' protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the SCCs."

And that's the second reference, Judge, to the SCCs. 11:41
And if you go forward to page 72, which is perhaps the clearest reference to the SCCs, in the fourth paragraph on that page.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: "*This memorandum describes a new mechanism* 11:41 *that the Senior Coordinator will follow to facilitate the process of requests relating to national security access to data transmitted from the EU to the US pursuant to the Privacy Shield, standard contractual clauses, binding corporate rules, derogations."* 11:41

And that is the legal basis, it would appear, and it seems the sole legal basis on which the Ombudsman applies to the SCCs. There isn't an amendment to the SCC decision or indeed any express reference in the 11:42 Privacy Shield decision except in recital 33. So it's a little bit unclear, but I think I have already explained to you my client's position on it.

So what that means, Judge, is, if, I can respectfully so submit, Privacy Shield applies only to Privacy Shield, it applies only to data transferred in reliance on Privacy Shield. The Adequacy Decision, therefore, does not and cannot bind the court or anyone else in relation to an assessment of the validity of the SCCs. We do raise an issue, as we are entitled to for the reasons I explained on Friday afternoon, as regards the Ombudsperson. If we're right in that it may have implications for the Privacy Shield decision, we're not challenging the Privacy Shield decision. 11:42 11:42

And in my submission when you look closely at those paragraphs, 115 and following of the recitals, the analysis conducted by the Commission actually supports the analysis which the Commissioner, which my client has reached to the extent that it is quite clear that the Ombudsman is introduced to plug the very significant gaps which we have identified. 11:43

So, that is what I have to say, Judge, about the Privacy Shield.

MR. GALLAGHER: Judge, I am very loathe to interrupt but there is a point I want to make. It does appear as if the DPC is raising a new issue now that was never canvassed in opening and it's this: Mr. Murray lays a lot of emphasis on the fact that the Commission decision refers to the Privacy Shield and adequacy in that context, implying that the findings with regard to 11:43

national security law and the redress provisions, including the Ombudsman person, are not findings as to adequacy in relation to that sphere and that the Adequacy Decision is solely conditioned on the signing up to the Privacy Shield. 11:44

Now, that was never made as part of their case. If I have misunderstood the case he is now making I will sit down, but that is of some importance, Judge. Because you will remember the Privacy Shield documents 11:44 and assessments are divided in two. The first relates to what I call the private sphere where you sign up to the principles and the second, beginning on page 13, relates to the public sphere. Both are assessed separately. No issue has ever been made by the DPC 11:44 about the adequacy of the SCC clauses in relation to the private sphere.

So the only part of the Privacy Shield decision that is relevant to the issue before you is that that relates 11:45 to the public sphere, the finding of strictly necessary, and the finding of adequacy of remedies, including the Ombudsperson. And if the DPC is now contending, which I said was never contended in the submissions, never contended in Mr. Collins' opening, 11:45 that the Privacy Shield adequacy finding is only binding on this court and is only relevant to this court where somebody is transferring under the Privacy Shield, they are not entitled to make that case now.

That is a conflation of two different strands of the Privacy Shield and that is very important.

MR. MURRAY: Well, Judge --

MS. JUSTICE COSTELLO: Just a moment, just before Mr. Murray. As I understood it, and I haven't looked at the pleadings for what seems like a long while at this stage. 11:45

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: The Privacy Shield wasn't initially part of the Plaintiff's case at all for obvious reasons. 11:45

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: It emerged by way of defence.

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: And then it was responded to in reply, we rely on it for its full force, meaning and effect. 11:46

MR. GALLAGHER: Exactly.

MS. JUSTICE COSTELLO: So it is not really the case that it's your defence and they are responding to it rather than her case. Now maybe I have misunderstood this. 11:46

MR. GALLAGHER: Well, except they said they would rely on it for its full meaning and effect. Mr. Collins referred to it in the opening, he could have left it to the defence. 11:46

MS. JUSTICE COSTELLO: Well, I think to be fair to him in his opening he did say that he was also going to open the positions advanced by the other parties, if

I can to put it that way as well.

MR. GALLAGHER: Yes. Oh, I make no criticism of him, but it is part, they said they would rely on it for full force and effect. If they are now contending that the Privacy Shield isn't relevant or doesn't constitute a finding as to adequacy because Facebook has not signed up to the Privacy Shield. 11:46

MR. MURRAY: I didn't say that.

MR. GALLAGHER: Well, sorry, excuse me.

MS. JUSTICE COSTELLO: No, what he said was that it's a finding of adequacy in a limited scope. 11:47

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: Just as, for example, you were arguing that the **Schrems** decision is limited because it doesn't define that US law is inadequate, it only finds that the decision of the Commission failed to address those issues and therefore it was invalid. So he has said that it's a narrow decision and therefore it's not, because I had asked was it binding upon the court. 11:47

MR. GALLAGHER: Yes. 11:47

MS. JUSTICE COSTELLO: And...

MR. GALLAGHER: And he seems to be saying now, that's why I said at the very beginning if I have misunderstood the position I will happily sit down, but he does seem to be saying that the finding of adequacy, and he drew your attention to the Articles of the decision, is in the context of signing up to the Privacy Shield, but that ignores the fact that the Commission's analysis examines two strands. It 11:47

examines what I have called the private transfer where you must sign up to the principles.

MS. JUSTICE COSTELLO: Mm hmm.

MR. GALLAGHER: And, separately from page 13 on, the transfer in the context of the national security sphere. 11:47

MS. JUSTICE COSTELLO: Mm hmm.

MR. GALLAGHER: In respect of both it finds adequacy. There has never been any suggestion that the protections in the private sphere that are provided by the SCCs are in any way inadequate. That has never been suggested, they were never even looked at and therefore the only part of the Privacy Shield decision that is relevant to the court's examination of the issue in this case, national surveillance, is the analysis that relates to that issue and, separately, in relation to that issue, the Commission finds that the protections, including the redress which does involve the Ombudsperson, is adequate and that is the effect of -- 11:48 11:48

MS. JUSTICE COSTELLO: Well, just a moment, can you show me where that is? I know this is somewhat interfering with your reply.

MR. MURRAY: Well it is, Judge, and I think it is very unfair. Nobody interrupted Mr. Gallagher or Ms. Hyland when they were addressing the court making their submissions and I think it is very, very wrong for Mr. Gallagher to have stood up and interrupted my reply. If he wants to make a point at the conclusion 11:48

he can do so, but this is an attempt by him to make submissions in the middle of my reply and I have to say, Judge, it should be deprecated.

MS. JUSTICE COSTELLO: Well, Mr. Gallagher, I will park that argument in relation to it. 11:49

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: But I mean it did see that, and I know because I have got your marks on it as well as Mr. Collins' marks, that my attention was drawn to the actual decision itself which on its face says that *"the personal data transferred from the Union to organisations in the United States under the Privacy Shield"*, so it has to be under the whole lot, you can't go under a half a leg. 11:49

MR. GALLAGHER: Yes. That is true, Judge. Sorry, I don't, I can understand Mr. Murray objecting, I don't agree with his criticisms and I deliberately didn't want to interrupt his presentation and that's why I allowed him finish that particular point. 11:49

But, Judge, the examination involves the two strands. There has never been any suggestion in the DPC's decision that in the private sphere the SCCs are inadequate; therefore, the aspect of the Privacy Shield that is relevant is its analysis of adequacy in the context of the public sphere. 11:50

MS. JUSTICE COSTELLO: Well, I will consider your point, but I'm not too sure that it is well raised, but I will consider it because I do think that they did

reserve their case to say full force meaning and effect. But I will look back at the pleadings and stuff because it was a case that it was part of your case that they were responding to, not the case as originally brought. But I will look at it and I will re-read the opening carefully with that comment in mind.

MR. GALLAGHER: Thank you.

MS. JUSTICE COSTELLO: That observation in mind.

MR. MURRAY: And you will recall that I interrupted Mr. Gallagher while he raised this issue in his opening observing that there were questions around what was in his submissions and pleadings. No issue arises in relation to whether things are pleaded or not or in submissions, we're not making that point. It's in that context that I now analyse it, and the decision, Judge, speaks for itself. 11:50

Now, I want to move on, Judge, to the fourth item on the list I handed you on Friday which is US law and what findings you should make in relation to that. Just perhaps to begin by making some comments about the evidence you have heard. 11:51

Obviously, Judge, it will be a matter for the court to reach the conclusions it reaches regarding the expert witnesses, and I don't want to say too much about any particular witness or the factors the court may bring to bear on its assessment of their credibility, but 11:51

I will say this about Prof. Swire. In my respectful submission Prof. Swire was not in a position to assist the court on the critical issues with which it was concerned. His report contained a *fundamental* error in his explanation of US constitutional law insofar as it applied to non-US persons, which of course is what we were about, it was at the heart of the case. He was not, in my respectful submission, in a position to provide any explanation as to how he had made that error. He cited a case as authority for the proposition which it simply did not sustain, and I understood him to accept that, eventually, in his evidence. 11:52 11:52

He adhered on oath doggedly to an interpretation of the Supreme Court decision in **Clapper**, which anybody who had been in the court for the preceding ten days would have known was untenable and which he retracted only when asked to read out the wording of the Supreme Court judgment itself. 11:52

He didn't read the **Spokeo** case because it was in his inbox, even though it was an Article III case concerned with standing in data protection cases. His report was 146,500 words long, 310 pages, produced in a very short period of time with the assistance of a large number of other people, a fact which was not disclosed in the report itself. 11:53

I would surge you to look at the corrections that the US government helpfully made to Prof. Swire rescuing him from further cross-examination in the course of the his evidence as regards errors that he had made in his report. In my respectful submission I would ask you to 11:53
bear those comments in mind as you consider Prof. Swire's evidence.

Prof. Vladeck's report was, perhaps somewhat unusually, not one where he was asked to express his opinion per 11:54
se on the issues, but effectively, as I understood his evidence, to do a critique of the DPC decision, and that may be why he didn't state in his report what his views actually were as recorded elsewhere regarding the efficacy of the House Intelligence Committee. We also 11:54
know, as with all but one of the other Facebook witnesses, that Prof. Vladeck's report was also the subject of comment by the US government, although we do not know what that comment was.

11:54

There is a criticism made of Mr. Serwin insofar as it is said he wasn't a national security expert. He was, Judge, an expert in cyber security and privacy litigation and enforcement. He's the author of a work on information security and privacy, he was well placed 11:54
to give evidence regarding the actual issue, namely the remedial scheme in place in the United States.

And just one point of detail, Judge, well actually two

points of detail, none of which are of any significance but just to observe them so the court isn't - they are not corrected. It was put to Mr. Serwin on a number of occasions that he was the only US law witness or person consulted by the Commissioner and that's correct, and 11:55
he confirmed that that was correct. But it should be noted, Judge, that, when you look at the DPC decision, the Commissioner records the fact that she had regard to a number of documents, including the European Commission November 2013 Working Group Report, the 11:55
Commission Report on the Functioning of the Safe Harbour, the communication from the Commission to the Parliament and Council of February 2016 and of course she is also a member of the Article 29 Working Group which has obviously been concerned in this issue for 11:55
some time. And those documents variously make references to US law.

MS. JUSTICE COSTELLO: They are recited in the Draft Decision.

MR. MURRAY: They are in the decision, just to observe 11:56
that.

And the other point again of detail which I think is inconsequential is just to say, it was said on a number of occasions that Prof. Richards had prepared his 11:56
report with the benefit of assistance. He didn't. He never said he did. He was asked a question by Mr. Gallagher, a sort of rolled-up question which referred to his assistance. He answered the question,

he didn't say 'I don't have assistance', but he certainly didn't ever say that he did. That again is a point of detail.

All of that said, Judge, and putting the assessment of the witnesses to one side, which is of course a matter for the court, I think, and I think this is in particular the case when you look at the second day of Prof. Vladeck's evidence, I think that there perhaps isn't a huge amount between the parties in terms of what US law says or doesn't say. You'll see on Day 13 page 43 that Prof. Vladeck's disagreement - sorry, the comments Prof. Vladeck had to make on Mr. Serwin's report and the DPC decision were this: He had eight points in his report. 11:56 11:56 11:57

Two of them were on matters on which he and the DPC agreed, 12333 and the limitations on the JRA and Privacy Act; two of them related to matters that were not remedies that were generally available to non-EU persons or indeed EU persons, criminal, exclusionary remedy, possibility of criminal prosecutions; of the remaining four, one was standing, which he accepted was, in his own words, a *substantial* obstacle; and the other was the APA which I think he also accepted, and I'll come back to this shortly, was a remedy with some limitations. 11:57 11:58

There were two then final issues, Rule 11 and its

relevance, and you have heard what you have heard about that and I don't want propose to say any more about it and then issues around the immunity and sovereign immunity and recoverability of damages. I don't believe that they are key. 11:58

But, subject to that, in my respectful submission, the DPC analysis of US law and Mr. Serwin's analysis in his report is not questioned by Prof. Vladeck. 11:58

Insofar as I can ascertain I think the principal difference between Prof. Richards and Prof. Vladeck, subject to just this issue of standing, of **Clapper** standing if I can use that phrase which I will come back to, was differences to the effect of the decision in **Spokeo** and that difference was undoubtedly there. 11:59

So, Judge, in the light of that could I respectfully submit that the court should draw eight conclusions in relation to US law. The first and simplest is there is no provision in US law for the giving of notice after the fact that surveillance has taken place and there is no dispute about that. 11:59

You'll recall Ms. Gorski's evidence which was that most people in the US who have been surveilled will never know of that fact. She advocated, as you will recall, the prospect of delayed notification. I do think it's of some significance that even Prof. Swire writing in 11:59

2004 had called for reconsideration of that position. As I said that's page 98 of his report. That's the first issue, it's clear-cut, no dispute.

The second issue then, Judge, relates to the findings that should be made in relation to the **Clapper** standing, if I can so phrase it. Again I don't believe - well, sorry, there is no room for dispute as to what the test articulated by the United States Supreme Court was. It is not an objectively reasonable likelihood that communications will be intercepted. It is a requirement of certainty and of imminence. The threatened injury must be certainly impending. That's page, sorry, 1147 of the **Clapper** judgment, it's been opened to you many times. I'll just let the stenographer change. 12:00 12:00 12:00

Even if one takes the evidence provided by Facebook at its height in the form of Prof. Vladeck's evidence on standing, his formula was that you would have to show that you *had been* the subject of surveillance or *would shortly* be the subject of surveillance. His phrase was "has *collected or* will shortly *collect*" - day 12, page 153. But that, of course, even that formula has to be refracted through the prism, as it were, of certainly impending - "will shortly" was the language used by Prof. Vladeck. 12:01 12:02

And I think, Judge, what is arresting about the

evidence given by Prof. Vladeck on standing is how readily and, let me say, properly, he accepted what a significant obstacle this was to litigants. On five occasions in his evidence he referred to it as a *substantial* obstacle. He also referred to it as an *extremely* high bar and an exceptionally high bar. Ms. Gorski described it as an extraordinarily difficult obstacle. And Prof. Richards described it as presenting a substantial obstacle. Indeed, it's difficult not to observe the similarity of the language to which all of the experts resorted in describing the effect of the **Clapper** case. 12:02 12:03

Prof. Swire - day 11, page 75 to 76 - agreed that people would not know of surveillance and that people who did not know they were being surveilled would have difficulty establishing standing. And this is the position - and these were his words - "*under* most *scenarios we can think of.*" 12:03

And, Judge, I would again remind you of Prof. Vladeck's articles, suggesting that Congress would broaden this standing out, it's not immutably fixed by Article 3 of the Constitution, in his opinion; it could be *aligned* with the test which, as he advocated it should be, it could be aligned with the test fixed by the United States Court of Appeals for the Second Circuit in **Clapper**, the case that -- not **ACLU -v- Clapper** --

MS. JUSTICE COSTELLO: No, no, **Amnesty**. 12:04

MR. MURRAY: -- the decision prior to the Supreme Court decision. But just to stop there. I mean, Mr. Gallagher's analysis, 'Well, you've got to have proportionality and strict necessity'; I mean, it is striking that the United States Court of Appeals for the Second Circuit saw *little* difficulty in formulating a test of standing based upon objectively reasonable, an objectively reasonable likelihood. It was sufficient for *them*. 12:04

So I would just ask you to bear that in mind and we'll come back to that when we look at these issues around proportionality and how critically important it is for national security law that you have these constraints which are imposed by the US federal system. 12:05

So I'm going to come back very shortly and, when I've finished my points on American law, just try to match them up against what we know about the law of the EU. It is *absolutely* clear that the **Clapper** test has *no* analogue in EU law. And in fact, when you look at the decisions of the Court of Human Rights that were opened by Ms. Hyland, you'll see, I suppose, an interesting calculus posited by the court that you have to look at a range of considerations when you decide how easy it should be to *bring* challenges to national surveillance -- sorry, national security surveillance. And in the absence of notification and in the absence of remedies in the individual contracting states, the 12:04 12:05 12:05

European Court of Human Rights applies a *very* weak test, far weaker than even the Second Circuit in **Clapper**, to deciding when there will be an entitlement to proceed in that court.

MS. JUSTICE COSTELLO: When you say "Second Circuit", you mean the Court of Appeal decision that was overturned by the Supreme -- 12:06

MR. MURRAY: I do.

MS. JUSTICE COSTELLO: -- Court? Yes.

MR. MURRAY: I do, yes. Sorry. 12:06

MS. JUSTICE COSTELLO: Because we were all referring to the Second Circuit as **ACLU**.

MR. MURRAY: I know. Because that was also -- yes. Yes, indeed. And on a number of occasions colleagues said 'Well, you have *some* remedies under US law' - this was a regularly recurring theme - 'You have *some* remedies under US law', so the fact it's not exactly the same as in Europe, that can hardly be the ground for complaint'. But without standing, you have *no* remedy. And at the end of the day, the analysis of US law can be expressed in a sentence: There's no obligation to tell you and if you don't know, it's very difficult to sue. And in our respectful submission, that is a state of affairs which is *patently* inconsistent with Article 47. 12:06 12:07 12:07

So I think it was Ms. Barrington who referred to a remedy with limitations being provided by US law. And it's wrong -- that's an incorrect description, with

respect. This is a situation in which there is, in that circumstance, in truth, no remedy.

MS. JUSTICE COSTELLO: Well, what do you say to the Data Commissioner's, I think it's paragraph 44 of her draft decision, saying that there are *some* remedies? 12:07

MR. MURRAY: Oh, yeah, there *are* some remedies. But you can't invoke *any* of them unless you've standing.

MS. JUSTICE COSTELLO: So you're saying effectively they're almost illusionary, is that what you --

MR. MURRAY: There is no remedy you can invoke without Article 3 standing, *none*. 12:08

So, Judge, that's notice and it's standing. And a third issue - and this, I suppose, leads on to what you've just observed - even if you can establish standing, you can't obtain damages for the bare violation of your privacy right - **FAA -v- Cooper** and **Doe -v- Chao**; you cannot obtain declaratory relief for *some* aspects of FISA, because the APA is precluded; and even if you can - and this, I think, is an important detail, Judge, which may have got a little lost because we perhaps all assume that a declaration is a declaration, you get them in the same way you might get them in this jurisdiction in respect of an historic event - it was made absolutely clear by Prof. Vladeck at day 12, page 176 that to obtain declaratory relief you have to establish that the harm is still occurring *or* that it's likely to occur again in the future. 12:08 12:08 12:09

So what that means is that even if you surmount Article 3 standing, you will not be able to obtain relief for a breach that has already occurred in the past unless you can prove loss to get damages or unless you can prove a likelihood of recurrence to obtain declaratory or injunctive relief. Your information may have been unlawfully disclosed and there is *no* remedy for that historic fact. And this *must* be why the Commission, in the paragraphs in the Privacy Shield Decision which I opened to you, emphasised that aspect of US law in its footnote. That's the third point. 12:10 12:10

Fourth, a finding we would urge you to make is that even if you establish standing and even if you establish pecuniary loss such as to entitle you to damages, *that's* not enough; you have to prove willfulness. That's the standard in Section 2712 and it governs actions under 1806(a), 1825 and 1845. The government agent must've acted with the conscious objective of committing a violation. 12:10 12:11

This is brushed aside in the submissions. I can't remember who, one counsel said 'Ah, sure look, that's just like the decision in **Glencar**, that's the law here'. It is emphatically *not*. **Glencar** is a decision about the exceptional tort of misfeasance in public office, the knowing abuse of powers, for which, unsurprisingly, you have to prove not just an abuse, but that it was knowing. *This* is about a violation of 12:11

protective privacy rights. And the position in US law is that you cannot *obtain* damages under these various sections where that violation occurs other than willfully.

12:11

Fifth, another point on which again I hope that the various points I've made are *not* the subject of dispute, I tried to take them as much as I can from Prof. Vladeck's evidence, the fifth point, again *not* in dispute, as non-US citizens you have no entitlement to 12:12 implead or rely upon the provisions of the Constitution. So you've no Fourth Amendment rights, you can't sue for damages for violation of the Fourth Amendment rights and you have *absolutely* no entitlement to challenge a state of affairs whereby, pursuant to 12:12 legislation, your information gets seized and accessed without any prior independent review, warrant, judicial or otherwise, where you become part of a retrospective annual review conducted by the FISA court. You cannot raise any issue as to that state of affairs. 12:13

Now, sixth - and here there *was* a dispute - **Spokeo**, there were differences perhaps in some respects of emphasis. But there's a number of aspects of that decision which are clear: Injuries have to be concrete 12:13 before they meet Article 3 standing requirements; a mere violation of a statute will not alone meet that test; it is clear that the test has been applied by lower courts to preclude claims under certain statutes

for bare violation of privacy interests - now, I have to emphasise, Judge, in fairness, Prof. Vladeck says these were all cases involving private actors and that in his opinion, the position would be different against a government actor in the context of national surveillance. But there is *no* law which has so determined since **Spokeo**.

Prof. Vladeck agreed that the doctrine could have application to cases of unlawful retention of information in a national security context. In that regard he thought that there was an issue as to whether the concreteness test would be met. And I think it's fair to say that there's a division between the experts as to whether the doctrine could function to preclude claims for unlawful disclosure of information or unlawful *obtaining* of information where there was no damage established. But I do think it important to emphasise, Judge, that Prof. Vladeck did say that in his view, the situation could be different in the context of national security issues. I'm not sure if that was ever put to Prof. Richards - certainly he never expressed a position that agreed with that. His view was that **Spokeo** had added another significant complication to data privacy cases. And you've seen the decisions of the lower courts holding bare privacy violations, albeit in the private context, as not entitling a claim for damages.

12:14

12:14

12:14

12:15

12:15

Then, Judge - I said I'd eight points, but I've only seven - the seventh and final one is that EU citizens, as with US nationals, are subject to significant constraints: The NSA excluded from the Redress Act; Privacy Act is subject to so many exceptions. And indeed Prof. Vladeck himself, in his evidence, said he didn't believe the Act was of much significance. And also, Judge, you've seen how Prof. Vladeck, in his writings, had criticised the rules in relation to state secrecy, calling for those to be abrogated and replaced with more tailored provisions. 12:15 12:16

So that's the framework of US law without ignoring what I said at the very start, which is that, save for his eight points, it's our understanding that the Data Protection Commissioner's analysis of US law and Mr. Serwin's are accepted, save for those eight points. 12:16

So where does that then leave us in terms of a comparison between those various points and the position under EU law? I think that some aspects of this can be dealt with relatively quickly and I'll address them in the order that I've just outlined them as applying to the US system. 12:16

So to deal first with notice. And that is, that, as you know, is addressed, Judge, at tab 37 in **Watson** and, Judge, going to perhaps overlap with the national security issue just as I open this case to you and I 12:17

want to draw some parts of it to your attention and I'll elaborate upon them again when I look at national security later this afternoon. If you look first of all at the laws that were in issue in **Watson**. The Swedish law is summarised at paragraph 16 of the decision. 12:18

MS. JUSTICE COSTELLO: Sorry, just a moment. There's numbers in brackets and then I just have to find what page it's on.

MR. MURRAY: Yes. Judge, it's page eight. 12:18

MS. JUSTICE COSTELLO: Thank you. Paragraph 16. Thank you.

MR. MURRAY: Yes. So this was the Swedish law with which the court was concerned: Access to data is regulated by the lagen -- well, I shouldn't have begun that, because there's no way I'm going to be able to finish it. We'll pass from that. The law "*on gathering of data relating to electronic communications as part of intelligence gathering by law enforcement authorities.*" So it was the Swedish law concerned generally with intelligence gathering. Then if you go to paragraph 33 you'll see - at page 12. 12:18 12:19

MS. JUSTICE COSTELLO: Thank you.

MR. MURRAY: The UK law. And here -- and of course, **Watson** was a case about retention. The RIPA, Section 22 provides: 12:19

"*This section applies where a person designated for the purposes of this Chapter believes that it is necessary*

on grounds falling within subsection (2) to obtain any communications data.

(2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary:
(a) in the interests of national security;
(b) for the purpose of preventing or detecting crime or of preventing disorder;
(c) in the interests of the economic well-being...
(d) ... of public safety;
(e) ... public health."

And so forth. Now, at paragraph 103, on page 24 the court made it clear that it was not just dealing with ordinary crime when it considered the issue of mandatory retention, which was the position both in the UK *and* in Sweden. 12:20

"... *while the effectiveness of the fight against serious crime*" - and it's interesting to note that within the context of "serious crime" the court felt fell "*in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary* 12:20

for the purposes of that fight."

So I do, Judge, with respect, suggest to you that my Friends are in error when they suggest that in some sense national security was being hived out by the Court of Justice from its analysis. That had never happened in any -- the other cases, **Digital Rights** or **Schrems** and there's nothing in the language of the decision that suggests that it was in fact observations like that one, of which there are a number, suggest otherwise. 12:21 12:21

Indeed if you turn to paragraph 111, on page 25:

"*As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation*" - and this is the legislation which the Court of Justice feels has to be there to allow retention - "*must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*" - and they are again all bunched together as part of the same justification - "*Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in* 12:21 12:22

one or more geographical areas, a high risk of preparation for or commission of such offences."

Then if you turn to paragraph 119, what is said is, at the bottom of page 26: 12:22

"*Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime... However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.*"

Again, the court does not see national security as

being *outside* the parameter of its analysis *at all*. On the contrary, it's specifically distinguishing between the requirements that might apply for access to be obtained to retained data in the situations to which it arises there and the particular situation of a *vital* national security interest which is threatened by terrorist activities -- sorry, if national security, defence or public security is threatened by terrorist activities, access might be granted where there's objective evidence. 12:23 12:24

And that's the context in which the court then moves, in paragraph 120, to say:

"... *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... 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... within the framework of procedures for the prevention, detection or prosecution of crime.*"

Now, it takes a great deal of strain to conclude that at paragraph 119 the court is talking about national security, because it obviously feels it's legitimately within its realms of consideration, but suddenly has

now forgotten about that entirely and is just talking about crime *excluding* national security.

MS. JUSTICE COSTELLO: Is there -- there was a point being made that, it might have been in one of the documents rather than in a submission, where you're dealing with crime, it's usually not so much preventative as looking back and solving it, whereas national security is much more focused on preventative and looking forward. I mean, that's a very crude characterisation of the argument. But is there any distinction there? 12:25

MR. MURRAY: No, well, in fact it's interesting, Judge, that you say that, because my recollection - I'd better check it before I say it - yes, the court talks about *fighting* crime. 12:25

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: "*Combating*" is a phrase used. Not detection and prosecution of past events. In fact the very formulation in the court's answer to the questions on page 29 supports the proposition that whether that distinction is a valid one or not, what the court was dealing with here was something far broader. 12:25

MS. JUSTICE COSTELLO: Yes, because obviously with terrorism, they really would be focusing on trying to prevent it rather than -- 12:26

MR. MURRAY: Yeah. Yeah.

MR. GALLAGHER: Judge, it's page 19 of the adequacy decision. The last footnote - I can't read what it is - is what draws that distinction you're referring to.

MS. JUSTICE COSTELLO: Thank you.

MR. GALLAGHER: Page 19 of the adequacy decision.

MS. JUSTICE COSTELLO: That's the Privacy Shield?

MR. GALLAGHER: Yes.

MR. MURRAY: Yeah. It's quoted in Mr. Gallagher's note on national security which was furnished to us, Judge, the other day. 12:26

So the -- and indeed you'll see there in paragraph 120 that the court is concerned with the framework for the prevention, which again feeds into Mr. Gallagher's own analysis of the distinction between national security and crime. 12:26

So then if you turn to paragraph 121 in *that* context: 12:26

"... *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... legal remedy, expressly provided for in Article 15(2) of* [the Directive], *read together with Article 22... where their rights have been infringed.*"

So what you see there is a principle that is *not* subject to proportionality, because it has proportionality built into it. It's not a freestanding

obligation to notify *everybody* immediately or at a fixed point in time, but it *is* an obligation to notify, as long as the notification is no longer liable to jeopardise the investigations. And *that* is something which, of course, is missing and absent from the United States regime. But aside from being missing, it means that these ideas that have been suggested to you - 'Well, sure look, that can be just cancelled out by considerations of proportionality' - is wrong. Because as I've said, proportionality is built into the formula of the obligation. 12:27 12:28

So in my respectful submission - and I will, of course, come back to this later this afternoon - the proposition that the court, in the *context* of legislation which *expressly* encompassed national security within it, giving rise to the reference, was, without ever saying so and actually referring to national security throughout the decision, was in some sense excluding it from the formulation of its principle and obligation is *impossible* to accept and involves turning logic upside down by saying, well, national security is excluded and, therefore, we have to assume that they were excluding it, even though they never so said, when in fact the proper analysis is that they considered national security, *it must follow* that they were devising a rule which applied across the board. And that reflects precisely the approach taken in **Schrems**, which, if Mr. Gallagher is right, has to 12:28 12:28 12:28

have proceeded from a fundamentally mistaken basis.

So that's notice, Judge. The -- well, yes, indeed Ms. Hyland, I just note, had said on day 18 that this was not concerned with national security, because it could not be the case that the Court of Justice unilaterally would have imposed an obligation on all intelligence services to notify without *any* caveat or possibility for that notification to be restricted where the national security demands that to be the case. But that's in the formula. That is in the formula itself. 12:29 12:29

So in our respectful submission, on the first of the points I looked at in US law, there is a sharp dichotomy, a clear principle of EU law which is not observed in the US. And of course, as the decision in **Schrems** acknowledges, you're going to have that; you can't expect one legal system to be the carbon copy of another. But there are certain fundamental entitlements which go to the very essence of the right. And as you will have seen from the analysis at paragraph 120, the right to notice is an aspect of the entitlement to invoke a remedy, because without notice your ability to do so is constrained. 12:29 12:30 12:30

In relation to standing, Judge - and I *am* conscious that these decisions have been opened to you, but I'm afraid I *am* going to ask you to go back and look at

them very quickly - Hogan J's judgment in **Schrems** in fact provides an authoritative consideration of the standing requirements. It's at tab 20. And if I can ask you to go to paragraph 41. And there - I think this was opened to you, I don't recall it, but just to emphasise it in any event - at paragraph 41 you'll see the Commissioner had advanced the proposition that Mr. Schrems' case was hypothetical because he couldn't prove that his information had ever -- that there was no evidence that there was an imminent risk of grave harm to him or any of his data was, had been or was likely to be accessed. And -- 12:31 12:32

MS. JUSTICE COSTELLO: That's effectively a sort of a US-type argument.

MR. MURRAY: It is, yes. And in fact some of the language is exactly the same as **Clapper**. And Hogan J. says: 12:32

"*42. For my part, I do* not *think that this objection is well founded. The Snowden revelations demonstrate - almost beyond peradventure - that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control. It is true that Mr. Schrems cannot show any evidence that his data has been accessed in this fashion, but this is*

not really the gist of the objection.

43. The essence of the right to data privacy is that, so far as national law is concerned and by analogy with the protection afforded by Article 40.5 of the Constitution, that privacy should remain inviolate and not be interfered with save in the manner provided for by law."

And he gives examples of that. 12:33

"*44. This is also* clearly *the position*", Hogan J. felt, "*under EU law as well, a point recently confirmed by the Court of Justice in... Digital Rights Ireland in a case where the Data Retention Directive... was held to be invalid by reason of the absence of sufficient safeguards in respect of the accessing of such data.*"

And there he reads paragraph 32. That's been opened to you before: 12:33

"*By requiring the retention of the data listed in Article 5...* [it] *...derogates from the system of protection of the right to privacy established by* [the Directives]."

Then paragraph 33:

"*To establish the existence of an interference with the*

fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way."

It's of some note that Hogan J. thought that statement was relevant to the question of standing.

"*As a result, the obligation imposed by Articles 3 and 6 of* [the Directive] *on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5... constitutes in itself an interference with the rights guaranteed by Article 7.*"

Then he talks about the access of national authorities, or the court, to the data constitutes a further interference with that right. And then Hogan J., at paragraph 45, said: 12:34

"*The same reasoning applies here. Quite obviously, Mr. Schrems cannot say whether his own personal data has ever been accessed or whether it would ever be accessed by the US authorities. But even if this were considered to be unlikely, he is nonetheless certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents*

and purposes, appears to provide only a limited protection against any interference with that private data by the US security authorities.

46. It is manifestly obvious that the present case raises issues of both national and EU law, although in the event the issue is largely governed by EU law given the central importance of the Commission decision."

So there is, in my respectful submission, an authoritative consideration by Hogan J. of what the standing requirements imposed by EU law are in *exactly* this situation, and they are diametrically opposed to those enabled under the law of the United States. 12:35

Ms. Barrington, I think it was, posed the rhetorical question: Well, how would Mr. Schrems do if he sought standing in Ireland in the light of the various, the information that's been disclosed to the court? And the answer is: Pretty well, on the basis of the decision. The case makes it absolutely clear, in my respectful submission, that facts which in United States law would not be sufficient to establish standing and could not do so are sufficient under the law of the European Union. 12:35 12:36

Judge, can I just remind you of one aspect of this? If I could ask you to go forward to paragraph 49? There, Hogan J. says:

"*The mere fact that these rights are thus engaged does not necessarily mean that the interception of communications by State authorities is necessarily or always unlawful*" - and he refers to the preamble to the Constitution - "*Provided appropriate safeguards are in place, it would have to be acknowledged that in a modern society electronic surveillance and interception of communications is indispensable to the preservation of State security.*" 12:36

Now, again, on Facebook's argument, Hogan J. has completely misunderstood and forgotten about these key limitations on Union competence.

"*It is accordingly plain that legislation of this general kind serves important – indeed, vital and indispensable - State goals and interests.*"

Then if you go forward, Judge, to paragraph 62, he again emphasises his understanding of the legal structures around surveillance regulation in the United States, the operation of the FISA court and is clearly in *no* doubt and under no misapprehension that what he is asking the Court of Justice to do is to embark upon a consideration of the implication of transfer to the United States *because* the national security authorities in that jurisdiction have accessed information in the manner in which they did. 12:37 12:37

In that book, Judge - and this was opened by Ms. Barrington to you - but if I can ask you to go back to tab 19, where you'll see **Digital Rights**. And here the State raised the argument that the applicants, whose standing was based solely upon their ownership of a mobile telephone, that they could not establish standing. And if you go to page 275, McKechnie J., at paragraph 44, quotes from the **Verholen** case, where he says -- where the court said: 12:38 12:38

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

And it is very hard to see how it can be credibly said in the light of the evidence of Facebook's own US expert witnesses that that is not *exactly* the effect of the combination of there being no obligation to give notice and of the standing rules as articulated by the Supreme Court in **Clapper**. It is virtually impossible - indeed on the basis of Ms. Gorski's evidence, *actually* impossible for the vast majority of people who have been surveilled to proceed to seek a legal remedy. 12:39

If you turn over the page, the quotation from the **Unibet** case, 275 - this was opened to you. But if you go to page 276.

MS. JUSTICE COSTELLO: Yes. 12:39

MR. MURRAY: Again you see another useful formulation at paragraphs 42 and 43; you can't undermine the right to effective judicial protection. 43:

"*The detailed procedural rules governing actions for safeguarding an individual's rights under Community law must be no less favourable than those governing similar domestic actions... and must not render practically impossible or excessively difficult.*"

Again I would pose the question: Can it be *seriously* said that US law does not have the effect in the circumstances that we are considering of rendering it excessively difficult or practically impossible to exercise rights? Indeed, the very descriptions recorded 12:40 in Prof. Vladeck's evidence, leaving aside the descriptions accorded by other witnesses, would fit almost exactly with that language.

There was some time spent on EU law dealing with direct 12:40 action and an attempt to suggest that this in some way meant it would be *okay* in domestic legal systems to create a practical impossibility for the agitation of Article 47 rights. And that would be all right if

there was what was described by reference to one of the cases as an *indirect* remedy. And that, to use language which has in fact been used by counsel in another context, is actually to compare apples and oranges. The rules around direct action are there really as part of the *structure* of EU administrative law and are there *because* of the ability of the national courts applying *precisely* these standing rules to refer, as you are being asked to do, to the Court of Justice. So it is, with respect, a completely *inapposite* analogy. 12:41

So, Judge, I have already outlined - and it's, I think, paragraph 89 of **Schrems**, as quoted by the European Commission in **Safe Harbour** - how the requirement to prove some type of financial loss or pecuniary loss is *not* consistent with the essence of the privacy right. And the critical issues, that being the case, as you match those various provisions of US law against EU law come down to, I think, three propositions, which are recorded on the list of questions that I handed up to you on Friday: One, is proportionality analysis always necessary, or is it sufficient to look and see if the *essence* of the right is protected in the third country? Two, if it *is* sufficient to look at the essence of the right, is the essence of the Article 47 right impaired by US law? And three, insofar as Article 47 is concerned with judicial remedies, is it possible or permissible to look at non-judicial remedies? And each of those, in our respectful submission, can be answered 12:41 12:42 12:42

really quite briefly.

The Charter itself, in Article 52 - and this is book one, tab one...

MS. JUSTICE COSTELLO: Can I put aside **Digital Rights** for now? 12:43

MR. MURRAY: Well, I -- yes. Yes, Judge.

MS. JUSTICE COSTELLO: Yes, I have it.

MR. MURRAY: So if you turn to Article 52, the function of the court in considering limitations on the exercise of rights and freedoms is described: 12:43

"*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law* and respect the essence *of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest.*"

Just while we're on that, Judge - it'll save me coming back to it - can I ask you to note no. 3 in Article 52: 12:44

"*In so far as this Charter contains rights which correspond to rights guaranteed by the Convention*" - ECHR - "*the meaning and scope of those rights shall be the same as those laid down by the said Convention.* [But this] *shall not prevent Union law providing more extensive protection.*"

And I think Mr. McCullough referred to that provision the other day. So you start off from a regime whereby the first issue, as defined by the article itself, is: Has the essence of the right been impaired? So that, just to give you the reference rather than to ask you to open it again, that is reflected in the very analysis adopted by the -- that is reflected in the very analysis adopted by the Advocate General at paragraph 132 of **Watson**; is the essence of the right respected? 12:45

And we are criticised, the Commissioner is criticised trenchantly for not conducting some wide ranging proportionality analysis - not looking at national security and identifying what the exigencies of it were and deciding whether restrictions on the exercise of rights enabled by US law were required to achieve that objective and went no further than necessary to do so. This criticism is repeated again and again. And she's also criticise d for not looking at the substantive content of the rules relating to national security. 12:45 12:46

But in truth, *none* of that was necessary. Because much indeed, as with the analysis of the Commission in the Privacy Shield Decision, the concern of the Commissioner was with remedies. And her conclusion, which I would respectfully submit, for the reasons I've just outlined, is *amply* supported by the evidence you've now heard, was that the *essence*, the essential 12:46

requirements of the remedies under Article 47 had been impaired in the United States system. So the question of proportionality *doesn't arise*. The issue is: Was the essence of the rights interfered with? And it was, for the very reason that I have outlined probably at excessive length already. 12:47

I think, Judge, that when the court looks at the core paragraph in **Schrems**, paragraph 95, there is no proportionality analysis *there* and none required. The question is a binary one: Was there or was there not the provision or facility for a remedy under Article 47, that being the essence of the right in issue? 12:47

Going back to the second of the third questions that I've just identified, that formulation answers that question, because the essence of that right *is* impaired. And it also answers the third part of the question, because it is a right to a determination by a tribunal as provided for in Article 47, which means a tribunal which is independent and established by law. And that is something of which EU citizens are deprived in *each* of the respects which I've outlined, but in particular in relation to standing, in relation to notice and in relation to their inability to deploy constitutional entitlements. 12:48 12:48

So in my respectful submission - and this, I suppose, goes back to one of the three core points that I

outlined to you on Friday - in our respectful submission, the issues around - and a huge amount of the evidence is directed, as you know, to this argument as to proportionality - the evidence is not relevant to the issue before you and it *wasn't* relevant to the Commissioner. 12:49

But even if it *was*, what *exactly* is the justification by reference to *any* principle of proportionality for *not* providing notice after the investigation is no longer compromised by providing notice? What *is* the justification for that and where is it to be found? And what is the justification for having a rule of standing which prevents persons who apprehend on reasonable grounds that their privacy is going to be violated by state surveillance, what is the rule of public policy or national security which says 'No, you can't sue'? And why did the originally -- well, I can't remember, the majority of the judges in the Second Circuit in the first **Clapper** case and in fact, unless I'm mistaken, that case was re-heard by 12 judges, who divided equally six/six, resulting in the original decision standing; how come they didn't understand that they were opening the doors to some national security disaster? It really, with respect, makes *no* sense. 12:49 12:50 12:50

And when one comes back and looks at what the European Court of Human Rights has said about the entitlement to claim the position of victim under the Convention in

exactly this situation, it is obvious that there is and *can be* no justification for either of those two elements. But that is very much a side consideration and a secondary argument, because the Commissioner's decision, in our respectful submission, stands and stands correctly in its own terms. 12:51

Now, we've had a lot of interesting discussion - I'm going to move on to the next headline issue, Judge, which is the SCCs - a lot of interesting discussion about what's adequate and what's sufficient and what's the Polish for "adequate" or the French for "sufficient" and where does that all get us? And that certainly led to an engaging couple of hours. And then we have had a very helpful discussion of what's in the SCCs and increasingly barbed criticism of the Commissioner for not engaging in some greater analysis of the SCCs. But one of the striking - a word which has perhaps been overused by everybody in submissions in this case - one of the noticeable aspects of what you've heard about the SCCs from my Friends is this: The argument has been advanced to you almost entirely - the argument that they do in fact provide an adequate/sufficient/Article 26(2) compliant level of protection - it has been presented almost entirely in the abstract. 12:51 12:52 12:52

I would've thought that had it been said, or if it were to be said to you that actually the SCCs *do* provide a

proper remedy - we'll just use that word for the moment, a proper remedy for the purposes of Article 26(2) - I would've expected that somebody would've said 'Right, let's take the Commissioner's objections and *pretend* they're correct, her conclusions on US law are correct, and let's now look at each of them and we will show you how the SCCs provide a remedy in that situation. And if there are some where it doesn't provide a remedy, we will now tell you *why* it is that the SCCs were not actually required to do so'. That, one would've thought, is the analysis you'd expect to have heard were the case -- sorry, having regard to the essential argument that's being made. 12:52 12:53

But who went through that analysis with you? Ms. Hyland certainly, in fairness, went through in some detail the SCCs. Mr. Collins went through the SCCs in some, albeit somewhat louder, detail. But where did you actually, where were you actually told which were the provisions in the SCCs that remedied the deficiencies which the Commissioner rightly or wrongly, or the gaps which the Commissioner had rightly or wrongly found in US law and where were you told that, given the fact that the SCCs did not provide a remedy in circumstances A to D, actually that was fine? 12:53 12:54

MS. JUSTICE COSTELLO: Well, Mr. Cush had a different analysis - and I'm summarising it very crudely; his analysis was of course contracts don't remedy state laws, but you've got an alternative effectively, he

called it compensation if I'm remembering it correctly.
MR. MURRAY: Yes.
MS. JUSTICE COSTELLO: So he was sort of saying 'You're not going to get your apple, you're going to get your orange'. 12:54
MR. MURRAY: Yes.
MS. JUSTICE COSTELLO: 'And that's good enough'.
MR. MURRAY: Well, what does --
MS. JUSTICE COSTELLO: Now, that's very, very crude.
MR. MURRAY: Yeah. No, but that is exactly the example I was thinking of. What does the man who doesn't know he's under surveillance get? What does the man or woman who believes they're under surveillance in a reasonable -- with reasonable likelihood and wants to litigate that fact get? What does the person whose information is unlawfully disclosed by the NSA, in circumstances where, as a matter of EU law, it may be said they ought not to have had the information at all, what do *they* get? What's the provision in the SCCs that gives them *anything*? 12:54 12:55

In fact, if one wishes to stay with the apples and oranges and move them into a Christmas analogy, you get the stocking with the block of coal in it. You don't get *anything*. And it is particularly significant, as Mr. McCullough emphasised on Friday, that Clause 4(a) in the SCC articles is the one for which there is *no* contractual responsibility. 12:55

So where that takes you is to the following proposition, which is in truth and in terms what the Commissioner said in her decision: That there are going to be certain circumstances in which there is a deficiency in *a* legal system which has not been and in some circumstances *cannot be* remedied by an SCC. And that *must* be the case. 12:56

If the difficulty is with Article 47 and if the deficiency is the absence of an Article 47 compliant remedy or any ability to obtain one, that is not and cannot be resolved by the SCCs. It is, if I can respectfully say so, as simple as that. Which is why the Commissioner's decision, correctly, does not engage in pages of analysis to reach it. It is that simple. 12:56

And if it is *not* that simple then it means that under Article 26 SCCs can be produced and can be incorporated into the law and applicable to particular states, but data transferred under those SCCs to a jurisdiction where there is no equivalent to *the most basic* requirement imposed by EU law at the remedial level. And maybe that *is* the case. But in our view, it's not the case. And at the very least that is a question which the Court of Justice, never having elaborated upon it, must conclude. 12:57

And can I -- again I'm, I suppose, hesitant to re-open cases and paragraphs that have been opened to you on

too many times already, but can I just remind you, I think it was Mr. McCullough who drew this to your attention, and we entirely agree with it, that in, in particular, the Advocate General's ruling in **Schrems** - and I'll have the paragraph numbers for you after lunch - there's an analysis of the meaning of the word "adequate". It's a memorable paragraph, because it also quotes the equivalent word in the French version, "adéquat" and, well, does adequate mean appropriate or does it mean something else? 12:58

And this, if I can respectfully submit, is the solution to the word games dilemma arising from some of the submissions that you have heard: Really -- there are, of course, different terms used in different language texts, but ultimately the question as to what the meaning of the clauses is is to be determined in the light of their purpose and context, and in particular the purpose and context of a regime of data protection which, as is stated in all of the cases, envisages a "high level of protection". 12:58 12:59

That's ultimately the test. And no one says, nor could they say that there has to be some equivalence between the legal systems applicable to data protection, no one says there has to be a carbon copy of the Data Protection Directive in all Member States to which information, or to all states to which information is transferred. *But* there are certain *minimum* 12:59

requirements that *must* be addressed. And in our respectful submission, for the reasons that I've outlined, in the case of the United States, there are not and the SCCs do not and cannot remedy them.

13:00

So, Judge, subject to the court, I can pick that up --

MS. JUSTICE COSTELLO: Yes, I'll take that up at two. Thank you.

13:00

(LUNCHEON ADJOURNMENT)

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

MS. JUSTICE COSTELLO: Thank you. Good afternoon.
REGISTRAR: In the matter of Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 14:04
MS. JUSTICE COSTELLO: Mr. Murray, I know you have come on to the SCCs and one of the questions I didn't ask you this morning, I sort of held back for when you got on to the SCCs was, when you are analysing and responding to the arguments can you address the issue as to what is the purpose of Article 26(2). Because it's predicated on the lack of adequacy in the national laws of the third country and how were the SCCs meant to deal with that inadequacy in your submission in a way that's workable. I am assuming that there has to be some sort of workability here or else it can be an avoidance mechanism which would drive a coach and four through the Article 25 requirement. 14:04 14:05
MR. MURRAY: Yes.
MS. JUSTICE COSTELLO: It's in relation to the balance.
MR. MURRAY: And maybe, Judge, just in dealing with that question before I look at the text of the SCCs, can I ask you to look at the Advocate General's judgment -- 14:05
MS. JUSTICE COSTELLO: In?
MR. MURRAY: -- in Schrems.
MS. JUSTICE COSTELLO: Schrems. What tab is it again?
MR. MURRAY: Now, I am sorry, Judge, it's Tab 36B.

MS. JUSTICE COSTELLO: Yes. And you were mentioning paragraph?

MR. MURRAY: Yes, I just wanted to open the four or five paragraphs in which this appears. Again I do apologise for opening paragraphs that have already been opened to you, but it's really I suppose with a view to putting them into -- 14:06

MS. JUSTICE COSTELLO: Sorry. My highlighter was hiding, that's all.

MR. MURRAY: So, Judge, sorry, Tab 36B. 14:06

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: And I'm going to ask you to go to paragraph 139.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: So you start off with, the Advocate General explains: 14:06

"Article 25 is based entirely on the principle that the transfer of personal data to a third country cannot take place unless that third country guarantees an adequate level of protection. The objective of the article is thus to ensure the continuity of the protection afforded by the directive where personal data is transferred to a third country." 14:07

And that word *"continuity"* I think is important:

"It is appropriate, in that regard, to bear in mind that the directive affords a high level of protection

of citizens of the Union with regard to the processing of their personal data.

140. In view of the important role played by the protection of personal data with regard to the fundamental right to privacy, this kind of high level of protection must, therefore, be guaranteed, including where the data is transferred to a third country.

14:07

141. It is for that reason that I consider the Commission can find, on the basis of Article 25, that a third country ensures an adequate level of protection only where, following a global assessment of the law and practice, it is able to establish that that third country offers a level of protection that is essentially equivalent to that afforded by the directive, even though the manner in which that protection is implemented may differ from that generally encountered within the Union."

14:07

14:08

Now again, Judge, obviously he's dealing with Article 25 rather than Article 26, but it clearly defines the context. And the key, I suppose, concepts there are that of continuity of the high level of protection achieved through essential equivalence, although the manner in which protection is implemented may differ.

14:08

And then over the page:

"142. Although the English word 'adequate' may be understood, from a linguistic viewpoint, as designating a level of protection that is just satisfactory or sufficient, and thus as having a different semantic scope from the French word, the only criterion that must guide the interpretation of that word is the objective of attaining a high level of protection of fundamental rights as required by the directive.

14:08

143. Examination of the level of protection afforded by a third country must focus on two fundamental elements, the content of the applicable rules and the means of ensuring compliance with those rules.

14:09

144. To my mind, in order to attain a level of protection essentially equivalent to that in force in the Union, the safe harbour scheme, largely based on self-certification and the self-assessment by the organisations participating voluntarily in that scheme, should be accompanied by adequate guarantees and a sufficient control mechanism. Thus, transfers of personal data to third countries should not be given a lower level of protection than processing within the European Union,.

14:09

14:09

145. In that regard, I would observe at the outset that within the European Union the prevailing notion is that an external control mechanism in the form of an independent authority is a necessary component of any

system designed to ensure compliance with the rules on the protection of personal data."

Just to stop there. I mean there's a lot in that and a lot which is directly relevant, including the last paragraph which ties in clearly to the Ombudsman who is not independent of the Executive, although it is consistently said he is independent of the security services, something which comes from the Strasbourg jurisprudence which I will come back to. 14:09 14:10

That is the context in which the court looks at Article 26, bearing in mind that Article 26 has to be interpreted in the light of those principles and objectives as described by the Advocate General. And you then turn, Judge, to Article 26 itself, you will recall it's in Tab No. 4 page -- 14:10

MS. JUSTICE COSTELLO: I have it, thanks.

MR. MURRAY: -- 46 and paragraph 2 then: 14:11

"*A Member State may authorise a transfer or 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 - and you will recall it was with the word 'adequate' that some issue was taken by Mr. Cush - with respect to the protection of the privacy of fundamental rights and freedom of individuals and as regards the exercise of the corresponding rights. Such safeguards may in* 14:11

particular result from appropriate contractual clauses."

Now the objective is to ensure, in this case through the mechanism of the standard contractual clauses, that the protections which are identified by the Advocate General, and which follow in any event from Article 25, are provided. So, and if you want to use Mr. Cush's language, the clauses can compensate for what would otherwise be an inadequacy in the third country, third party state when compared with EU law. And the way they can do that, obviously I'm sure a myriad of different ways, depending on how the third party state is found to be inadequate in its legal system to begin with or its protections. 14:11 14:12 14:12

It may be that an inadequacy is something which can readily be addressed through a contractual clause. For example, if you have a third party state that has a completely, if I can use the word, adequate system of remedies within its own judicial system but an aspect thereof, let's to take one just isolated example: A preclusion on recovering compensation except where there is financial damage proven. Let's say that is not adequate protection. Well, the standard contractual clauses could - if you take this example, but otherwise an adequate system with courts that you can access without the substantial obstacle of standing, you can establish your entitlement to a 14:13 14:13

remedy but you have that cap, just take that example. You can't obtain compensation for what in European law is required in order to have a proper system of protection.

14:13

Well, in that situation you could have a system whereby the standard contractual clauses allowed compensation equivalent to that which is required in European law to be made available under the clauses for the breach. That would satisfy the breach. So you have your system 14:14 and if you want to go and get rectification or destruction of information you go to Ruritania's courts and they have the jurisdiction and power to give you what you are seeking but they have this one aspect which falls short of what is required in the European 14:14 system and that can be remedied through the standard contractual clauses. And you could I'm sure conceive and consider and examine many other similar examples of those types of deficiencies where, in combination with the third party legal system and the supplement 14:14 provided by the SCCs, you are brought back to the position such that the essential entitlements that you are guaranteed under European data protection law are in one form or another remedied and protected.

14:14

To do that, and this again goes back, I suppose the point I made in the opening, Mr. Collins made in the opening, and the Commissioner did - and which the Commissioner adopted in her decision - to find out if

that's working you've got to, your first question has to be what is the inadequacy, what is the deficiency, what is the respect in which the third party state is not complying with the requirements identified by the Court of Justice. 14:15

Then, having identified that, the second question in fact logically is can that deficiency be remedied by an SCC; and the third question is, well if it can, has the SCC in place and in operation achieved that objective. 14:15

MS. JUSTICE COSTELLO: What's troubling me is that the SCCs to an extent are universal and, to put it colloquially, it is sort of one-size-fits-all. You could have any number of ways in which different states could have inadequacies, to use the language of the 14:16 Directive, and the SCCs are sort of there meant to be addressing it; is the critical third element then meant to be Article 4 of the SCCs, the individual suspension in respect of individual?

MR. MURRAY: Yes, and you will see from my road map, 14:16 Article 4 I'm going to come back and deal with separately.

MS. JUSTICE COSTELLO: Yes. The one thing that has troubled me is how the extremes of either end of the interpretations of 25 and 26 can each cancel out the 14:16 effect of 25 and 26?

MR. MURRAY: No, I fully understand. But in many respects, Judge, the point you make that it's one-size-fits-all is the very point. Because in other,

in systems other than the United States, the fundamental difficulty that presents itself here - I mean the SCCs are not intended to be a complete, well it is not necessary that the SCCs be a complete substitute for your entitlement to go to the third party system, they are a third party judicial system. It is just, and there may be jurisdictions where the fundamental difficulty arising in this case viz standing is not a problem. So the SCCs are very much a fallback in that event. 14:17

The problem here is one which cannot be remedied by the SCCs, just cannot be.

MS. JUSTICE COSTELLO: But even when the SCCs operate, we go to Ruritania and there is no problems with standing, the reliefs added to the picture by the SCCs are these third party contractual rights; isn't that right? 14:17

MR. MURRAY: Correct.

MS. JUSTICE COSTELLO: So what you are really doing is providing an additional type of remedy. 14:18

MR. MURRAY: Exactly. Then in any given situation, and this is why the submission that was made to you, I think it was Mr. Maurice Collins, that in some sense the idea of data flows to one jurisdiction being prohibited, which of course is the relief which we have sought, he suggested that this was inappropriate or inapposite. Actually it's quite right because it depends on how the SCCs intersect with each individual 14:18

system as to whether there has been an inadequacy.

And, Judge, if you take it back, and I know I am repeating myself and please forgive me.

MS. JUSTICE COSTELLO: No, no. 14:18

MR. MURRAY: But if you take it back to the core problem here which is the, as Prof. Vladeck describes it, substantial obstacle of standing, combined with the fact that the person does not know whether they have been the subject of surveillance, combined with the 14:19
fact that you cannot obtain damages absent proof of loss, combined with the fact that you cannot obtain relief absent by way of damages, absent proof of wilfulness, combined with the fact that your entitlement even to declaratory relief where the APA 14:19
functions is constrained by reference to the need to prove either present or future likelihood of harm, present harm or future likelihood, then you have your list of inadequacies and the next step logically has to be to do what I am now going to ask you to do which is 14:19
to look at the SCCs and ask 'well it's almost before and after, here are the deficiencies in the third party system, here is the SCC and after the SCC have those deficiencies, if such they be, as we say they are, been remedied'. 14:20

And I think, if I can respectfully say so, when one approaches it that way, whether the word one uses is adequate or sufficient or proper compensation really

slides behind the primacy of the objective which is as identified in the Advocate General's opinion in our submission.

So if I can ask you, Judge, because it's in the same book, to turn to the SCC decision and to engage in that very exercise. The relevant clause is on page 11 and it's Tab No. 10. 14:20

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

MR. MURRAY: And it is Clause 3, so you can see the core third party enforcement right given by Clause 3. 14:20

MS. JUSTICE COSTELLO: This is the Clause 3 in the standard clauses rather than the article itself; is that right?

MR. MURRAY: Well, it's... 14:21

MS. JUSTICE COSTELLO: I just want to make sure which 3 am I looking at.

MR. MURRAY: Yes, exactly, I am terribly sorry. It's in the annex to the decision.

MS. JUSTICE COSTELLO: Yes. 14:21

MR. MURRAY: You see "*the data subject can enforce against the data exporter*", so if you just stop there. And one can see that there would be issues with third party states where this provides, this fills the gap, this provides a mechanism for getting something which the third party state does not provide you with but which, through the mechanism of contractual liability, you can obtain: 14:21

"*The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i).*"

And you'll just note there, as Mr. McCullough emphasised, that excludes (a) and (, judge,): "*Clause 5(a) to (e), and (g) to (, judge,), 6(1) and (2), 7, 8(2) and 9 to 12 as third-party beneficiary.*" 14:21

So that contractual right is given and Ms. Hyland said 'well this shows you how' or the theory of this is that, I can't remember the exact phrase that she used, but it was to the effect that the domestic law protection including the Charter we would say travels, travels with the information. 14:22

But in truth it doesn't or does not in a fundamental respect which is relevant to this case. Because, as Mr. McCullough emphasised, the critical obligation in Clause 4(a) does not trigger liability under the SCCs. That is the one which says that the data exporter on the one hand agrees and warrants: 14:22 14:23

"*That the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate relevant*

provisions of that State." But that's excluded.

And if you turn over the page, (, judge,), which is the undertaking to ensure compliance with clauses 4(a) to (i), is excluded as well. So how does this clause, one in truth, with respect, doesn't even get to adequate or sufficient or compensatable or comparable, how do these clauses provide *any* remedy in the context of and having regard to the difficulties which I have identified. 14:23

14:24

And whether it's an unusual situation matters not, but it is the situation that the clauses combine with a legal system which operates because of its own rules to prevent *any* remedial, we say any remedy being available in a broad range of circumstances and that's the problem in our respectful submission. 14:24

MS. HYLAND: Judge, I think there is something wrong with what's being said, and I don't want to interrupt Mr. Murray, but at the end I would like to come back. I think there is a factual inaccuracy in what's being said. 14:24

MR. MURRAY: Well I think, Ms. Hyland can identify the fact inaccuracy now, Judge.

MS. HYLAND: Yes, Judge, because if one goes to look at Clause 3, one sees there that there's an entitlement to enforce against the exporter clauses 5(a) to (e) and 5(a) is in relation to the agreement of the data importer. 14:24

MR. MURRAY: Well, I wonder does that really affect the

situation, Judge? I mean, if we look at 5(a), the data importer: "*To process the personal data only on behalf of the data exporter and compliance with its instructions and with the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data.*" 14:25

How does that solve my problem if I have a reasonably well grounded belief that the National Security Agency has been listening to my telephone calls, reading my e-mails or reviewing the internet, my internet traffic, how does that give me anything? And that, if anything, if I can respectfully say so, proves the point. 14:25

Judge, then the next issue is well does the Ombudsman remedy this? Because you can go to the Ombudsman and subject to the proviso, if such it be, that there is a certain lack of clarity around the Ombudsman and the SCCs, but if we take it that the SCCs function vis-à-vis the data transferred under the standard contractual clauses, does that resolve the problem? Because you can go to the Ombudsman and you, Judge, obvious from your question this morning, are familiar with the process that that entails. The Ombudsman is appointed, in fact perhaps it's worth looking at the Privacy Shield decision Annex III A section 4(e) and again that should be open before the court. 14:26 14:26

MS. JUSTICE COSTELLO: I have that.

MR. MURRAY: So if you go to page, it is page 74, Judge.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: "*Once a request has been completed and as described in section 3, the Privacy Shield Ombudsman 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 Ombudsman will provide a response to the submitting handling body confirming EU individual complaint confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives 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 non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsman will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsman confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed.*" 14:27 14:27 14:28 14:28

So that's the core of the Ombudsman's functions. So you can say or it might be said 'well this resolves part of your difficulty because now you don't have to establish **Clapper** standing, you can go to this third

party and you can get a remedy'. So that then begs the question: Well does that resolve the difficulty? And in our respectful submission, and just to remind you, Judge, that this was an issue that was specifically addressed by Mr. Richards in his evidence and unless I am very much mistaken, it may also be -- no, in fact it may be an issue which Mr. Ferguson QC also addressed. 14:28

MS. JUSTICE COSTELLO: I don't think I have come across a Mr. Ferguson. I have come across a Mr. Robertson. 14:29

MR. MURRAY: Mr. Robertson, I am sorry.

MS. JUSTICE COSTELLO: But I haven't - unless that was one of the ones I ruled out.

MR. MURRAY: No. I'm sorry, Judge, I don't know where that came from. Mr. Robertson QC I think may refer to it, but in any event is that an Article 47 compliant remedy of the kind that we are concerned with? 14:29

In fairness, I think Ms. Hyland may have observed this, you will see that there is, and in fact in some of the footnotes in Privacy Shield decision there is sort of a relationship identified between this and the ECHR case of **Kennedy**. 14:29

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: Where I think it was Lord Justice Mummery was in charge of a procedure under the RIPA of a kind that had some of these features. 14:29

In our respectful submission there are well-founded

concerns about the efficacy of the Ombudsman and they derive from the simple and obvious fact that the Ombudsman is an appointee of the Executive under the auspices of the Secretary of State.

MS. JUSTICE COSTELLO: Well that obviously didn't bother the Commission. 14:30

MR. MURRAY: Excuse me, Judge?

MS. JUSTICE COSTELLO: That obviously didn't bother the Commission because they didn't take that point and accept it. 14:30

MR. MURRAY: No, that is correct and that is why, that is I suppose the issue that would travel to the Court of Justice in the event that the court were to decide to refer, and clearly the fact of the Commission decision, we all agree, doesn't preclude the Court of Justice from considering that very issue. 14:30

But just look back, Judge, at the Charter itself in...

MS. JUSTICE COSTELLO: Am I keeping this clause open or am I finished with it? 14:31

MR. MURRAY: No, and the court - that was just I suppose to outline the headline features of it.

MS. JUSTICE COSTELLO: Hmm.

MR. MURRAY: But if you turn, Judge, to Article 47.

MS. JUSTICE COSTELLO: Yes. 14:31

MR. MURRAY: And this is what the court in **Schrems** was concerned with: "*Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in*

compliance with the conditions laid down in this Article." And: *"Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal."*

14:31

That notion of independence has, is and always has been key to the Community concept of an independent tribunal of the kind envisaged by Article 47. If you just take, and I think that book the court can put to one side until I come back and look at Article 4 which will be the towards the end of the afternoon.

14:32

If you turn to Tab 25 you will see one of the many cases addressing the analogous concept, and the textbooks on the Charter I think all make clear that the analogy is a good one, between court or tribunal for the purposes of Article 234. So this is the case, Judge, of **Denuit**, Tab 25, if I can ask you to go to Tab 12?

14:32

MS. JUSTICE COSTELLO: Tab 12 or paragraph 25?.

MR. MURRAY: I am sorry, paragraph 12 Tab 25.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: So:

"*In order to determine whether a body making a reference is a court or tribunal of the Member State, the Court takes account of a number of factors, such as whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory,*

14:33

whether its procedure is inter partes, whether it applies rule of law and whether it is independent."

And again the texts on Article 47 make it clear that those, as one would expect, are critical indicia also of the court under Article 47. So how is it and how can it be that the body to whom you go in substitution, as you will have seen, for a proper remedial system, as you will have seen from the Privacy Shield decision, and perhaps *"proper"* is an unfair description, but in substitution for what the Charter would regard as an adequate remedial system, as I think is evident from the Commission's analysis of the issue, where it identified the difficulties with standing and the remedies available; how is it that someone serving under the pleasure of the Secretary of State and part of the Executive satisfies or could possibly satisfy that criteria? And that is aside entirely from the fact that it's not unusual in our systems of course to have bodies that are part of the Executive making decisions of one kind or another, but they are always subject to review by the courts. That is not the case here. There is no provision for review by a court, it is not established by law, it is not permanent, it doesn't give decisions or reasons, it doesn't grant compensation. It does exactly what I have just shown you.

14:33 14:33 14:34 14:34 14:34

And that, in our respectful submission, clearly

discloses a well founded basis for concern as to whether the difficulties which are identified in the Commissioner's decision, which of course to emphasise predated the Privacy Shield decision, have been addressed. 14:35

So, Judge, the next issue is one that I spoke to you about on Friday afternoon which is whether the comparator is EU law or the law of the Member States. I said quite a bit about it then and I won't go back 14:35 over it again, save just to remind you that the notion that you define your standard by reference to the laws of individual Member States rather than by reference to European law was not the approach adopted in **Schrems**, nor was it the approach adopted by the Commission in 14:36 the Privacy Shield. In fact, insofar as we can see, it's not the approach adopted by anyone ever anywhere.

It seems to us, and again I am repeating what I said on Friday afternoon but just to sign off on this issue, it 14:36 seems to us to be very difficult to see how in theory you could say that adequacy in the manner identified by the Advocate General in **Digital Rights** is met by some sort of a survey of Member State law in circumstances where the cases themselves show that the law of the 14:36 Member States on occasion does lag behind what the Court of Justice interprets the Charter as requiring, and that has been a feature and a striking one of both **Digital Rights** and **Watson**.

It's very difficult to see how you conduct that exercise in comparison, whether it's the average approach taken by the Member States or the approach only taken by some Member States or some lowest common denominator. Insofar as we can ascertain, Judge, no authority of any kind in the Directive or in the Charter or anywhere else has been identified as grounding that proposition. So that, as it were, in our respectful submission disposes of that. 14:37

And shall I just say this: If we are correct in what I have said to you about proportionality, and if I am correct in what I say to you about the laws of the individual Member States, well then actually a huge amount of the evidence which has been adduced before you by Facebook actually falls to one side because it is not in truth germane to any of the actual issues with which the court is concerned. 14:37

The next question then is the Convention and the role that it plays. I opened to you Article 52(3) --

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: -- a little while ago and it sort of explains the role of the Convention. I won't open this, but I will just give you the reference. There is a short discussion in the **Watson** judgment at paragraphs 126 to 131 of the status of the Convention in which it emphasises, what I think has already been said to you, 14:38

that the Charter is not part of EU law and that.

MS. JUSTICE COSTELLO: Sorry, the Convention I presume you mean?

MR. MURRAY: I am sorry, the Convention is not part of EU law, and that the Charter envisaged the potential for greater protection than the Convention, and indeed that the *Convention* has no equivalent of Article 8, no express protection for data privacy. So that's the first, I suppose, general point to bear in mind, Judge, as you look at the Convention cases. They are undoubtedly of some assistance. It could not be said that the Court of Justice would regard them as irrelevant to its interpretation of the issues. It refers to decisions of the Strasbourg court not infrequently in this context, but they are certainly not dispositive. That's the first thing. 14:39 14:39 14:39

The second thing, Judge, which is perhaps more important as you look at the Convention law, is to I suppose bear in mind the critical difference legally between what the Strasbourg court is doing and what the Court of Justice is doing. The European Convention on Human Rights is an international treaty. The Court of Human Rights superintends that treaty, but it does so in a context where it does not expect or impose uniformity on all of the legal systems which have subscribed to it. 14:39 14:40

The starting point, therefore, when you look at the

Strasbourg case law is the fact that the European Court of Human Rights is considering a large number of different legal systems which it acknowledges are entitled to regulate their affairs according to different modalities and therefore, and it's for this reason that the Court of Human Rights has the concept of margin of appreciation which effectively gives the state, the individual states the competence to decide themselves how they will go about giving effect to the Court of Human Rights decisions. 14:40 14:41

By contrast of course the Charter is an instrument which has an entirely different and immediate effect in all of the legal systems which must comply with it, insofar as it operates. And, Judge, we would, insofar as it is suggested in the submissions in Facebook and their analysis of the Court of Human Rights cases, insofar as it is suggested that the Strasbourg case law shows that the US system would pass the test in the Strasbourg court, we profoundly disagree with that. And I think, Judge, when you look at the case law and consider it in the light of the evidence you have heard of US law, it does become apparent that the position is quite different. 14:41 14:42

Can I ask you just to look at Prof. Brown's report. I made a passing reference to this this morning, and I actually put this to Prof. Swire, but this is at tab, it's in book -- it's in the book of the US materials, 14:42

Judge.

MS. JUSTICE COSTELLO: I am just waiting to hear which book it was or what tab it is?

MR. MURRAY: I am just waiting to...

MS. JUSTICE COSTELLO: Is it in the index? 14:42

MR. MURRAY: It's Book 5, Judge, Tab 66.

MS. JUSTICE COSTELLO: This is the US?

MR. MURRAY: This is, yes. And this is the report which both Prof. Swire and...

MS. JUSTICE COSTELLO: Yes, I have it, thanks. I think 14:43 Mr. Robertson.

MR. MURRAY: Robertson, I am trying to get Ferguson out of my mind, Mr. Robertson QC referred to. And if you turn to page 16 you will see.

MS. JUSTICE COSTELLO: Sorry the numbers are very tiny, 14:43 just a moment. Yes, I have it, thank you.

MR. MURRAY: Yes. You will see a helpful enough list under section 3.4:

"*Despite the relatively weak standards on foreign* 14:43 *intelligence collection by EU Member States, the European Convention to which those states [are parties] sets relatively high standards in terms of the compliance of all surveillance régimes with the rule of law.*" 14:43

Then he refers to a commentator who has identified the following minimum standards which should apply to all surveillance practices by Council of Member States:

"*Powers must be set out in statute law, rather than in subsidiary rules, orders or manuals. The rule must be a form which is open to security and knowledge. Secret, unpublished, rules are fundamentally contrary to the rule of law;*

Offences and activities to which surveillance may be order should be spelled out in a clear and precise manner; 14:44

The law should clearly indicate which categories of people may be subject to surveillance;

There must be strict limits on the duration of surveillance; there must be strict procedures to be followed for ordering the examination, use and storage of data; there must be strong safeguards against abuse; there must be strict rules on the destruction/erasure." 14:44

And then: "*Persons who have been subjected to surveillance should be informed of this as soon as it is possible without endangering national security or criminal investigations so that they can exercise their right to an effective remedy at least ex post facto."* 14:44

And then finally again, perhaps of some significance when you look at the Ombudsman: "*The bodies charged with supervising the use of surveillance powers should*

be independent and responsible to, and be appointed by Parliament rather than the Executive."

If you look then at page 3.

MS. JUSTICE COSTELLO: I thought we were on page -- oh, we are going back. 14:45

MR. MURRAY: Back to page 3, sorry. There's this comment at the bottom of the page:

"*In the absence of clear and specific rules in other countries, ironically the US now serves as a baseline for foreign surveillance standards - although the European Convention on Human Rights, which requires protection of the rights of all those within States parties' jurisdiction, sets a higher general standard than the US government's interpretation of its international human rights law obligations as applying only within its own territory.*" 14:45 14:45

Now, Judge, when you look at the cases, and I'm not going to open all of the cases opened by Ms. Hyland, but I will just look at a handful of the more recent ones. What I think emerges from those cases is that, and I think all of these aspects of the approach taken by the Court of Human Rights are products of the phenomenon that I have identified earlier on, namely the fact that they are dealing with myriad different legal systems without any requirement of uniformity and therefore subject to the margin of appreciation. 14:45 14:46

One of the first things they look at when they have these cases is to see well is there an effective remedy available under national law? And if there is effective remedies available under national law, the 14:46
human rights court tends to step back from investigating or examining the complaint.

If there is *no* possibility under national law of challenging the surveillance measures, the court 14:47
applies greater scrutiny. Second, if there is no effective remedy under national law the ECHR tends to allow standing before it if persons can establish a reasonable likelihood of surveillance, and you'll see in fact in some of the more recent cases an even weaker 14:47
standard being applied.

MS. JUSTICE COSTELLO: What was that you said, if they can establish, what's the word you used?

MR. MURRAY: If a person can establish a *reasonable* likelihood of surveillance. 14:47

MS. JUSTICE COSTELLO: Thank you.

MR. MURRAY: And, thirdly, the ECHR in our submission as one looks at the cases imposes an obligation to notify as a general principle but that obligation is qualified to the extent that it will not operate if the 14:47
investigation will be jeopardised by notification.

And also, in some of the cases, the court will not find an obligation to notify if there is a sufficient legal

remedy in the national system. That's rather like the point I made to you earlier on about the relationship between notification and standing, if you have got liberal standing rules then the need for notification may be abated. 14:48

So, Judge, these cases are contained in Book 4, and I think Ms. Hyland opened a number of earlier cases, **Klass**, which dates from 1976, and **Weber** and the **Silver** case. But I'm going to ask you to start with **Kennedy** 14:49 which is 2010. And just to explain, I'm going to open, Judge, to you just three of these cases, **Kennedy**, **Zakharov** and **Szabo** and the facts of each are important in terms of understanding why the court reached the conclusion that it did. 14:49

In **Kennedy** the court was concerned with the compatibility of the UK Regulation of Investigatory Powers Act with the Convention. This was a case brought by an individual who had served time in prison 14:49 and who subsequently set up, well became an advocate for those who had been involved I think in miscarriages of justice. He claimed that his communications were being monitored under the RIPA, the Regulation of Investigatory Powers Act. That legislation established 14:50 what was called an Investigatory Powers Tribunal and it was chaired by a Lord Justice of appeal, Lord Justice Mummery, and, not unlike the Ombudsman, it had a provision whereby you could make no determination or

advise that any illegality had been resolved and he made no determination in favour of the applicant, and that meant one of two things but they didn't tell you which: Either that there had been no interception of your communications or that such interception as had taken place had been lawful. 14:50

So, in terms of the English legal system there was this independent, and it was an independent body, to which you could bring a complaint without proving that you had in fact been the subject of surveillance or meeting some very high threshold. 14:51

And if you look at paragraph 57, Judge, you will see the court explains, this is on page 15: "*Section 57 of the RIPA provides that the Prime Minister shall appoint an Interception of Communications Commissioner. He must be a person who holds or has held high judicial office. The Commissioner is appointed for a three-year, renewable term. To date, there have been two Commissioners. Both are former judges of the Court of Appeal.*" 14:51 14:51

So the court, if you move forward to page 36.

MS. JUSTICE COSTELLO: Page 36? 14:51

MR. MURRAY: Yes, Judge, paragraph 122, explains the standing requirement that the court envisaged and it summarises this after consideration of **Klass**. And they say:

"*Following **Klass** and **Malone**, the former Commission - that's the European Commission on Human Rights - in a number of cases against the United Kingdom in which the applicants alleged actual interception of their communications, emphasised that the test in **Klass and Others** could not be interpreted so broadly as to encompass every person in the UK who feared that the security services may have conducted surveillance of him. Accordingly, the Commission required applicants to establish that there was a 'reasonable likelihood' that the measures had been applied to them."* 14:52 14:52

So that was the standard applied by the Commission:

"*123. In cases concerning general complaints about legislation and practice permitting secret surveillance measures, the Court has reiterated the **Klass** approach on a number of occasions."* 14:53 14:53

And then it quotes **Weber**, which was also opened by Ms. Hyland. And at the end of that citation it says this:

"*Where actual interception was alleged, the Court has held that in order for there to be an interference, it has to be satisfied there was a reasonable likelihood that surveillance measures were applied to the applicant."* 14:53 And that's the test explained there.

MS. JUSTICE COSTELLO: So that might have been the sort of situation where you had all the attorneys who were dealing with --

MR. MURRAY: Exactly.

MS. JUSTICE COSTELLO: -- people in Guantanamo. 14:53

MR. MURRAY: Exactly.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: And that becomes even clearer when we look at some of the later cases:

14:53

"*The Court will make its assessment in light of all of the circumstances of the case and will not limit its review to the existence of direct proof that surveillance has taken place given that such proof is generally difficult or impossible to obtain.*" 14:53

"*Sight*", they say over the page: "*Should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right* 14:54 *to challenge a law in abstracto. The principal reason was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities. In order to assess, in* 14:54 *a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any*

remedies at the national level and the risk of secret surveillance measures being applied to him. Where there is no possibility of challenging the alleged application of secret surveillance measures at a domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even whether the actual risk of surveillance is low, there is a greater need for scrutiny by this court." 14:54 14:55

So you see, Judge, how the, I suppose, range of review by the Strasbourg court is in inverse proportion to the remedies that are available in the domestic states. If the domestic states don't have any remedies at all, an expansive view of the Strasbourg court's standing or the standing of the victim to come to the Strasbourg court is taken. 14:55

MS. JUSTICE COSTELLO: So the same factual situations in different states could result in different decisions on standing because of the different legal régimes? 14:55

MR. MURRAY: Exactly, exactly. But the key driver, to use the phrase, is what the court explains there in paragraph 124, what you cannot have is a situation where secret surveillance is effectively unchallengeable. 14:55

And then at 125: "*The Court observes that the present applicant complained of an interference with his*

communications both on the basis that, given the circumstances of this particular case, he had established a reasonable likelihood of interception and on the basis of the very existence of measures permitting secret surveillance." 14:56

Now remember in the UK Mr. Kennedy could go to the RIPA where he didn't have to prove any surveillance. And he says: 14:56

"126. The applicant has alleged that the fact that calls were not put through to him and that he received hoax calls demonstrates a reasonable likelihood that his communications are being intercepted. The Court disagrees that such allegations are sufficient to support the applicant's contention that his communications have been intercepted. Accordingly, it concludes that the applicant has failed to demonstrate a reasonable likelihood that there was actual interception in his case.

127. Insofar as the applicant complains about the RIPA régime itself, the Court observes, first, that the RIPA provisions allow any individual who alleges interception of his communications to lodge a complaint 14:56 *with an independent tribunal - and again the independence of the tribunal is emphasised - a possibility which was taken up by the applicant. The IPT concluded that no unlawful, within the meaning of*

RIPA, interception had taken place.

128. As to whether a particular risk of surveillance arises in the applicant's case, the Court notes that under the provisions of RIPA on internal communications any person within the UK may have his communications intercepted if interception is deemed necessary or one or more of the grounds listed in the section. The applicant has alleged that he is at particular risk of having his communications intercepted as a result of his high-profile murder case in which he made allegations of police impropriety." 14:57 14:57

And there is the type of analogy with the people who are in contact with the men in Guantanamo Bay or who by virtue of their occupations are likely to be talking to targets of communications. 14:57

"*The Court observes that neither of these reasons would appear to fall within the grounds listed in section 5(3) RIPA. However, in light of the applicant's allegations that any interception is taking place without lawful basis in order to intimidate him, the Court considers it cannot be excluded that secret surveillance measures were applied to him or that he was, at the material time, potentially at risk of being subjected to such measures.* 14:57 14:58

129. In those circumstances he was given the entitlement to complain of an interference with Article 8."

Now, Judge, if you move forward then to - I'm sorry, yes - paragraph 166 on page 51. Here the court explains why ultimately it believes that the system in place in the UK meets the standard having regard to the 14:59
margin of appreciation fixed by the Convention. And at paragraph 166 the court says:

"*As regards the supervision of the RIPA régime, the Court observes that apart from the periodic review of* 14:59
interception warrants and materials by intercepting agencies and, where appropriate, the Secretary of State, the Interception of Communications Commissioner established under RIPA is tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants. He has described his role as one of protecting members of the public from unlawful intrusion into their private lives, of assisting the intercepting agencies in their work, of ensuring that proper safeguards are in place to protect the public and of advising the Government and approving the safeguard documents. The Court notes that the Commissioner is independent of the executive and the legislature and is a person who holds or has held high judicial office. He reports annually to the 14:59
Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes) which is laid before Parliament. In undertaking his review of surveillance practices, he has access to all

relevant documents, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires. The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken." 15:00

And then: "*In practice, the Commissioner reviews, provides advice on and approves the Section 15 arrangements. The Court considers that the Commissioner's role in ensuring the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorised provides important control.*" 15:00

I just see the stenographer is here, Judge.

But it's paragraph 167, Judge, I just want to draw your attention to: 15:01

"*The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge... In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike*

in many other domestic systems... any person who suspects that his communications have been or are being intercepted may apply to the IPT... The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers... In undertaking its examination of complaints... the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant... In the event that the IPT finds in the applicant's favour, it can... quash any interception order, require destruction of intercept material and order compensation to be paid... The publication of the IPT's legal rulings further enhances the level of scrutiny."

And whether or not that, Judge, is a system which would ultimately pass muster with the European -- with the CJEU under the Charter, it is *certainly* a system which differs in a number of significant respects from that in the United States. 15:02

Now, Judge, the next case is **Zakharov**. And this is a

2015 judgment. And this concerned a journalist in Russia who claimed that his communications had been intercepted by the FSB. And the court will find -- if you go forward, Judge, to paragraph 163 on page 38, where it says:

"*The Court observes that the applicant in the present case claims that there has been an interference with his rights as a result of the mere existence of legislation permitting covert interception of mobile telephone communications and a risk of being subjected to interception measures, rather than as a result of any specific interception measures applied to him.*"

And at paragraph...

MS. JUSTICE COSTELLO: That would be a bit like what they call the facial challenges in the United States.

MR. MURRAY: Well, it would. It would be a bit like what McKechnie J. actually allowed in **Digital Rights**, where the possession of the mobile phone was sufficient to allow you to challenge the fact of a mandatory retention regime and the possibility that the State - guards/revenue - could access that information.

At paragraph 164 the court summarises its case law. It says:

"*The Court has consistently held in its case-law that the Convention does not provide for the institution of*

an actio popularis and that its task is not normally to review the relevant law and practice in abstracto, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention."

There's a number of cases cited.

"*Accordingly, in order to be able to lodge an application in accordance with Article 34, an individual must be able to show that he or she was 'directly affected' by the measure complained of. This is indispensable for putting the protection mechanism of the Convention into motion, although this criterion is not to be applied in a rigid, mechanical and inflexible way...*

165. Thus, the Court has permitted general challenges to the relevant legislative regime in the sphere of secret surveillance in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them. In the case of Klass... the Court held that an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him. The relevant conditions were to be

determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures... and the connection between the applicant and those measures."

15:05

Then, Judge, down the page at 167, having quoted from **Klass**, they said:

"*In several cases the Commission and the Court held that the test in Klass and Others could not be interpreted so broadly as to encompass every person in the respondent State who feared that the security services might have compiled information about him or her. An applicant could not, however, be reasonably expected to prove that information concerning his or her private life had been compiled and retained. It was sufficient, in the area of secret measures, that the existence of practices permitting secret surveillance be established and that there was a reasonable likelihood that the security services had compiled and retained information concerning his or her private life.*"

And again that's redolent of the Second Circuit in **Clapper** in the one that went to the Supreme Court. 15:06
Then if you turn over the page then to paragraph 169. After they've observed the various chilling effects on different rights that such regimes can have:

"Finally, in its most recent case on the subject, Kennedy... the Court held that sight should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right to challenge a law in abstracto. The principal reason was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court. In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him or her. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court."

So what they then do, Judge, over the page, is try to put together a synthesis of the court's jurisprudence in relation to the entitlement to bring challenges to these types of secret surveillance measures, having

regard to the law as it's developed. And that consideration starts at paragraph 171:

"*In the Court's view the Kennedy approach is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities... Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. As the Court underlined in Kennedy, where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among*

the general public that secret surveillance powers are being abused cannot be said to be unjustified... In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law in abstracto, is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is [personally] *at risk.*"

Now --

MS. JUSTICE COSTELLO: "*Potentially*".

MR. MURRAY: Sorry, "*he is potentially at risk*", excuse me. So that's the twofold test: If there's *no* remedies in the national system, they will *actually* let someone bring an abstract challenge, saying 'My communications -- my communication is chilled by the

15:10

knowledge of this secret surveillance'; if there's a more generous system of remedies then the standing rule is tightened. But look to what it's tightened to - you're potentially at risk.

15:10

And, Judge, can I respectfully submit that I don't know of any case in which -- sorry, the Court of Justice has made it clear that it is entitled to apply a *higher* standard than the Strasbourg court. But it *cannot* be said that it's going to apply a *lower* one.

15:11

MS. JUSTICE COSTELLO: That's your Article 52(3)?

MR. MURRAY: Correct. And insofar as the court decides, wishes to try and, I suppose, develop or analyse further, then in our submission - it's already clearly articulated in **Schrems** what the requirements for access to the judicial remedies are - then that formulation is useful, in our submission, and it makes it very difficult, in our respectful submission, to see how it could be said that the US system meets it.

15:11

15:11

Now, the same judgment deals with the issue of notification. And this is picked up at paragraph 287 on page 73. And again I think in this judgment -- and I'm going to, I'm afraid, open a number of pages of this, because it just saves going back over the earlier cases and it's a synthesis of legal position. So at paragraph 286 they explain that they're now turning to the issue of notification. And they observe in that paragraph, as we've seen ourselves, that it is

15:12

inextricably linked to the effectiveness of remedies. And they say:

"*It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not 'necessary...', as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned.*"

And that again is a formulation which is uncannily similar to that ultimately adopted by the Court of Justice in **Watson**.

"*The Court also takes note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without his or her knowledge, and unless the data are deleted, he or she should be informed, where practicable, that information is held... as soon as the object of the police activities is no longer likely to be prejudiced.*"

Then he turns to **Klass**:

"*In... Klass... and Weber... the Court examined German legislation which provided for notification of surveillance as soon as that could be done after its termination without jeopardising its purpose. The Court took into account that it was an independent authority, the G10 Commission, which had the power to decide whether an individual being monitored was to be notified of a surveillance measure. The Court found that the provision in question ensured an effective notification mechanism which contributed to keeping the interference with the secrecy of telecommunications within the limits of what was necessary to achieve the legitimate aims.*"

Then they quote those cases and say:

"*In... Association for European Integration and Human Rights... the Court found that the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective. The national law thus eschewed an important safeguard against the improper use of special means of surveillance... By contrast, in the case of Kennedy the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification.*"

So you can see there, Judge, again how within the margin of appreciation different solutions are enabled by the Strasbourg court; you don't *have* to notify if you have a system where you can apply to an independent tribunal for an adjudication without proving that you were under surveillance. If you're *not* in that situation, the obligation to notify is triggered. 15:15

"*289. Turning now to the circumstances of the present*

case, the Court observes that in Russia persons whose communications have been intercepted are not notified of this fact at any *point or under* any *circumstances. It follows that, unless criminal proceedings have been opened against the interception subject and the intercepted data have been used in evidence, or unless there has been a leak, the person concerned is unlikely ever to find out if his or her communications have been intercepted.*"

And that's precisely the position in the United States.

"*290. The Court takes note of the fact that a person who has somehow learned that his or her communications have been intercepted may request information about the... data... It is worth noting in this connection that in order to be entitled to lodge such a request the person must be in possession of the facts of the operational-search measures to which he or she was subjected. It follows that the access to information is conditional on the person's ability to prove that his or her communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive 'information' about the collected data. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure*

prescribed by law, that is, he or she has not been charged or the charges have been dropped on the ground that the alleged offence was not committed."

And he continues then. Then paragraph 291 says: 15:17

"*The Court will bear the above factors - the absence of notification and the lack of an effective possibility to request and obtain information about interceptions from the authorities - in mind when assessing the effectiveness of remedies available under Russian law.*

292. Russian law provides that a person claiming that his or her rights have been... violated... may complain to the official's superior [or] *a prosecutor... The Court reiterates that a hierarchical appeal to a direct supervisor of the authority... does not meet the requisite standards of independence.*"

And it says a prosecutor also lacks independence. 15:17
Then, Judge, if you go forward to paragraph 296:

"*As regards the judicial review complaint under the Judicial Review Act... the burden of proof is on the claimant to show that the interception has taken place and that his or her rights were thereby breached... In the absence of notification or some form of access to official documents... such a burden of proof is virtually impossible to satisfy. Indeed, the*

applicant's judicial complaint was rejected by the domestic courts on the ground that he had failed to prove that his telephone communications had been intercepted... The Court notes that the Government submitted several judicial decisions taken under Chapter 25 of the Code of Civil Procedure or Article 1069 of the Civil Code... However, all of those decisions, with one exception, concern searches or seizures of documents or objects, that is, operational-search measures carried out with the knowledge of the person concerned. Only one judicial decision concerns interception of communications. In that case the intercept subject was able to discharge the burden... because she had learned about the interception... in the course of criminal proceedings...

297... the Court takes note of the Government's argument that Russian law provides for criminal remedies for abuse of power, unauthorised collection or dissemination of information about a person's private and family life and breach of citizens' right to privacy... For the reasons set out in the preceding paragraphs these remedies are also available only to persons who are capable of submitting to the prosecuting authorities at least some factual information about the interception of their communications...

298. The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is... undermined by the absence of a requirement to notify... or an adequate possibility to request and obtain information... Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy."

And it was on that basis that the court found that the Russian system was defective. But obviously the Russian system is whatever it is and I'm sure one can say, viewing the system as a whole, it had deficiencies of a different kind than those in the United States and 15:19
none of these systems are the same. But the essential theory, as it were, of that decision, in our respectful submission, sets out the parameters of the requirement to give notice when it doesn't apply, what happens when it doesn't apply and what *must* be provided in terms of 15:19
remedy to -- or access to an independent tribunal for a remedy.

And I think it's important, Judge, to observe that these decisions are arrived at in the *very* context for 15:20
which Mr. Gallagher contends, Mr. Gallagher and Ms. Hyland contend in this case, namely a proportionality analysis that takes account of the nature of national security surveillance and of the

particular characteristics of it and considerations that have to be brought to bear on it. And even *with* that, they reach the conclusions which I've outlined in terms of standing and in terms of the obligation to notify. 15:20

Then finally, Judge, paragraph -- sorry, tab 46 is **Szabó**. And, yes, these concern members of an NGO which voiced frequent criticism of the government and they challenged the validity of the Hungarian state's national security surveillance powers. And I just want to open, Judge, to you page 28, because they go through a lengthy analysis of the cases up to and including the **Zakharov** case. 15:20

15:21

You'll see here in addressing the entitlement of the applicants to claim victim status, paragraph 38, they say that:

"*Affiliation with a civil-society organisation does not fall within the grounds listed in section 7/E (1) point (a) sub-point and point (e) of the Police Act*" - that was the source of the surveillance power - "*which concern in essence terrorist threats and rescue operations to the benefit of Hungarian citizens in dangerous situations abroad. Nevertheless, it appears that under these provisions* any *person within Hungary may have his communications intercepted if interception is deemed necessary on one of the grounds enumerated in*

the law... The Court considers that it cannot be excluded that the applicants are at risk of being subjected to such measures should the authorities perceive that to do so might be of use to pre-empt or avert a threat foreseen by the legislation especially since the law contains the notion of 'persons concerned identified ... as a range of persons' which might include indeed any person."

And that test, which is a highly diluted one, was sufficient in the circumstances of that case to give standing. And if you go to page 43, paragraph 86, they turn to notice. 15:22

MS. JUSTICE COSTELLO: Page 43?

MR. MURRAY: Page 43, paragraph 86. 15:22

"Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification... As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned."

And I think the, again, unequivocal nature of that statement and its similarity to that in **Watson** is notable.

15:23

"*In Hungarian law... no notification, of* any *kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates that the legislation falls short of securing adequate safeguards.*

87. It should be added that although the Constitutional Court held that various provisions in the domestic law read in conjunction secured sufficient safeguards for data storage, processing and deletion, special reference was made to the importance of individual complaints made in this context... For the Court, the latter procedure is hardly conceivable, since once more it transpires from the legislation that the persons concerned will not be notified of the application of secret surveillance to them."

And in the last part of paragraph 89 they say:

"*Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses*

of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation."

And I suppose, in fairness, it has to be said that all of these cases tend to roll up a whole range of considerations, of which the remedies are but one, in reaching the ultimate conclusions that they do. But I think and would submit, Judge, that the conclusions on the core issues of notification and standing are clear. 15:24

Now, Judge, I just want to turn now to the national security issue. And once again this is an issue which I referred to on Friday. And I think it's very important, Judge, to try and understand the *precise* argument which is being advanced by my Friends. It is an argument which has evolved from the point when the written submissions were delivered. It was certainly our understanding that the case that was made was that the references, Article 4(2), the references -- sorry, Article 4(2) TEU and Article 3(2) of the Directive to national security were to everyone's national security and that effectively, therefore, any issue touching on national security processing in the United States was effectively, for that reason, off limits. That was our understanding of the case that's made, and you'll see it in the written submissions - I don't think it was an 15:25 15:25 15:26

unreasonable one.

So that has now evolved, as I've said, and it's -- and I think first presented in Mr. Gallagher's opening that, well, no, it's not just that, although that case is still being made as we understand it, it's that within the Member States - and this is the point, Judge, to which you adverted at the start of this morning - within the individual Member States there would be no application of the Charter or of the principles to processing for the purpose of national security and, therefore, if we understand the argument correctly, there is no comparator. And although this isn't said, I think the point of conclusion of the argument has to be that effectively the individual Member States in Europe can do as they please when it comes to processing of data for the purpose of national security and that, therefore, the United States system cannot be subjected to any of the scrutiny with which we're concerned, because there's nothing to compare it against. 15:26 15:26 15:27 15:27

That certainly, as we understand it, is the terminus of that argument. Because you'll see in particular in the most recent speaking note -- or sorry, it's not a speaking note, it's, well, the paper produced in response to our speaking note, that there's constant reference to the absence of a comparator. 15:27

The evolution of the argument is not without significance -- oh, I'm sorry, there's one third point which I should advert to, which is now, as presented by Mr. Gallagher, the centrepiece of the national security argument is a case called **The European Parliament -V- The Commission**, which didn't feature in Facebook's submissions to the court *at all*; in fact *we* included it in our speaking note and they have availed of it to say that it actually proves everything that you need to know about national security processing. 15:28

Judge, we don't understand how it can be said plausibly that Article 4(2), when it refers to national security, is referring to the national security of states other than the Member States. We just don't understand how that can possibly be the case. I don't think it's unfair to say that no authority has been cited in support of that proposition. And insofar as the second argument is concerned, the one in relation to comparator, in our respectful submission, as I outlined to you on Friday, it means that *everybody* was wrong when they looked at these issues in, in particular in **Schrems**. But also, going back to the passages in **Watson** which I opened to you this morning, the fact that the court in that case/the Advocate General proceeded with the analysis that he, it and he did makes it very difficult to see how this argument could possibly be well founded. Everybody has overlooked it. 15:28 15:28 15:29 15:29

And I do just, in that connection, want to start off by just reminding the court as to just how many references there are made in the course of, in particular the **Schrems** case, to the national security issue. So if you can turn to tab 36(b) in the first instance. And I've already opened to you this morning Hogan J's judgment - he overlooked this fundamental issue of competence. And if you look at 36(b) you'll see the Advocate General's -- sorry, Judge. You start off at paragraph 25. This, Judge, is page five. Paragraph 25: 15:30 15:31

"*Mr. Schrems lodged a complaint with the Commissioner*" - that's my client - "*claiming, in essence, that the law and practices of the United States offer no real protection of the data kept in the United States against State surveillance. That was said to follow from the revelations made by... Snowden from May 2013 concerning the activities of the United States intelligence services, in particular those of the National Security Agency.*"

And really, if Mr. Gallagher is correct in either version of his argument, the Advocate General really should've been saying 'Well, that's the end of that so. This is nothing to do with us, we've no interest in how the United States proceeds to process information for the purposes of national security'. And, Judge, I do think it is of some significance that at -- I'm subject 15:31

to correction, but I do not believe that at *any* point in Mr. Gallagher's submissions was an explanation given as to *how* these cases could have been determined as they were had that national security argument been addressed, except for the reference which may have been made on one or two occasions that nobody raised it. But with respect, this is at the very centre of the decision of the court in this case. And the argument that's advanced, taken to its conclusion, is that really they just should've said from the start 'This is nothing to do with us', instead of striking down the **Safe Harbour** decision in that and *only* in that context. It makes, with respect, little sense. 15:32 15:32

Paragraph 34 over the page: 15:33

"*Mr. Schrems brought proceedings before the High Court for judicial review of the Commissioner's decision rejecting his complaint. After examining the evidence adduced in the main proceedings, the High Court found that the electronic surveillance and interception of personal data serve necessary and indispensable objectives in the public interest, namely the preservation of national security and the prevention of serious crime.*"

Then if you move on to paragraph 53:

"*As Mr. Schrems states in his observations, for the*

purposes of the complaint at issue in the main proceedings the key issue is that of the transfer of personal data from Facebook... to Facebook... in the light of the generalised access which the NSA and other United States security agencies have under the powers conferred on them by [the legislation]."

Paragraph 199 on page 28:

"*Indeed, the access of the United States intelligence services to the data transferred covers, in a comprehensive manner, all persons using electronic communications services, without any requirement that the persons concerned represent a threat to national security.*"

And if you turn over the page, Judge, to paragraph two -- sorry, if you just look at paragraph 206 at the bottom of that page:

15:34

"*Citizens of the Union whose data has been transferred may approach specialist dispute resolution bodies established in the United States... to request information as to whether the undertaking holding their personal data is infringing the conditions of the self-certification regime. The private dispute resolution carried out by* [such bodies] *cannot deal with breaches of the right to protection of personal data by bodies or authorities other than self-certified*

undertakings. Those dispute resolution bodies have no power to rule on the lawfulness of the activities of the United States security agencies."

But nor, on this construct, do the European courts. 15:35
Then if you turn over the page, you'll see at 210 - and I just emphasise this when we look at the Ombudsman:

"*The intervention of independent supervisory authorities is in fact at the heart of the European system of personal data protection. It is therefore natural that the existence of such authorities was considered from the outset to be one of the conditions necessary for a finding that the level of protection afforded by third countries was adequate; and it is a condition that must be satisfied in order for data flows from the territory of the Member States to the territory of third countries... As noted in the working document adopted by the Working Party established by Article 29... in Europe there is broad agreement that 'a system of "external supervision" in the form of an independent authority is a necessary feature of a data protection compliance system'.*

211. I observe, moreover, that the FISC does not offer an effective judicial remedy to citizens of the Union whose personal data is transferred to the United States. The protection against surveillance by government services provided for in section 702...

applies only to United States citizens and to foreign citizens legally resident on a permanent basis in the United States. As the Commission itself has observed, the oversight of United States intelligence collection programmes would be improved by strengthening the role of the FISC and by introducing remedies for individuals. Those mechanisms could reduce the processing of personal data of citizens of the Union that is not relevant for national security purposes."

I probably have already over-laboured the point, I won't do it any further by going through the equivalent paragraphs in the judgment, but just to identify paragraph 28 and 82 to 87, where again --

MS. JUSTICE COSTELLO: Sorry, what were those numbers? 15:36

MR. MURRAY: Sorry, 28 and 82 to 87. Where again the fact that the court was concerned with US national security data processing and data processing in that context and the legal controls and remedies constructed around that was *central* to the recitation of the facts 15:37 and the outcome. There was *no* and could have been no issue about it.

So how did this happen? How did it come about that the court embarked upon this errand when actually it 15:37 should've been simply pulling the shutters down? And of course, needless to say, not only does it not advert to the competence, if Mr. Gallagher is right that national security means national security *everywhere*, but

actually -- but furthermore, does not engage in any consideration of the law of the individual Member States or any suggestion, well, there's no comparator because in some sense the individual states' national security processing is also off limits. 15:37

So that, I suppose, is the point that I emphasised last Friday and it's the point which, in our respectful submission, means that insofar as the court adopts the view that this argument has any substance at all, it is 15:38 an issue that *has* to be referred. Because for the court to say, as you are being invited to do, 'Well, national security is off limits' could only be to reach a conclusion which is at loggerheads, as I think I said on Friday, with the analysis adopted by the European 15:38 Court. And the extracts from the FRA at pages 10 and 11, which I opened to you on Friday, similarly make that absolutely clear.

The fact of the matter, in our respectful submission, 15:39 is this, and if I can ask you to go back to book one, the Charter -- sorry, the TEU, in Article 16 - and you'll find this in tab two - confers the right to protection of personal data. And it's conferred in terms which are clear and unqualified: 15:39

"*1. Everyone has the right to the protection of personal data concerning them.*"

The Union is conferred with competence by that paragraph. You should note that the following paragraph is qualified:

"*2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.*"

So you start off from the proposition that the Union has competence arising from the first paragraph of Article 16. And how national security relates to that is evident in one case which I think is referred to in my Friends' submissions, which is footnoted in the extract from the FRA report which I opened on the last occasion and it's the **ZZ -v- Secretary of State for the Home Department** (Same Handed). 15:40 15:41

In this case the issue before the court related to and arose in the context of a refusal of leave to enter the UK by an individual who had had permanent resident status and who was subsequently deprived of that status having gone, I think, to Afghanistan and he brought proceedings before the Special Tribunal in the UK 15:41

arising from that and he raised contentions before ultimately, I think, the Court of Appeal, which referred to the Court of Justice, as to whether the procedure operated by the Special Tribunal had been fair and in compliance with his Article 47 Charter rights in circumstances where it had not given a full decision, it hadn't disclosed all of the information on the basis of which ZZ was being refused access to the UK. 15:42

So a similar, not a data protection case, but a case presenting some of the similar issues of national security that arise in the context of national surveillance; you don't want to be -- or, sorry, national security surveillance; you don't want to be telling people who are under surveillance too much about the information you've gathered. And similarly, in **ZZ** they did not wish to provide information in an unadulterated form to him, although it I think it was given to a special advocate who had appeared on his behalf. 15:42

So if you turn to paragraph three you will see, Judge, that:

"*Chapter VI of* [the relevant Directive] *contains provisions relating to restriction by the Member States of the right of entry and the right of residence of citizens of the European Union on grounds of public*

policy, public security or public health."

And if you go forward then to paragraph 22 on page eight, the essential facts are outlined:

"*ZZ has dual French and Algerian nationality... married to a British national since 1990 and the couple had... children... ZZ resided lawfully in the United Kingdom* [and he was given] *a right of... residence.*"

I said he'd gone to Afghanistan; he went to Algeria, it says in the next paragraph, in August 2005.

"*The Secretary of State decided to cancel his right of residence and to exclude him from the United Kingdom on the ground that his presence was not conducive to the public good. SIAC*" - that's the special court - "*stated in its judgment that ZZ had no right of appeal against that decision cancelling his right of residence.*

24... ZZ travelled to the United Kingdom, where a decision refusing him admission was taken by the Secretary of State... Following that decision, ZZ was removed to Algeria. On the date when the present request for a preliminary ruling was lodged he was residing in France.

25. ZZ lodged an appeal... which was dismissed by SIAC

on the basis that that decision was justified by imperative grounds of public security. Before SIAC, ZZ was represented by a solicitor and a barrister of his own choosing...

26. In those appeal proceedings, the Secretary of State objected to the disclosure to ZZ of material upon which he relied in opposition to ZZ's appeal. In accordance with the rules of procedure applicable before SIAC, two special advocates were appointed to represent ZZ's interests. These special advocates had consultations with ZZ based upon the 'open evidence'.

27. Subsequently, the information not disclosed to ZZ upon which the decision refusing entry at issue in the main proceedings was based was disclosed to those special advocates, who were from then on precluded from seeking further instructions from, or providing information to, ZZ or his personal advisers without the permission of SIAC."

Then the special advocates proceeded. So then you'll see over the page at paragraph 30:

"*SIAC dismissed ZZ's appeal, and gave an 'open' judgment and a 'closed' judgment, the latter being provided only to the Secretary of State and ZZ's special advocates. In its open judgment, SIAC held, in particular, that 'little of the case against' ZZ had*

been disclosed to him and that that which had been disclosed did not concern 'the critical issues'."

If you go down to paragraph 34, the matter having come before the Court of Appeal, they referred the question: 15:45

"*Does the principle of effective judicial protection, set out in* [the Directive]... *require that a judicial body considering an appeal from a decision to exclude a European Union citizen from a Member State on grounds of public policy and public security... ensure that the European Union citizen... is informed of the essence of the grounds against him, notwithstanding the fact that the authorities of the Member State and the relevant domestic court, after consideration of the totality of the evidence against the European Union citizen relied upon by the authorities of the Member State, conclude that the disclosure of the essence of the grounds against him would be contrary to the interests of State security?*"

Now, there you can see, Judge, an immediate analogue with the argument that's advanced here insofar as it's said you can't apply the Charter to the German surveillance regime. Here there is a clear national 15:46 security issue in play, it relates directly to the proceedings in which ZZ is involved, and that is raised as the basis on which the national authorities seek to say that the principal effect of judicial protection

doesn't require the disclosure of certain information.

But if you turn over the page, Judge, to the top of the page, they're recording the government's submission. Just the first full paragraph on that page says: 15:46

"*It is clear from Article 4(2) TEU and Article 346(1)(a) TFEU that State security remains the responsibility of solely the Member States. The question... thus relates to an area governed by national law and, for that reason, does not fall within European Union competence.*"

So again, in our respectful submission, the analogy is clear; on Mr. Gallagher's case, if someone were to seek 15:47 to agitate the Charter against the German national security surveillance regime, they would be entitled to say 'Sorry, this is a matter which is outside the competence of the Union. Our data processing for national security process is off limits' -- 'purposes', 15:47 sorry, 'is off limits and to that extent, the Charter doesn't apply, Article 47 doesn't apply'. There *is* no comparator Mr. Gallagher would say.

But that's wrong. And the reason it's wrong is because 15:47 in *this* case the court was concerned with a matter, namely the right of entry of someone who had been a former, a permanent resident, which *is* within European Union competence. And you can't play the trump card of

national security and say 'Well, you simply can't look at this now, none of the rules that would otherwise apply apply'.

And if you see at paragraph 38 -- in fact, maybe I should open all of it. Paragraph 36 says: 15:48

"... *the Court's settled case-law should be recalled according to which, in proceedings under Article 267... which are based on a clear separation of functions between the national courts and the Court of Justice, the national court alone has jurisdiction to find and assess the facts in the case before it and to interpret and apply national law. Similarly, it is* solely *for the national court, before which the dispute has been brought and which must assume responsibility for the judicial decision to be made, to determine, in the light of the particular circumstances of the case, both the need for and the relevance of the questions that it submits to the Court. Consequently, where the questions submitted concern the interpretation of European Union law, the Court is in principle bound to give a ruling...*

37. The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of European Union law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is

hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer...

38. That is not the case here. First, the question referred relates to the interpretation of Article 30(2) of [the Directive], *read in the light, in particular, of Article 47 of the Charter. Second, that question arises in the context of a genuine dispute relating to the legality of a decision refusing entry taken, pursuant to the directive, by the Secretary of State against ZZ. Furthermore, although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable.*"

Now, if you turn over the page, Judge, to page 11, at paragraph 49:

"*It is only*", they say, "*by way of derogation that Article 30(2) of Directive 2004/38 permits the Member States to limit the information sent to the person concerned in the interests of State security. As a derogation from the rule set out in the preceding paragraph of the present judgment, this provision must be interpreted strictly, but without depriving it of its effectiveness.*

50. It is in that context that it must be determined whether and to what extent Articles 30(2) and 31 of [the Directive], *the provisions of which must be interpreted in a manner which complies with the requirements flowing from Article 47... permit the grounds of a decision taken under Article 27 of the directive not to be disclosed precisely and in full.*"

They then say:

"*It is to be borne in mind that interpretation in compliance with those requirements must take account of the significance, as resulting from the system applied by the Charter as a whole, of the fundamental right guaranteed by Article 47... In particular, it should be taken into account that, whilst Article 52(1)... admittedly allows limitations on the exercise of the rights enshrined by the Charter, it nevertheless lays down that any limitation must in particular respect the essence of the fundamental right in question and requires, in addition, that, subject to the principle of proportionality, the limitation must be necessary and genuinely meet objectives of general interest recognised by* [European Union law]."

And that, I suppose, takes us back to a theme of before lunch where *precisely* the analysis which we have urged upon you, Judge, in relation to proportionality is applied; you start off by ensuring that the limitation

respects the essence of the fundamental right and requires, in addition, that, subject to the principle of proportionality, it must meet the relevant test.

"*52. Therefore, the interpretation of Articles 30(2) and 31 of* [the Directive]*, read in the light of Article 47... cannot have the effect of failing to meet the level of protection that is guaranteed in the manner described in the preceding paragraph of the present judgment.* 15:51

53. According to the Court's settled case-law, if the judicial review guaranteed by Article 47... is to be effective, the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him is based, either by reading the decision itself or by requesting and obtaining notification of those reasons, without prejudice to the power of the court with jurisdiction to require the authority concerned to provide that information."

Then he refers to cases, or they refer to cases there.

"*So as to make it possible for him to defend his rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his applying to the court with jurisdiction, and in order to put the latter fully in a position in which it may carry out the review of the*

lawfulness of the... decision...

54... it may prove necessary, both in administrative proceedings and in judicial proceedings, not to disclose certain information...

55. As regards judicial proceedings, the Court has already held that, having regard to the adversarial principle that forms part of the rights of the defence, which are referred to in Article 47... the parties to a case must have the right to examine all the documents..."

Then paragraph 56:

"*The fundamental right to an effective legal remedy would be infringed if* [the decision] *were founded on facts... which the parties* [had not received].

57... in exceptional cases, [if the] *national authority opposes... full disclosure... of the grounds which constitute the basis of a decision... by invoking reasons of State security, the court with jurisdiction in the Member State... must have at its disposal and apply techniques and rules of procedural law which accommodate, on the one hand, legitimate State security considerations regarding the nature and sources of the information taken into account in the adoption of such a decision and, on the other hand, the need to ensure*

sufficient compliance with the person's procedural rights."

Now, of course, if the argument advanced by my Friends was right, actually that would be totally wrong, you wouldn't engage in that exercise *at all*, you would say 'Oh, sorry, this is a situation which, on the grounds of national security, we are *not* providing this information and you have *no* jurisdiction to inquire into whether that's compliant with Article 47 or not, because as the English government argued in this case, national security is off bounds, it's outside EU competence, it is nothing to do with the court'. But that's not the approach taken. 15:53 15:54

And there is, as I said, a direct, in our respectful submission, analogue. Because in the case where the German national security surveillance laws were to be reviewed, they would be reviewed under Article 47, *with, of course*, accommodation of the fact that it's a national security case, as one takes accommodation of *any* particular feature of any specific case which may impact upon the operation of the Charter rights. But you *must* protect the essence of the right. And the court's inquiry is operative irrespective of the fact that is it's a national security case. And if the position were otherwise, this case could not have been decided as it was. And if the position *is* as the case would suggest then my Friends' submission in relation 15:54 15:54

to national security *must* be wrong.

Then they continue at paragraph 61:

"... *the competent national authority has the task of proving, in accordance with the national procedural rules, that State security would in fact be compromised by precise and full disclosure.*"

And the grounds on which the decision was reached. And then it proceeds to observe the independent examination which should be taken into account. And if you turn over the page then, Judge, at paragraph 69: 15:55

"*In the light of the foregoing considerations, the answer to the question referred is that Articles 30(2) and 31 of* [the Directive]*, read in the light of Article 47... must be interpreted as requiring the national court with jurisdiction to ensure that failure by the competent national authority to disclose to the person concerned, precisely and in full, the grounds on which a decision taken under Article 27 of that directive is based and to disclose the related evidence to him is limited to that which is strictly necessary, and that he is informed, in any event, of the essence of those grounds in a manner which takes due account of the necessary confidentiality of the evidence.*"

Judge, we therefore say that the application of the

same principles results in the conclusion stated in the FRA report, which is, of course, that national security data processing *remains* subject to the Charter, subject to the requirements.

15:56

Now, what does that mean? Well, it means first of all, in my respectful submission - I've dealt with this briefly; I think I dealt with it when I opened the case, and we referred to it in our speaking note - there is simply *no* basis on which it can be said national security refers to national security of third party states. That is just, in our submission, a far fetched submission unsupported by authority *or* by the text. But insofar as the second argument is concerned, it's wrong, because in fact the national security surveillance of Member States falls within the Charter and *must* respect the essence of the Charter rights, and therefore, the United States system of national security surveillance must do likewise.

15:56

15:57

15:57

Judge, I want to move on now to deal with the last question on Facebook's case which is on my list and then I need to deal with Mr --

MS. JUSTICE COSTELLO: Well, I think maybe tomorrow might make it more sensible.

15:57

MR. MURRAY: Certainly, Judge. Thank you.

MS. JUSTICE COSTELLO: So eleven o'clock then tomorrow.

MR. MURRAY: May it please the court.

THE HEARING WAS THEN ADJOURNED UNTIL WEDNESDAY, 15TH MARCH AT 11:00

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z

–

—