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, 7th MARCH 2017 - DAY 16

16

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, 7TH MARCH 2017

MS. JUSTICE COSTELLO: Good morning.

REGISTRAR: Matter at hearing, Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 11:04

SUBMISSION BY MR. GALLAGHER:

MR. GALLAGHER: May it please you, Judge. Judge, we do have that folder ready to hand into you shortly, there is a change to be made to the index, but we'll have it today for you that you can put the various documents into. 11:04

MS. JUSTICE COSTELLO: Thank you. 11:05

MR. GALLAGHER: Judge, I was looking at the Privacy Shield, and that was in Book 1 of 13 in my pagination, and I'll also be referring to Book 2 of 13 during the course of the morning. That's the agreed EU authorities. 11:05

MS. JUSTICE COSTELLO: Oh the agreed EU authorities?

MR. GALLAGHER: Yes, sorry.

MS. JUSTICE COSTELLO: Privacy Shield, that's Tab 10, is it?

MR. GALLAGHER: That's Tab -- 11:05

MS. JUSTICE COSTELLO: No.

MR. GALLAGHER: -- 13.

MS. JUSTICE COSTELLO: 13.

MR. GALLAGHER: And I was on page 32 paragraph 140 to

which I drew your attention.

MS. JUSTICE COSTELLO: Yes, I have that, thank you.

MR. GALLAGHER: And I would like to just briefly draw your attention on page 33 to paragraph 145 and following. This provides for the periodic review so that it's apparent the nature of that review: 11:06

"*In the light of the fact that the level of protection afforded by US legal order may be liable to change, the Commission, following adoption of this decision, will check periodically whether the findings relating to the adequacy of the level of protection ensured by the United States under the EU-US Privacy Shield are still factually and legally justified. Such a check is required in any event, when the Commission acquires any information giving rise to a justified doubt in that regard.*" 11:06

And that of course follows from **Schrems**, that adequacy may exist at a point in time but it needs to be monitored to take account of changes in the legal environment. 11:06

And 146: "*Therefore, the Commission will continuously monitor the overall framework for the transfer of personal data created by the Privacy Shield as well as compliance by US authorities with the representations and commitments contained in the documents attached to this decision. To facilitate this process, the US has* 11:06

committed to inform the Commission of material developments in US law when relevant to the Privacy Shield in the field of data protection and the limitations and safeguards applicable to access to personal data by public authorities. Moreover, this decision will be subject to an Annual Joint Review which will cover all aspects of the functioning of the EU-US Privacy Shield, including the operation of the national security and law enforcement exceptions to the Principles. In addition, since the adequacy finding mate also be influenced by legal developments in Union law, the Commission will assess the level of protection provided by the Privacy Shield following the entry into application of the GDPR." 11:07

11:07

To which I referred on the last occasion. And you'll see there are a number of features of that paragraph that are important; the undertaking by the US to inform the Commission of material developments in US law and the limitations and safeguards applicable to access to personal data. So that's an obligation solemnly undertaken and it extends beyond US law. And the relevance of the GDPR, that this in any event is going to be further assessed in the context of the GDPR. 11:08

11:08

And 147: "*To perform the annual review referred to in Annexes I, II and VI, the Commission will meet with the Department of Commerce and FTC, accompanied, if appropriate, by other departments and agencies involved*

in the implementation of the Privacy Shield arrangement, as well as, for matters pertaining to national security, representatives of the ODNI, other Intelligence Community elements and the Ombudsperson. The participation in this meeting will be open for EU DPAs and the representatives of the Article 29 Working Party."

So the review is obviously a very significant formalised feature of the Privacy Shield that will involve the input of all those interested, including the EU DPAs, of which of course the Plaintiff is one, and representatives of the Article 29 Working Party which has that role that is identified in the Directive. 11:08 11:09 11:09

And 148: "*In the framework of the Annual Joint Review, the Commission will request that the Department of Commerce provides comprehensive information on all relevant aspects of the functioning of the EU-US Privacy Shield, including referrals received by the Department of Commerce from DPAs - that's obviously in the context of the Ombudsperson procedure - and the results of ex officio compliance reviews. The Commission will also seek explanations concerning any questions or matters concerning the Privacy Shield and its operation arising from any information available, including transparency reports allowed under the Act, public reports by US national intelligence authorities,* 11:09 11:09

the DPAs, privacy groups, media reports, or any other possible source. Moreover, in order to facilitate the Commission's task in this regard, the Member States should inform the Commission of cases where the actions of bodies responsible for ensuring compliance with the 11:10
Principles in the US fail to secure compliance and of any indications that the actions of US public authorities responsible for national security or the prevention, investigation, direction or prosecution of criminal offences do not ensure the required level of 11:10
protection."

So again that amplifies on what is entailed in the review and the extent of it and its significance, all of which is going to occur imminently and is of great 11:10
significance in relation to the case generally, but also this mootness and hypothetical assumed facts issue that I addressed the court on on the last day.

The significance, therefore, of the manner in which the 11:11
Privacy Shield was arrived at, the nature of the analysis that was undertaken in relation to the adequacy of EU law and the provision for the further review makes it all more difficult to understand, to put it mildly, why the Director or, sorry, the DPC took 11:11
the view that she could not have regard to the Privacy Shield decision in reaching the Draft Decision as the same had not been implemented. It was clearly there in draft form, there was no time limit for the decision

and it was of fundamental importance.

MS. JUSTICE COSTELLO: Mr. Gallagher, have I any indication as to how draft the draft form was or how close it was to the final version?

MR. GALLAGHER: Yes, I can give it to you. There are some changes, there's no doubt about that. But the analysis and the whole approach is precisely the same. But there is a version, I think there's a version showing the changes and I can let you have that. 11:12

I just didn't want to overload you, but the fact that it was coming, the approach that was taken and that it was imminent and that there was input, this came on the 26th July, I think, or 20th July, the decision, as you know, was on 24th May -- 11:12

MS. JUSTICE COSTELLO: Hmm.

MR. GALLAGHER: -- but there was no time limit for the decision. And to make the decision without awaiting what was, on any view, an entirely different analysis, both in methodology, in legal approach and in substance of the adequacy made it in our view, as I say, very surprising to put it mildly as to how it was thought appropriate to even arrive at provisional conclusions without this critical evidence in relation to adequacy. 11:12 11:13

And if I can then, before putting away this decision for the moment, ask you to go back to page 2 of the decision.

MS. JUSTICE COSTELLO: This is the Privacy Shield

decision?

MR. GALLAGHER: The Privacy Shield decision. It's just in fact the first page, the inside of the first page.

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: And you'll see in recital 5: 11:13

"*Pursuant to Article 25(2) of the Directive, the level of data protection afforded by a third country should be assessed in the light of all of the circumstances surrounding a data transfer operation or set of data* 11:13 *transfer operations, including the rules of law, both general and sectoral, in force in third countries in question.*"

That's telling you how you approach this issue. It is 11:13 entirely consistent with **Schrems**, as you will see, and follows the wording of Article 25(2) and its approach, an approach that was not adopted here, rather the novel approach is identified in the Draft Decision and, as explained by Mr. Collins, was that it was appropriate 11:14 to look at one sector remedies, that that was a threshold decision or a threshold in examination, if it didn't pass muster in the remedies that was an end of it. That's not the way that you are entitled to conduct an adequacy assessment and that is clear from 11:14 the decision.

Then if you look at paragraph 11, it is a reference back to paragraph 9 which refers to **Schrems**, and it

says:

"*The Court of Justice criticised the lack of sufficient findings in the decision regarding the existence, in the US, of rules adopted by the State to limit any interference with the fundamental rights of the persons whose data is transferred from the Union to the US, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and the existence of effective legal protection against interference of that kind.*"

So the Commission, noting what **Schrems** says unambiguously, a lack of a sufficient finding in the decision, which was the ratio of **Schrems**, as you know, but the finding and what it should have been embraced is of significance. 11:15

It was a finding in relation to the existence in the US of *"rules adopted by the State intended to limit any interference with the fundamental rights"*, not just the remedies, but the rules intended to limit the interference with the human rights and the existence of effective legal protection against interference of that kind. 11:15 11:16

And then in paragraph 13, the Commission noting what it had done, it has:

"*Carefully analysed US law and practice, including those official representations and commitments. Based on the findings developed in recitals 136 to 140 - to which I have referred you at the end of the day on Friday - the Commission concludes that the US ensures an adequate level of protection for personal data under the EU-US Privacy Shield.*"

And of course the process, which began, as I say, in February with the publication of the draft, then involved the interaction and commenting of various bodies, including the Article 29 Working Party, on that draft before it reached its final form and was finally approved, as you know, by Member States with a number, a limited number of abstentions but no Member State taking issue with it. 11:16 11:16 11:17

Judge, I want to put that aside for a moment and I do want to then look at the decisions in relation to national security, and if I could explain the position in this way so that there is no misunderstanding. I did indicate to you on Friday, and I think we have made it clear in our opening submissions as well, that nobody gainsays that the Directive doesn't have application to the transfer, that is explicit in Articles 25 and 26. 11:17 11:17

The question is how do you assess whether the conditions are fulfilled, and in making that assessment

you need to recognise that the processing, which was the subject of scrutiny by the DPC, is processing in a national surveillance context, as she herself identified, and national surveillance is outside the scope of EU law obviously in the context of the Member States, not just by virtue of Article 3(2) of the Directive but by virtue of Article 4(2) of TEU, Article 5 and also outside the scope of the Charter as a result, Article 6 TEU, Article 51 of the Charter which makes it clear the Charter doesn't extend the scope of EU law. 11:18 11:18

So on any version that is something very important that needs to be considered and it is not considered at all, it's not taken into account in any way whatsoever. That is, we say, a fundamental mistake in and of itself and results in a number of errors which I will highlight as I go through the cases. 11:18

Further, I did make the point that the Directive imposes an obligation to introduce within the Member States a national law that provides the protection for the Directive, but, by definition, that national law doesn't extend to controlling processing by national security in Member States, because that's explicitly outside the scope of the Directive and the Treaty. 11:19 11:19

And when the adequacy assessment is being made, it's an adequacy assessment by reference to primarily in any

event the law of the Member States because that is assumed to have implemented the Directive, and there's no suggestion that any Member State has not implemented the Directive. But the law of the Member State excludes, as I said, national surveillance, national security surveillance, and there is no comprehensive law of the type referred to by the DPC by way of criticism of the system in America dealing with national surveillance in the Member States. 11:20

Indeed, it is clear from the evidence before the court that there are significant variations in the national legal systems in that regard and, as I said, on any version the law of the US is as good as best in class and perhaps better than any of them and is the benchmark for that law. That critical aspect is entirely ignored. 11:20

Judge, it is --

MS. JUSTICE COSTELLO: I just want to understand this at an abstract level. You are saying the Directive excludes national security for the Member States? 11:21

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: So when you're looking at transfer to a third country, we won't say America. 11:21

MR. GALLAGHER: Yes, whatever country.

MS. JUSTICE COSTELLO: Whatever country, and it could be a country that's a very intolerant régime or it could be a highly liberal protected régime.

MR. GALLAGHER: Yes.
MS. JUSTICE COSTELLO: It will have its own national security laws which will permit it to a lesser or greater extent to survey the intelligence, and are you saying that there is no comparator to what occurs in the third country within the Union because (a) it is excluded from the Directive and (b) it is fragmentary because it reflects the 29 or 28 different states or whatever it may be. 11:21
MR. GALLAGHER: That's precisely it. And it's not only excluded from the Directive, it's excluded from the scope of EU law, so EU law -- 11:21
MS. JUSTICE COSTELLO: And regardless of whether it's in an oppressive régime or a liberal régime, if I can use a parameter. 11:22
MR. GALLAGHER: Yes. I suppose if you take it in two stages.
MS. JUSTICE COSTELLO: That's a matter of principle as opposed to what happens in the third country.
MR. GALLAGHER: Yes, that's correct. Obviously any assessment of adequacy will take account of the features of the particular country in respect of which the assessment is made. Similarly, as I explained when you come to the SCCs, the features of the particular country may be relevant, but I'll leave that aside for the moment. 11:22 11:22

Within the EU there is one factor that you will be aware of and that I have mentioned already; while the

national security law is outside the scope of EU law, every Member State subscribes to the European Convention on Human Rights. The European Convention of Human Rights does impact on national security laws within the Member States, it defines in a sense the boundaries and the scope of those for the very, I suppose, obvious reason, or the reasons certainly articulated by the court, that it doesn't allow a Member State to say 'I'm doing this in the name of national security, I'm taking all your rights away' and that would mean the Convention had no application. 11:22 11:23

So, as you will see, and as Ms. Hyland will elaborate in terms of the cases, the ECHR *does* exercise a jurisdiction with regard to the scope of national security. That's part of the laws of the Member States. But the national laws, which provide for national security surveillance, are set out in the domestic laws of each of the Member States in the absence of a finding that they are inconsistent with the ECHR, they are there and they are the laws of the Member States. 11:23 11:23

I'll come and very briefly refer to them, Ms. Hyland will deal with that in more detail, but I did, for example, instance for you on Friday the example at page 67 of the from a of the challenge before a federal administrative court in Germany by an applicant who said he was objecting to the surveillance carried out 11:23

by the BND, which is the organisation in Germany that carries it out. They had used some dragnet search operation or collection operation to collect 32 million communications of which it transpired only 12 were actually relevant to national security. The particular plaintiff couldn't prove that his was one of those 32 million communications and his claim failed and the court said 'it doesn't matter that you can't prove that you were the subject of that, the fact is you cannot prove it and your claim failed'. 11:24

So the laws in the Member States, obviously only some Member States have developed national security apparatus: Germany is one, France is another, Holland is another, the UK is another, France [sic] is another, Spain is another, Italy is another, the smaller Member States would be less significant in terms of their examination of communications in the context of national security. 11:25

So that is the position in the Member States. It's a position that derives from their own domestic laws subject ultimately to the ECHR - I'll say the ECHR, the Convention - and the limitations that it imposes on the scope of national security. So that is the position, but that derives, not from European law, but from the domestic law and the Convention. 11:25

The European court initially followed that very easily

and very understandably in the **European Parliament** case that I'll open in a minute. In more recent cases the position is less clear in the context of the European court decisions with regard to the precise boundaries of the interaction between European law and national surveillance law. 11:26

But one thing is very clear: If you adopt the principles of **Schrems**, of **Watson**, of **Digital Rights**, and of the approach taken by the Commission in the Adequacy Decision, and even accepting that for the sake of argument, which I do for the sake of the argument I'm now going to make and develop. 11:26

The approach is an approach that merely examines whether the régime of national security surveillance that includes the substantive law, the limitations on the safeguards and the remedies go no further than is strictly necessary. That is very much analogous to the approach taken by the ECHR when examining whether something is exempted under national security law. 11:26 11:27

And if I may call that for simplicity the *strictly necessary* approach. And you will remember from the passages of the Privacy Shield decision that I drew your attention to on the last occasion, in particular paragraphs 136 to 140 and paragraph 140 in particular, the EU or the Commission decided that US law with regard to national surveillance went no further than 11:27

was strictly necessary and therefore it met the adequacy test. That happens to be similar, as I say, to the approach, if not identical to the approach that the ECHR would take in examining the laws of the Member States. 11:28

What it did not do was examine Article 47 in the abstract or in isolation and say 'we'll have a look at the remedies and we'll have a big argument over the remedies and the extent of them and if we don't think 11:28
those remedies are sufficient judged in the abstract we'll say the law is inadequate'. It doesn't do that, and one feature of the Adequacy Decision is it identifies the limitations and the remedies that you have heard, including the standing limitation. There's 11:28
an argument about the extent of those as you know, but, leaving that aside for the moment, even taking the DPC's evidence as its highest, this is something that is taken into account by the Privacy Shield.

11:28

So it takes all that into account, it concludes that US law goes no further than is strictly necessary and then it concludes that it is adequate in terms of the public law and that meets the requirements of Article 25 assuming that is the test. 11:29

That is *entirely* consistent with **Schrems**, it is entirely consistent with **Watson**, it is entirety consistent with **Digital Rights**, but it is entirely

inconsistent with the approach which the DPC took in this case. It recognises that national security is in a different category, that it is assessed differently, that in looking at its remedies you're not looking at the remedies provided by the Directive, you're not looking at a wholesale entitlement to sue somebody without limitation where there is some infringement of a data right. It requires you to look at, not only the protections laid down in law, but all of the limitations that are in fact applied in practice, all the matters that go to protecting the rights and in the end the question is do the restrictions on the protection of the rights, infringements if you wish to call it that, but I think it's better to say limitations or restrictions on the protection of data protection rights or, sorry, of data rights go further than is strictly necessary. And that's precisely how it is approached and I hold that in up in entire contradistinction to the DPC's approach and as a basis for invalidating that approach. 11:29 11:30 11:30 11:30

So that's taking the law in terms of **Schrems** and in terms of the Privacy Shield, though issues do arise that haven't been fully canvassed in recent cases as to whether even the EU can go that far in terms of its analysis. That's a matter obviously for the European court, if the matter should ever get there, and I want to preserve those arguments. But I'm taking it at its highest in terms of the existing law and dealing with 11:31

it that way and that's what I intend now to do, if I may.

So the European - sorry, in my book it's the second of the agreed authorities and the decision is in divide, 11:31
sorry, 26 and it is the **European Parliament -v- European Data Protection Supervisor**.

So this reaffirms and establishes the points I make
which are Member States are not bound by their charter 11:31
when they are conducting or regulating national security surveillance because this is an activity which is expressly placed outside the purview of Union law and beyond the competence of the CJEU and there is
nothing in any of the cases which undermines that 11:32
fundamental position.

If you go to the European Parliament, this was a decision in which the European Parliament challenged a
decision of the Commission and the Council and it 11:32
sought their annulment. If you go to page 4798 and paragraph 2 you will see - sorry, paragraphs 1 and 2 - an annulment of a Council decision and an annulment of a Commission decision relating to whether adequate
protection of personal data was contained in the 11:32
passenger name record of air passengers transferred to the US Bureau of Customs and Border Protection, which is referred to as CBP in the case, and passenger name record is PNR. A decision was made following 2011 that

this information or this data could be transferred and that it benefitted from adequate protection.

There's an analysis initially of the Directive that you are concerned with and then there's a more detailed analysis of the decision. If you go to 4811. 11:33

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: You will see in paragraph 21 the 11th recital to the decision adopted by the Commission with regard to adequacy states that: 11:33

"*The processing by CBP of personal data contained in the PNR is governed by conditions set out in various Undertakings and in United States domestic legislation to the extent indicated in the undertakings.*" 11:34

And an analysis of the type that was carried out by the Commission in the Privacy Shield is then conducted in relation to the various undertakings over the next ten or so pages. And one doesn't need to deal with the substance of that but go, if you would, to page 4822 and paragraph 33 and it explains the background to this issue, the 2001 attack on the Twin Towers. 11:34

Then it describes the decisions of the Commission and the Council, I don't think we need to delay on it, and if you go to 4826 you will at paragraph *30* at the top of the page. 11:34

MS. JUSTICE COSTELLO: I think that's 50.

MR. GALLAGHER: 50, sorry, 50 at the top of the page: "*That the Parliament advances four pleas for annulment, respectively ultra vires action, breach of fundamental principles of the Directive, fundamental rights and principles of proportionality.*" 11:35

And in 52 it says: "*In the parliament's submission, there is no doubt that the processing of PNR data after transfer to the US authority covered by the decision on adequacy is, and will be, carried out in the course of* 11:35 *activities of the State as referred to in paragraph 43 of the judgment.*"

So it said this is ultra vires, EU law doesn't extend this far, this is being transferred in the course of 11:35 activities of the State. And then you'll see 54:

"*The first indent of Article 3(2) of the Directive excludes from the Directive's scope the processing of personal data in the course of an activity which falls* 11:35 *outside the scope of Community law, such as activities provided for by Titles V and VI of the Treaty on European Union, and in any case processing operations concerning public security, defence, State security, activities of the State in the area of criminal law.*" 11:36

And in 55: "*The decision on adequacy concerns only PNR data transferred to CBP. It is apparent from the sixth recital in the preamble to the decision that the*

requirements for that transfer are based on a statute enacted by the US in November 2001 and on implementing regulations adopted by CBP under that statute. According to the seventh recital in the preamble, the United States legislation in question concerns the 11:36
enhancement of security and the conditions under which persons may enter and leave the country. The eighth recital states that the Community is fully committed to supporting the US in the fight against the terrorism within the limits supposed by Community law. The 15th 11:36
recital states that PNR data will be used strictly for purposes of preventing and combating terrorism and related crimes, other serious criticisms, including organised crime, that are transnational in nature, and flight from warrants or custody for those crimes." 11:37

And over the page:

"56. It follows that the transfer of PNR data to CBP constitutes processing operations concerning public 11:37
security and the activities of the State in areas of criminal law.

57. While the view may rightly be taken that PNR data are initially collected by airlines in the course of an 11:37
activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision

on adequacy is, however, quite different in nature. As pointed out in paragraph 55 of the present judgment that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law enforcement purposes."

MS. JUSTICE COSTELLO: Can I just, I want to get this straight in my head. In this case Facebook Ireland will transfer data to Facebook Inc. and the vast majority of that has nothing to do with national security and it's for what we have broadly described as commercial purposes. 11:38

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: In this case the airlines were taking a record of the, what's it called again, the PNRs. 11:38

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: But that was initially for their commercial purposes --

MR. GALLAGHER: Exactly. 11:38

MS. JUSTICE COSTELLO: -- within the airlines?

MR. GALLAGHER: Exactly.

MS. JUSTICE COSTELLO: But then were they obliged to transfer it, the data that they had obtained for themselves? 11:38

MR. GALLAGHER: To get into the US and to land in the US they were obliged under US legislation to do it because the US wasn't prepared to receive their --

MS. JUSTICE COSTELLO: That's a transfer that wouldn't

have occurred but for that?

MR. GALLAGHER: Oh, absolutely. And I'm going to draw your attention, this is not an Article 25 transfer, this is different. What is critical, however, is the focus in paragraph 57 on the two stages. 11:39

MS. JUSTICE COSTELLO: Mm hmm.

MR. GALLAGHER: One, the initial collection, and in this case of course the initial collection and the transfer, and then the separate aspect which is the data processing that subsequently takes place which is 11:39 done for national security purposes.

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: So the transfer there is a requirement, if you want to, I suppose US law couldn't extend to oblige them to do anything, but if commercially you 11:39 wanted to land your planes you had to do it, but there is undoubtedly a distinction.

But the separate distinction, which is the one I want to emphasise for the moment that is not detracted from 11:39 in any of the cases, and in fact this case is referred to in the **Digital Rights** case without any suggestion that it was wrongly decided or that the exception which it recognises doesn't apply. There was then the subsequent processing in the US which was part of 11:40 public security.

And then it goes on, 58:

"*The court held in paragraph 43 of **Lindqvist**, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Article 3(2) of the Directive are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals.*"

Those are the national security etc.: "*However, this does not mean that, because the PNR data has been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by the provision. The interest rate falls within a framework established by the public authorities that relates to public security.*"

So to explain that as I understand it, the transfer is being done within a framework established by public authorities that have agreed to this as a security measure, so the transfer is on a different basis than that with which we are concerned here.

But the processing which is being declared to be adequate and which is the subject of the decision is a processing as part of a State activity by a State authority and the Directive does not apply to these activities of the States and State authorities unrelated to the fields of activity of individuals.

So when you come to look at what occurs subsequent to the transfer, and the processing that is done in the US, that is outside the scope of the Directive.

MS. JUSTICE COSTELLO: And you are saying that applies, that includes a third country state? 11:42

MR. GALLAGHER: Exactly. And the US happens to be the third country state here in this case and also in the present case.

And 59: "*It follows from the foregoing considerations that the decision on adequacy concerns processing of personal data as referred to in the first indent.*" 11:42

So the processing is the processing by the US, that is by a state authority, so the decision concerns that and the decision, therefore, does not fall within the scope of the Directive. 11:42

So that is obviously a very important decision highlighting the limit of the scope of EU law consistent with the Directive and consistent with any examination of the processing carried out by the US authorities which of course was the subject of the examination by the DPC in this case and of course the subject of the examination by the Commission in the Privacy Shield. 11:42 11:43

And then it goes on, 60:

"Accordingly, the first limb of the first plea, alleging that the first indemnity of Article 3(2) of the Directive was infringed, is well founded.

61. The decision on adequacy must consequently be annulled and it is not necessary to consider the other limbs of the first plea or the other plea relied upon by the Parliament."

So if the law related there you wouldn't look at this law, the law doesn't stop there. There are later decisions that the court of course must take account of, but that decision in terms of the principle of the different stages of the processing and the differences between what you are looking at when you are looking at processing within the EU and processing by the US state in the field of national security have not been elided in any of the decisions, in fact the distinction has been respected, albeit the approach has been different.

Then if you go to the challenge by Ireland to the 2006 Directive in divide 30, the 2006 Directive which was ultimately invalidated in **Digital Rights**, was challenged on a different ground by Ireland and it's a subject matter of this decision in 2009. Ireland had challenged it on the basis that the legal basis for the Directive was wrong, that Article 95, which dealt with developing the single market, didn't provide an appropriate legal basis for Directive 2006. It's a

narrow challenge that set out in the summary. The second paragraph refers to the purpose of Article 95, the third paragraph to the fact that there were differences between the national rules adopted on the retention of data relating to electronic communications which were liable to have direct impact on the functioning of the internal market, and it was foreseeable that that impact would become more serious within the passage of time. 11:45

And then it says: "*Furthermore, the Directive regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters, which fall, in principle, within the area covered by Title VI of the EU Treaty have been excluded from the provisions of the Directive. It follows that the substantive content of the Directive is directly essentially to the activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty, as it then was. In light of that substantive content, it must be held the Directive relates predominantly to the functioning of the internal market.*" 11:45 11:46 11:46

The Directive is summarised on page 3 and you will see, perhaps over on page 2 an equivalent article, sorry it refers to Article 3(2) of Directive 95/46, it then goes on to this Directive, sorry to the e-privacy directive, not this Directive, the 2002/58, which are the substantive provisions relating to data protection. And the Privacy Directive concerns the processing of personal data, the protection of privacy in the electronic communications sector with a view to supplementing Directive 95/46. 11:46 11:47

And under Article 6(1) of that Directive certain obligations are imposed. Article 15(1) says:

"*Member States may adopt legislative measures to restrict the scope of the rights and obligations provided by Articles 5 and 6 and those other Articles when such restrictions constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security.*" 11:47 11:47

That's similar to Article 13 of Directive 95/46 but different in a way that I'll come back to later and the various other provisions of that Directive are set out. 11:47

Then you come over the page to the paragraph, sorry I think it begins on page 3, it begins just after my reference to Article 15(1), Directive 2006/24 --

MS. JUSTICE COSTELLO: Hmm.

MR. GALLAGHER: -- which sets out what its provisions are and over the following pages sets them out in more detail.

11:48

And then you'll see in paragraph 23 on page 6, at paragraph 24 excuse me: *"Ireland claims that the court should annul the Directive on the ground that it was not adopted on an appropriate legal basis."*

11:48

Then you can go to page 11, if you would be kind enough, and the bottom three paragraphs refers again to the nature of the challenge. Paragraph 87, the second last paragraph says:

11:49

*"In paragraph 68 of the judgment in **Parliament -v- Council and Commission**, the Court held that the agreement related to the same transfer of data as did Commission Decision on the adequate protection of personal data contained in the passenger name records."* 11:49

And 88: *"The latter decision concerned the transfer of passenger data from the reservation systems of air carriers situated in the territory of the Member States to the US Department of Homeland Security and the Court held that the subject-matter of that decision was data-processing which was not necessary for a supply of services by the air carriers, but which was regarded as necessary for safeguarding public security and for law* 11:49

*enforcement purposes. In paragraphs 57 to 59 of the judgment in **Parliament -v- Council Commission**, the Court held that such data-processing was covered by Article 3(2) of the Directive, according to which that Directive does not apply, in particular, to the processing of personal data relating to public security and the activities of the State in the areas of criminal law. The Court accordingly concluded the decision did not fall within the scope of the Directive."* 11:50

And 89: *"Since the agreement which was the subject of Directive 2004/496 related, in the same way as that decision, to data-processing which was excluded from the scope of Directive 95/46, the Court held the decision could not have been validly adopted on the basis of Article 95.* 11:50

90. Such a line of argument cannot be transposed in relation to this Directive." 11:50

And in 91: *"Unlike the decisions which are under challenge in **Parliament -v- Council and Commission** which concerned a transfer of personal data within framework instituted by public authorities in order to ensure public security, the Directive covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law-enforcement purposes."* 11:50

So it said this Directive 2006 related to activities of electronic communications service providers within Europe and therefore the Directive could be introduced to harmonise the laws relating to that. It didn't cover the activities of or didn't contain any rules governing the activities of public authorities. 11:51

But no suggestion that **Parliament -v- Council** is in any way wrongly decided with regard to its understanding as to the scope of Article 3(2) of the Directive or the distinction it draws between State processing in the national surveillance sphere; however, it does draw the distinction that the ultra vires of course depended upon the fact that the transfer was being done by State authorities and that was the ratio of that case. 11:51 11:52

Then, Judge, if you come to the **Digital Rights** case which you'll find in divide 35 and if you would be kind enough to go to the court's decision which is in the same divide and it's about a little over half way through. You'll see the judgment of the court on the 8th April 2014. 11:52

I don't know whether you have managed to find that, Judge. They were joined cases, one relating to -- 11:52

MS. JUSTICE COSTELLO: I have internal divider so...

MR. GALLAGHER: Oh good.

MS. JUSTICE COSTELLO: Is it 8th April 2014?

MR. GALLAGHER: That's it, Judge, the report of the

case.

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: And there were two referrals, one, I think, from Germany and one from Ireland. You'll see on page 3 it sets out the legal connection of 94/46, then again the EU Privacy Directive and sets out various provisions of that which you have seen in the other case and then Directive 2006/24. But could I draw -- that's on page 5. 11:53

MS. JUSTICE COSTELLO: And which one was that one again? The numbers I glaze over. EU privacy was 2002. 11:53

MR. GALLAGHER: 2002.

MS. JUSTICE COSTELLO: 2006 is which one?

MR. GALLAGHER: Is the one that we just looked at in the context of Ireland's challenge. It was the measure harmonising the retention provisions in the Member States. 11:53

MS. JUSTICE COSTELLO: It's retention. I know it's the one we just looked at, I am just trying to remember what it was called. 11:53

MR. GALLAGHER: Yes, it is very confusing. And it may assist, Judge, if I just go back for a moment to Article 15, to paragraph 10 on page 5, which refers to Article 15 of the EU Privacy Directive.

MS. JUSTICE COSTELLO: Yes. 11:54

MR. GALLAGHER: And I said that this was in similar terms to Directive 95/46 --

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: -- to Article 13, but there is one

important difference that I want to draw your attention to.

And it says: "*Member States may adopt legislative measures to restricting the scope of the rights and obligations provided by those Articles of the EU Privacy Directive when such restrictions constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty of European Union.*"

11:54
11:54
11:55
11:55

Article 6(1) and (2) of the Treaty on European Union refer to the general principles of Community law and the Charter. So this is a sentence that is missing from Article 13 of 95/46. It is specifically limiting the measures that may be introduced in terms of their having to comply with this provision and this is

11:55

something that is obviously ultimately very relevant to its assessment of the validity of Directive 2006 which is the harmonising measure dealing with restrictions on the scope and rights and obligations in the ePrivacy Directive.

11:56

You'll see then it explains in 11 that the harmonising Directive: *"After having launched a consultation with representative law enforcement authorities, the electronic communications industry and data protection experts on 21 September 2005 the Commission presented an impact assessment of policy options in relation to the rules on the retention of traffic data ('the impact assessment'). That assessment served as the basis for the drawing up of the proposal for a directive of the European Parliament and of the Council on the retention of data [processed] in connection with the provision of public electronic communication services and amending Directive 2002/58."*

11:56

Then if you go to next paragraph 12: *"Recital 4 of the preamble to the Directive says: Article 15(1) of Directive 2002/58 sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in those Articles of the Directive. Any such restrictions must be necessary, appropriate and proportionate et cetera."*

11:57

You are familiar with that provision.

Then it goes on: "*According to the first sentence of the recital in the preamble to the Directive under consideration 'several Member States have adopted legislation providing for the retention of data by service providers for the prevention, instigation, detection and prosecution of criminal offences'.*"

And then the recitals go on to say: "*The Conclusions of Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in investigation.*" 11:57

Etc. It goes on to refer to recital 16, 21 and 22 on the next page. In paragraph or recital 21 I'd like to refer to in particular, which is contained in paragraph 15 half way down the page.

MS. JUSTICE COSTELLO: I have it. 11:58

MR. GALLAGHER: "*Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and protection of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at* 11:58

Community level, the Community may adopt measures, in accordance with the principle of subsidiarity set out in the Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that purpose."

You'll be familiar with that concept. It was, as I say, scrutinised in the challenge by Ireland to the validity of the Directive as to whether the proper legal basis was 95 and that it was contributing to the integration of the single market. But one of the constraints on the Community acting is of course where something can be better done by individual Member States it cannot act. All of those matters were thrashed out, if I may use that perhaps inelegant expression, in the Irish challenge and this is reciting the fact that that legal basis for the Directive and its ultimately relevant to how the court approaches the matter. 11:58 11:59 11:59 11:59

And then in paragraph 16, the subject matter and scope of the Directive, it aims to harmonise Member States provisions in the manner to which I drew your attention in the context of the recitals. 11:59

And I think we can move then to paragraph 34, Judge, and on page, excuse me, it's 18.

MS. JUSTICE COSTELLO: I think it's 15 if it's 31.

MR. GALLAGHER: Sorry, it's 15, my sight is failing me, I do apologise. It's 15 and 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.*" 12:00

And it refers to those decisions, and I think the stenographer wants to change. 12:00

Reiterating the principle that data, whether it's sensitive or not, is obviously protected by the Directive. Then 34: 12:01

"*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 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.*"

Then if you go over the page, at 44 on page 17, having reviewed the issue in the opposite page of the justification of the interference with the rights

guaranteed by Article 7, the court concludes:

"*It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by* [the Directive]*, genuinely satisfies an objective of general interest.*"

So in principle it is valid, it satisfies an objective general interest - in this case specifically criminal law and enforcement of criminal law. 12:02

Then it says the next step, in paragraph 45, is it's necessary to verify the proportionality of the interference found to exist. And it refers in paragraph 46 to the settled case law of the court that the principle of proportionality requires "*that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.*" 12:02

Then in 47:

"*With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a*

number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference." 12:03

Then if you'd be kind enough to go to the next page and paragraph 54. It says:

"*Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.*"

Then 55:

"*The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.*"

Then 56: 12:04

"*As for the question of whether the interference caused by* [the Directive] *is limited to what is strictly necessary, it should be observed that, in accordance*

with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all *traffic data*" - and that's very important - "*concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony.*"

Right across the, I suppose, spectrum of electronic communications.

"*It therefore applies to* all *means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of* [the Directive]*, the directive covers* all *subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.*"

And that paragraph is significant in terms of the court's conclusion as to what is strictly necessary. 12:05
And if you go on to 58:

"[The Directive] *affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link,*

even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."

Then if you go on to 59:

"*Moreover, whilst seeking to contribute to the fight against serious crime,* [the Directive] *does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.*

60. Secondly, not only is there a general absence of limits in [the Directive] *but* [the Directive] *also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view*

of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, [the Directive] *simply refers... in a general manner to serious crime, as defined by each Member State in its national law.*"

If I can refer you to 62:

"*In particular,* [the Directive] *does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.*"

And finally, if I may, 65:

"*It follows from the above that* [the Directive] *does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that* [the Directive] *entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.*"

Now, to then perhaps derive the principles that emerge from that case and to see how the Commission has taken them into account in its examination of the Privacy Shield. First, of course, a critical distinction recognised in the cases and in all of the analysis is this concerned the criminal law and not national security as such. And that does have an impact on the nature of the limitations and safeguards and also potentially on the remedies. 12:08 12:09

Secondly, the court held the objective was a legitimate objective. And then it carried out an analysis as to whether the obligations imposed were strictly necessary to achieve the objective. That is the approach that was taken by the Commission in the privacy decision, but not taken by the DPC in this case. 12:09

Thirdly, the data retention was generalised, bulk by its nature, it applied, as the paragraphs that I've referred you to demonstrate, to practically the entire European population and without any differentiation and, therefore, even to those without any link to serious crime. It made no exception in respect of obligations of professional secrecy. The data to be retained was not limited. There was no objective criterion set which determined in respect of which forms of serious crime national authorities could retain the data. There were no substantive or procedural conditions established to regulate national authorities' access to and use of the retained data. No objective criterion was laid down to limit the number of persons authorised to access and use retained data, and such access and use was not dependant on a prior review carried out by a court or independent administrative body. All data was to be retained for a period of six months, regardless of the data in question and its usefulness and, therefore, regardless of its necessity. No safeguards were established or required for the security and protection of the retained data in the light of risks of abuse and unlawful access and, to the contrary, service providers seemed to determine the levels of security to be applied having regard to economic considerations. And there was no system of oversight.

12:09 12:10 12:10 12:10 12:11

These were all the factors taken into account in

determining that issue, in the context, as I emphasise, of criminal law and in a context where the very terms of this exception from the E-Privacy Directive provided restrictions. And those restrictions are, as I identified for you, in Article 15 of the E-Privacy Directive, back on page five, paragraph ten, where the measures referred to had to be in accordance with the general principles, including those referred to in Article 6. 12:11

There's no equivalent provision in 95/46 relating to national security for very obvious reasons, that's outside the scope of EU law. But here, the very derogation by which Member States fixed their laws with regard to retention and which the Community, as it then was, was now legislating for through the Directive was constrained in that express way. And of course, what the court was pronouncing on, which it must always have jurisdiction to do, was the validity of a Directive. 12:12

So that is the **Digital Rights**. It's undoubtedly of importance. It doesn't decide the issue in this case, but it is important in showing that even where those other circumstances are concerned in terms of the different wording of the relevant legislative provision, the different subject matter, the strictly necessary approach is adopted. 12:12

Then that approach is, you'll see, referred to in the

Schrems decision. And I'm very conscious the court has looked at the **Schrems** decision, but there are some other paragraphs that I think in the light of this argument are perhaps relevant to refer the court to which no emphasis has been laid already and perhaps one or two just to mention again in this context to which your attention has been drawn, but without, I hope, repeating anything that has been said and I know the court will ask me to move on if I unintentionally do that. 12:13

You can go to, it's the next divide and you can go to page 15 and paragraph 31. And something that's very important to another matter that I'll come back to, and I hope I won't forget to do so, but I'll do it in the context of national security when I look at some of the evidence, the important issue that you raised, Judge, as to, for example, how Upstream works and the fact that if it carries out a search of a wide body of data, what is the significance of that, even if it is targeted? And I'll come back to that and show how Upstream, as it's explained in detail in pages 35 and 36 of the PCLOB report, is so wholly different to what was envisaged by the court in **Schrems** that it will (A) answer your question and (B) emphasise a very important distinction that is, of course, embraced and acknowledged in the Privacy Shield by the Commission, and I'll refer you to those paragraphs as well. 12:13 12:14 12:14

But it's very important, we say with the greatest of respect, that the facts set out by the High Court that were the subject matter of the reference were on the basis of newspaper reports which interpreted the revelations of Mr. Snowden to mean that PRISM and other programmes had enabled NSA to engage in bulk or generalised collections. And that certainly is, of course, a decisions, as Ms. Barrington's decisions urged on the court -- and I think I forgot to, I should've said I, of course, adopt all of Ms. Barrington's decisions on behalf of the US, as I think is already clear from the emphasis we place on the Privacy Shield and the facts and law set out therein. 12:15 12:15

But in paragraph 30, you will see that the High Court, in the last sentence, the CJEU refers to the fact that "*it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.*" 12:15

And 31:

"*According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an ex parte and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the*

NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale."

The court in **Schrems** was not provided with evidence of the considerable changes in US law consequent upon the 2013 Snowden revelations, nor did it consider whether there was any real or effective privacy protections offered in European states when the interference with privacy is justified on national security grounds -- 12:16

MS. JUSTICE COSTELLO: Can I just be clear what you say is, in the light of the evidence I have heard, factually incorrect here? Do you take issue with the first sentence? 12:16

MR. GALLAGHER: I do.

MS. JUSTICE COSTELLO: And then the second sentence, I think you probably accept, in the sense that "*Oversight of the intelligence services' actions is carried out within the framework of an ex parte and secret procedure*"; that's the FISA court, isn't it? 12:17

MR. GALLAGHER: It is. But it's a completely inadequate description of --

MS. JUSTICE COSTELLO: No, well, I accept that. But then the next sentence: "*Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies*"; as a matter of capacity, that's correct, isn't that right? 12:17

MR. GALLAGHER: It is. But it is --
MS. JUSTICE COSTELLO: And then -- so your issue is with the indiscriminate surveillance and interception?
MR. GALLAGHER: Exactly. And interception. That is the critical one. And also, if you go back - and I don't want to delay the court - there's some references to that in the Commission communication to Parliament as well. 12:17
MS. JUSTICE COSTELLO: Mm hmm.
MR. GALLAGHER: But if you took that paragraph, while some of the sentences are *literally* correct, they of course don't disclose the process and they don't disclose the nature of the protections. I mean, all you're told is that the oversight is ex parte and a secret procedure. There's no understanding of how the court operates, the significance of the FISC court, nor is there any understanding of the other oversights, there is no understanding of all the evidence before this court, not only by reference to the official reports, but by the evidence of Mr. DeLong and Prof. Clarke as to how these surveillance actually operate and the limitations on it. And those are matters that I will refer to. 12:17 12:18 12:18

But the impression created was of bulk indiscriminate collection and interception. And the scale of it was, of course, misdescribed; the US Government wasn't a party, Facebook was not a party. And therefore, the evidence that is *now* available to this court and the 12:18

evidence that was available and considered by the Commission is obviously of a very different nature.

So I do make the point, and it's an important point, you can, of course, refer to something in a way that's *literally* correct but the substance is not properly explained and it is misleading - not in any intentional way; there could be no criticism, there wasn't the evidence before the court, but the factual basis was very different. 12:19

MS. JUSTICE COSTELLO: I just wanted to focus on, be clear --

MR. GALLAGHER: No, and a very important --

MS. JUSTICE COSTELLO: -- as to where your issues were.

MR. GALLAGHER: -- a very important question, Judge. 12:19 And I'll come back to that in a little bit more detail.

If you look at 33:

"*The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle.*"

You'll see how the Commission deal with that and how that is dealt with and I'll come to that in a moment. 12:19 That is not an accurate description of how the surveillance is conducted. And then there is a reference to the Irish Constitution.

Judge, could I just ask you, to make the point, as it is an important point, to draw attention to the different factual basis in the Adequacy Decision itself and just give you the reference to a number of paragraphs that are relevant in that context? 12:20

MS. JUSTICE COSTELLO: By this you mean the Privacy Shield?

MR. GALLAGHER: The Privacy Shield Decision, which is, in that first book, divide 13. It's so that you'll have them. They've been referred to in a different 12:20 context, but I think it is important that you be given them in this particular context.

Firstly, you'll remember paragraph 82 to which I've already made reference, that's on page 18 of the 12:20 decision. Paragraph 88 to which I have made reference, that's on page 19. I'd also refer you to the footnote to paragraph -- at the bottom footnote on that page, I can't -- sorry, it's actually to paragraph 89. But if you look at the bottom footnote, it says: 12:21

"*The Court of Justice has clarified that national security constitutes a legitimate policy objective. See Schrems, paragraph 88. See also Digital Rights... in which the Court of Justice considered that the fight against serious crime, in particular organised crime and terrorism, may depend to a large extent on the use of modern investigation techniques. Moreover, unlike for criminal investigations that typically concern the*

retrospective determination of responsibility and guilt for past conduct, intelligence activities often focus on preventing threats to national security before harm has occurred. Therefore, such investigations may often have to cover a broader range of possible actors... and a wider geographic area."

And of course, that also has implications with regard to this question of notification. And it refers to ECHR cases in that context. 12:22

There is a footnote, another footnote that I won't delay if I can't -- I had it marked, but like a lot of these, one then loses where the marking is. Yes, sorry, it is on page 26 and it's the first footnote, 12:22 just something, a detail perhaps but something that I think *wasn't* emphasised, Judge, because you only very briefly saw the rules of procedure. But you'll see that:

"*Rule 13(b) of the FISC Rules of Procedure requires the government to file a written notice with the Court* immediately *upon discovering that any authority or approval granted by the Court has been implemented in a manner that does not comply with the Court's authorisation or approval, or with applicable law. It also requires the government to notify the Court in writing of the facts and circumstances relevant to such non-compliance. Typically, the government will file a*

final Rule 13(a) notice once the relevant facts are known and any unauthorized collection has been destroyed."

So that's the consequence of that. That's a limitation that's regarded as important. And while it's a detail in this context, before I forget it, I just want to refer you to it. 12:23

Then, of course, this decision refers to the Litt letter, which is on page 91. And that refers, on 91, to the PPD-28, and the last full paragraph, that it sets out principles and requirements that apply to all US signals intelligence and for all people, regardless of nationality or location. And it sets certain requirements and procedures to address the collection, retention and dissemination of personal information about non-US persons acquired pursuant to US signals intelligence. 12:23 12:24

Then if you look at the detail - and I'm not going to delay on it - that's set out in pages 92, 93, 94 and 95 with regard to how this operates, it gives quite a different description than one would glean from the **Schrems** decision. Also, 97, pages 97 and 99. And 99 I do want to draw your attention to, it's a statistic that you've seen elsewhere. But at the very top of the page, the paragraph that carries over from the previous page, you will see that there's a reference to 12:24 12:25

information being provided which establishes, the first line says --

MS. JUSTICE COSTELLO: Sorry, I'm just not quite there. 99?

MR. GALLAGHER: 99. And the very top paragraph, which is a continuation from the previous page. And it's the first full sentence on the first line: 12:25

"*The basis for selection of the target must be documented, and the documentation for every selector is subsequently reviewed by the Department of Justice. The US Government has released information showing that in 2014 there were approximately 90,000 individuals targeted under Section 702, a miniscule fraction of the over 3 billion internet users throughout the world.*"

So that's under the Section 702 programme. That's very different from the impression one would glean - and it's a not a criticism of Hogan J -- but that one would glean from the facts that engaged the court in **Schrems**, because clearly it wasn't finding the facts. 12:26

Then in paragraph 45 of **Schrems** there is a reference to **Parliament -v- Council** and paragraph 56 of that case. And it says -- it defines processing of personal data. It's more the fact that the decision is referred to without any suggestion that it's incorrect in any way or overruled in any way. And then the next paragraph, 46, is of some importance. It says: 12:26

"*Recital 60 in the preamble to* [the Directive] *states that transfers of personal data to third countries may be effected*" - and this is the important bit, Judge - "*only in* full *compliance with the provisions adopted by the Member States pursuant to the directive.*"

So the comparator, the compliance is assessed by reference to the provisions adopted by the Member States in compliance, or pursuant to that Directive. 12:27
That's the point I made earlier this morning and explicitly recognised in **Schrems** as the comparator; you effect them only in full compliance with those provisions. And:

"In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II."

That's a reference to **Lindqvist**, which I'm not going to open, you'll be glad to know. It's in book four of five and I'll give you the reference later. But the 12:28
relevant principles are referred to in later cases and it doesn't add anything to our knowledge of the principles that are relevant here.

Then paragraph 51 is important in terms of the Privacy Shield Decision. Apart from Section 11, that I referred to in my brief opening and the significance given to a decision in that context, indeed a significance recognised in terms of decisions being binding by the DPC but not followed through in having regard to the privacy decision - recognised in her draft decision that is, but not followed through - you'll see paragraph 51 says - and this is independent of anything in Section 11: 12:28 12:29

"*The Commission may adopt, on the basis of Article 25(6) of Directive... a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on* all *the Member States to which it is addressed and is therefore binding on all their organs... in so far as it has the effect of authorising transfers of personal data.*"

So it's binding on the DPC, which is an organ in this context, it's binding on the court, and that's quite independently of Section 11. And 52: 12:29

"*Thus, until such time as the Commission decision is declared invalid by the Court, the Member States* and

their organs, *which include their independent supervisory authorities*" - that is the DPC - "*admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection.*"

That's very important. You can raise an issue with *regard* to the decision which **Schrems** says must then be investigated by the DPC, but that's not the position here, that's not part of the claim put before this court by the DPC, by any of the parties. The DPC, as you know, in footnote 22 of her decision says she wasn't taking into account the provisions of the Privacy Shield. And more particularly, in paragraph 6(1) of the reply she says the same, that this is not taken into account. 12:30 12:30

Now, that was something that, in truth --

MS. JUSTICE COSTELLO: Wasn't she relying on its full force meaning and effect? 12:31

MR. GALLAGHER: Exactly. And she does not in any way challenge it, she says.

"*For the avoidance of doubt, the Commissioner could not have had regard to the privacy decision in reaching the draft decision, as same has not yet been implemented at date of adoption and the Commissioner will refer to the entirety of the Privacy Shield for its true meaning and* 12:31

effect."

So there's no challenge to it. And *we* are referring to it for its true meaning and its effect. Its effect is *binding* as a matter of EU law. And that is binding on her. So either she should have waited or she should have revisited this in the context of a binding decision. But what she can't do is put the matter before the court, ask the court to ignore it, refer something on a hypothesis to the EU and have the CJEU saying 'How is this before us? There is a binding decision here that hasn't been challenged in any way and that determines this matter and is binding on the DPC'. As I said on Friday, that's the beginning and the end of it. But I don't want to get distracted by that. I've made that point. But those are very, very important provisions. 12:31 12:31 12:32

I want to continue, if I'm wrong in that for any reason, as to why the approach was substantively wrong. In 55 and 56 you might just note the significant role accorded to the supervisory authority in the Directive, as recognised by the court. That's of relevance in answering your question, which I will deal with later, as to whether, if you had concerns independently of the DPC, somehow that would fill the gap. It doesn't. This is a procedure that is envisaged by the Directive laid down in the statute and it's the DPC that fulfills that role. But I'll come back to it - merely asking 12:32 12:32

you at the moment to look at 55 and 56. And in that context, paragraph 60 will also be relevant.

But continuing with this theme, 63, 64 and 65 are also relevant to that issue. And if I may, Judge, without wearying you having to come back to it again, I'll draw attention to them. I *will* come back to them, but it's a separate issue and perhaps better dealt with separately. 12:33

In the context of the points I'm now making, paragraph 76 is the next important paragraph. And it does reflect -- or, sorry, it does, I suppose, anticipate something, or articulates by way of anticipation something that is reflected in the Privacy Shield but derived from the Directive; that is: 12:33

"... *the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of* [the Directive]*, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified*". 12:34

MS. JUSTICE COSTELLO: I beg your pardon, which paragraph is this now?

MR. GALLAGHER: I'm terribly sorry, it's 76 on page 22.

MS. JUSTICE COSTELLO: 76. I beg your pardon. Yes, I

have it highlighted, yes.

MR. GALLAGHER: And that is the obligation to check. Then if you go to 88, which I suspect you may also have highlighted, because it predicts the ultimate ratio. The court notes that the decision, which is the **Safe Harbour** decision, did not contain *any* finding regarding the *existence* of rules adopted by the state, and this is important: 12:34

"*Intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be* authorised *to engage in when they pursue legitimate objectives.*"

So a recognition, as would have to follow, because EU law couldn't prevent non-EU countries having that as a legitimate objective, it's a legitimate objective of the EU, but the *criticism* of the decision is there's no analysis of the *rules* adopted by the state intended to limit any interference with the fundamental rights. That, as I have said from the beginning this morning, is the approach that you need to take in assessing adequacy and recognised in **Schrems**. And the Commission is implementing **Schrems** and **Digital Rights** in its approach. 12:35 12:35

Then if you go to paragraph 91. The court says:

"*As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access.*"

So a number of points of that is of importance; that looking at the interference with the rights and the limitations on those interference, the one thing that 12:36
is somewhat puzzling is the court's reference to the rights guaranteed by Articles 7 and 8 of the Charter. It's explicable in the sense that data privacy is a right protected by Article 7. The court isn't applying Article 7 and 8, but it's recognising this is a right, 12:37
and it's a fundamental right under the Charter. When one comes to look at the processing that is conducted by way of national surveillance or national security surveillance, one must look not at the rights enshrined

in the Directive, one looks at the extent of the interference and whether the interference goes further than is strictly necessary.

I say it's slightly puzzling because the court doesn't quite explain the precise context in which it's referring to the Charter. The test it adumbrates is no different to the test that was, in any event, applied by the Commission in the privacy decision and it represents the outer limits of what any EU body can do in assessing the adequacy of the protection. 12:37 12:37

So even if you apply -- and as I said to the court, I, of course, accept **Schrems** and **Digital Rights** and those principles for the purposes of the argument before the court. What the court is *explicitly* saying here is, whether viewed by reference to the Charter or whether viewed by reference to anything else, the inquiry inadequacy is a look at the rules and the strictly necessary. And that is clear from this paragraph and paragraph 88 that I've just referred to. 12:38 12:38

Then if you look at paragraph 92:

"*Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data.*" 12:38

So data, personal data is protected within the EU from the scope of EU law by Article 7 and 8, as it recognises, of the Charter, but the protection does require derogations and limitations *even* within the EU legal scheme. And it refers to **Digital Rights** that I drew your attention to 12:39

"*93. Legislation is not limited to what is strictly necessary where it authorises,* on a generalised basis, *storage of* all *the personal data of* all *the persons whose data has been transferred from the European Union to the United States.*"

But of course, that's not *what* takes place. All of that data is *not* stored by the US, that data is stored by the electronic communications providers and targeted access is allowed to that data. So that's a fundamental difference in facts, misunderstanding of the factual situation and deriving from those earlier paragraphs, 31 in particular and 32, that I referred to of the judgment. And -- 12:39 12:40

MS. JUSTICE COSTELLO: I think Mr. Collins, when he was opening this, laid emphasis on the fact that in these paragraphs they keep referring to legislation and they're saying, therefore, you have to look at the laws, it's not sufficient to look at what might be administrative decisions. And I don't know whether -- 12:40

MR. GALLAGHER: Oh, well, he does, of course, say that. And there it does refer to legislation. But all of the

comments that I've shown you demonstrate that you have to look at Article 25(2) says that as well and that the safeguards are absolutely critical. That's also clear from ECHR law, but it's clear from this as well. And I will develop that theme, if I may. 12:40

So obviously you look at legislation. But in assessing legislation and the extent of the intrusion, you look at all of the rules in respect of which it provides the context or practice in which that legislation operates, 12:41 as well as the protections provided in the legislation. And of course, something that *is* provided in the legislation is targeting procedures. The details of that are worked out administratively, but there are obligations in that respect. So there is nothing here 12:41 which suggests that what is said in all of the passages that I referred you to in **Digital Rights** and in this up until now, that you don't look at all the safeguards and limitations.

12:41

Then it goes on:

"... *storage of all the personal data of all the persons whose data has been transferred... without any* differentiation, limitation or exception *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 which both access to that data and its use entail (see, to this effect, concerning [the Directive]*... and... on the retention of data generated or processed in connection with the provision of publicly available electronic communications...).*"

So again, as you now know, that's not true: "*Without any differentiation, limitation or exception 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.*" 12:42

And of course, you'll remember, Judge, that in this case the DPC doesn't *look* at the substantive limitations. 12:42

MS. JUSTICE COSTELLO: Hmm.

MR. GALLAGHER: Doesn't address them at all. Just looks at remedies. But doesn't look even at the legal structure and the extent -- they were looked at in this court. But they are not looked at in the DPC decision. And she *says* 'I am looking at the remedies' and the provisions she *deals with* are the remedies, and she doesn't look at the substantive provisions. So that is obviously a very important -- of great importance. 12:43 12:43

And if you go on then to 94:

"*In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the* essence *of the fundamental right.*"

That's not the position here. That was in **Digital Rights** and the factors that I've drawn your attention to.

12:43

"95... *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.*"

And the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms are 12:44
guaranteed by the law of the European Union or violated to have a right to an effective remedy before a tribunal, in compliance with the conditions laid down in that article. And the very existence of an effective judicial review designed to ensure compliance 12:44
with provisions of the EU law is inherent in the existence of the rule of law.

So the generalised access, which doesn't apply here,

the lack of *any* possibility of an individual pursuing legal remedies doesn't apply here and, in terms of the draft decision, is *acknowledged* not to apply. And that is of importance, because in the context of the Charter and the ECHR, if the *essence* of the right is destroyed and not respected then you don't look at the limitations. But the essence of the right is, *of course*, respected here, but there are limitations, and those limitations are judged by the strictly necessary standard. And that is true whether you adopt the approach that *seems* to be favoured by the court in **Schrems** of looking at it in the context of Articles 7 and 8 and 47, without actually wrestling with the fundamental limitations on the scope of those protections, or whether you look at it in the context of the ECHR. 12:44 12:45 12:45

Then the final ratio on paragraph 98 to which you've already been referred.

So it's in that context and having regard to that approach that the Commission looked at *everything* and all of the safeguards and the limitations that apply that are so much -- so important a part of the fabric of the assessment. And I won't open it now, but you'll remember, Judge, that in the Directive itself, in Article 25(2), that the adequacy must be assessed in the light of *all* of the circumstances surrounding a data transfer operation or set of data transfer 12:45 12:46

operations.

"*Particular consideration shall be given to the nature of data, the purpose and duration of the proposed processing operation or operations, the country of origin, the country of final destination, rules of law both general and material in force in the country in question and the professional rules and security measures which are complied with in that country.*" 12:46

And of course one thing that is ignored completely, in fact isn't mentioned at all but is of importance is the suite of protections that derive from the role played by the electronic communications providers - you have the evidence of the measures taken by Facebook to ensure the law is complied with - their rights to challenge directives and their rights to invoke the Constitution, as was done by Yahoo and others. They're all part of the examination that is mandated by those cases. 12:47

And that brings me to **Watson**, which is, in my book, sorry, it's the next divide, I think, it's divide 37, I believe.

MS. JUSTICE COSTELLO: Yes, **Tele2 Sverige**. 12:47

MR. GALLAGHER: Yes. **Watson** then deals with a sort of a further development of this Retention Directive. I hope you have the divider in yours, but there's the Advocate General's decision and then there's the

decision of the court of 21st December 2016. And there is reference to the Advocate General's opinion in the submissions of Facebook, and indeed I think in other submissions. The court adopts a somewhat different approach and it's obviously to the court's decision, therefore, that I will pay attention. 12:48

MS. JUSTICE COSTELLO: So should I slightly replace what you're going to say now to me in relation to **Watson** with what is in the written submissions?

MR. GALLAGHER: I think it would be better to do that, Judge. It would be better to do that. I can't say I'll double-check that *every* comment is otiose, but certainly it's safer to proceed in that acknowledgment. 12:48

You'll see then this is another variation of this E-Privacy Directive and the permission it allows for Member States to intervene and impose -- or, sorry, restrict the application of the protections. And in order to understand the case, one might go, if I might suggest, to paragraph 11 of the decision, which is on page four. 12:49

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: "*Like Directive 95/46 of the*" -- it's not actually paragraph 11 of the decision, it's paragraph three of the decision, but it's paragraph 11 of the recitals, sorry. 12:49

MS. JUSTICE COSTELLO: Oh, sorry.

MR. GALLAGHER: So it's on page four, excuse me, and it's paragraph 11. I was slightly confused by my own

note. It's quoting from the recitals to the Directive and it says:

"*Like Directive 95/46/... this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law.*"

And that's what I've been saying in the context of 95/46 - it just doesn't affect those issues. 12:50

"*Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and*" - and this is important - "*in accordance with the European Convention... Such measures must be appropriate* [and strictly] *necessary.*"

So by **Watson**, the court is specifically identifying that when it comes to Member States carrying out

surveillance activities, (A) it's not covered by the Directive and the Directive doesn't affect how they do that, but in recognition that all of these Member States are members of the ECHR, they say the Convention governs. And the measures -- 12:51

MS. JUSTICE COSTELLO: I'm possibly getting a little confused at this stage, but why is it the Convention and not the Charter?

MR. GALLAGHER: Well, the court doesn't actually --

MS. JUSTICE COSTELLO: Oh, is that because this is a recital before the -- no, it's not. 12:51

MR. GALLAGHER: Sorry? Yes, it is.

MS. JUSTICE COSTELLO: It's not the date of the Charter, it was before --

MR. GALLAGHER: It is. It's recitals to the Directive. 12:52

MS. JUSTICE COSTELLO: Yes, but is that pre the Charter coming into effect?

MR. GALLAGHER: It is pre the Charter coming into effect. But the Charter was there as soft law and was part of the general principles of European law. And I'm going to -- 12:52

MS. JUSTICE COSTELLO: I was just wondering why it was referring to the Convention rather than the Charter.

MR. GALLAGHER: Yeah. That's why, the recitals are referring to it. And I'm going to show you how that develops. 12:52

MS. JUSTICE COSTELLO: Thank you.

MR. GALLAGHER: But it's just to the point that I made earlier that it's saying this is governed by Member

State law, the Charter doesn't extend *beyond* the scope of European law, Member State law in this area is *outside* European law, but it *is* governed by the Convention. So in respect of that aspect, that's correct before and after the Charter. 12:52

The separate issue is the extent to which the Charter applies in the adequacy assessment carried out after the Charter comes into force. But the Charter does not extend to the area which is declared to be outside the 12:52 scope of EU law, because as I drew your attention to, Article 6(1) of the TEU and Article 51 of the Charter expressly provides it only applies within the scope of EU law.

12:53

So this is absolutely correct, Judge, that it predates the Charter - the Charter was soft law then, general principles applied - but I think it's a slightly separate point and it is relevant to the operation of Member State law, to which I have referred. 12:53

Then you'll see, Judge, Article 15 of the Directive, which is on page seven and to which I've already drawn your attention. And that last sentence in, it's paragraph 11 of the decision, page seven and a little 12:53 over halfway down you'll see Article 15 quoted again.

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: And I've drawn your attention to the last sentence, which isn't part of Article 14.

MS. JUSTICE COSTELLO: 13, is it?
MR. GALLAGHER: It's paragraph 13. Sorry, excuse me. 13, you're absolutely right. And then, Judge, you will see that there's a reference to Swedish law in paragraph 24, because there was a reference from Sweden. And then the reference in paragraph 29 to the UK law, referred to as DRIPA. But we needn't delay on any of that.

If you go to the question referred by the Stockholm court, you'll see that's on paragraph 51, page 16 and referring to the extent of the obligation which was imposed by Swedish law to retain traffic data covering *all* persons, *all* means of electronic communications, *all* traffic data without any distinction, limitations or exceptions, for the purposes of combating crime. 12:54

That's very much in the terms of the 2006 Directive which had been invalidated in **Digital Rights**. What happened in Sweden after the invalidation was the Swedish Government asked an expert to look at their laws and say 'Do we need to change our laws in the light of the **Digital Rights** decision?' And the expert says 'No, you don't. Notwithstanding the decision, they're still fine'. But even from the way the court phrases the question, you see echoes of what had been held *not* to be fine in **Digital Rights**. 12:55

Then in the UK case, you'll see in paragraph 52, it was

a case before the High Court. And in paragraph 53 it's of just some importance to note that:

"*By its judgment*" - and this is important - "*the High Court... held that the Digital Rights judgment laid down 'mandatory requirements of EU law' applicable to the legislation of Member States on the retention of communications data and access to such data. According to the High Court... since the Court, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. It follows from the underlying logic of the Digital Rights judgment that legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, Section 1 of DRIPA is not compatible with Articles 7 and 8 of the Charter.*"

So the judge in the UK *did* compare it with the Charter. 12:57
Notwithstanding the recitals in the Directive about it being outside the scope of EU law, the court proceeds to assess it in that context. But what's important to remember is the High Court had said 'Actually,

following **Digital Rights**, our domestic law is invalid'. So this is, in a sense, just looking at **Digital Rights** again and seeing whether two laws within the legal systems relating to the prevention of crime are consistent with the court's ruling in **Digital Rights**. And the court ultimately holds they're not. But the basis on which it holds it is of some importance. 12:57

Then if you go, Judge, to the scope of the Directive, you might look at paragraph 71. And it refers to Article 15 - it's on page 20 - and it says the Directive states that Member States *may* adopt, subject to the conditions laid down, those legislative measures. So the basis on which *these* laws were invoked was on foot of the Directive, they were given a discretion to adopt them. 12:57 12:58

And in paragraph 73 the court says:

"... *having regard to the general structure of* [the Directive]*, the factors identified in the preceding paragraph of this judgment do not permit the conclusion that the legislative measures referred to in Article 15(1)... are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that*

directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met."

So one of the issues that was raised is: Is this within the scope of the Directive at all? The court answered that fairly simply; it said 'Well, Article 15 allows you to adopt, it gives you a discretion. You have done so. Looked at that article and the structure, we think this is within the scope of EU law'. It would've been surprising, in truth, if it had come to a different decision, because the court had already decided in **Digital Rights** and in the Irish challenge that, firstly, the Community, as it then was, could legislate in that area, as it did in 2006 in the 2006 Directive, and that it had jurisdiction to look at the validity of the Directive. So if it had jurisdiction to look at the validity of the Directive, which purported to *regulate* retention by Member States, it's not *surprising* that it followed the logic of that through in the context of **Watson** and said 'Well, we now actually look at the laws of the Member States which the invalid Directive purported to harmonise, but which itself was inconsistent with the protection that is required to be given to data privacy'.

So this is the follow-through, but it's in the area of combating crime. And as indicated to the court, crime is now the subject of the TEU, it was part of the

Treaty, the European Union Treaty and the subject of framework decisions in the pre-Lisbon. But the position with regard to national security is that it has always been wholly outside the Treaty and remains so. So anything said in **Watson** must be carefully considered in the context in which it's said. And the court is *very* adamant at stressing that context and stressing that these were measures to combat crime. And after lunch I'll take you through as to how they dealt with that, if I may. 13:01

MS. JUSTICE COSTELLO: Okay, thank you. Two o'clock.

(LUNCHEON ADJOURNMENT) 13:01

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

MS. JUSTICE COSTELLO: Good afternoon.

REGISTRAR: In the matter of Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 14:03

MR. GALLAGHER: We were on the **Watson** decision, Judge, if that's convenient, at page 20. And I think I had opened paragraph --

MR. MURRAY: I wonder could Mr. Gallagher refer to the paragraphs because unfortunately we are all on different versions of it. 14:03

MR. GALLAGHER: Oh, I will. I had just finished referring to paragraph 73 and I was going to move to paragraph 74, to give you an opportunity to get it, Judge. 14:03

MS. JUSTICE COSTELLO: I have it, thank you.

MR. GALLAGHER: Thank you. 74:

"*Further, the legislative measures referred to in Article 15(1) of the Directive govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services. Accordingly, Article 15(1), read together with Article 3 of that Directive, must be interpreted as meaning that legislative measures fall within the scope of that Directive.*" 14:03 14:04

Sorry, I may in fact have read that earlier. And

that's because, as I say, the provisions particularly directed to altering the régime, so far as electronic communications providers was concerned, they were the subject of Article 15. Article 15 invoked the Charter and the laws which the Member States introduced through 14:04
the derogation provided in Article 15 dealt with these issues. So that's fixing that the court *has* jurisdiction.

And then if you move to paragraph 80 on the opposite 14:04
page, they say: "*That interpretation is confirmed by Article 15(1b) of the Directive - to which I actually haven't drawn your attention but it is stated here what it is - which provides that providers are to establish internal procedures for responding to requests for* 14:05
access to users' personal data, based on provisions of national law pursuant to Article 15(1)."

Then paragraph 86 at the bottom of the page:
"*Accordingly, as confirmed by recitals 22 and 26 of the* 14:05
Directive, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing of marketing of services and the provision of value added services. As regards, in 14:05
particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that

period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous."

I have drawn attention to that provision because that's the provision which lays down the general rule for the service providers. That general rule may be *restricted* pursuant to legislation introduced by Article 15 and, for the reasons which I have outlined, the court says that actually gives us jurisdiction in this case to look at the legislation because it is specifically dealing with something that is provided for in the Directive, to which the Directive applies, the retention of data, and it is a restriction of a protection in the Directive, namely Article 6, which deals with that issue and the legislation is brought about through a derogation from the Directive. 14:06

So it's quite a different situation from the one we're dealing with here, it certainly raises different issues. That's not to say that it's of no relevance, it clearly is, and I'll just continue with the analysis. 14:07

Paragraph 90: "*It must, in that regard, be observed that the first sentence of Article 15(1) of the*

Directive provides that the objective pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to safeguard national security' - that is, State security - defence, public security et cetera, and the detection and prosecution of criminal offences or of unauthorised use of electronic communications system', or one of the other objectives specified in Article 13(1) of Directive 95/46." 14:07

Then it goes on: *"That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of the Directive which states the legislative measures must be justified on 'the grounds laid down' in the first sentence of that Article."* 14:07

And then 91: *"Further, the third sentence of Article 15(1) of the Directive provides that 'all the measured referred to in the Article shall be in accordance with the general principles of [EU] law, including those referred to in articles 6(1) and (2)' which include the general principles and fundamental rights now guaranteed by the Charter. Article 15(1) of the Directive must, therefore, be interpreted in the light of fundamental rights guaranteed by the Charter."* 14:08 14:08

So that is the ratio with regard to the application and why it applies in that case and one can see the

distinctions with the present case.

Then over the page in paragraph 94: *"In that regard, it must be recalled that under Article 52(1) of the Charter, any limitation on the exercise of rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest required by European law."* 14:08 14:09

And then if you go to paragraph 97: *"As regards whether national legislation, such as that at issue in that case, satisfies those conditions, it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously with no exceptions."* 14:09 14:09

That's a reprise of what was held in the **Digital Rights** to make the EU Directive invalid.

MS. JUSTICE COSTELLO: But the case he is referring to, is that the?

MR. GALLAGHER: It's this case, it's either the Swedish reference or --

MS. JUSTICE COSTELLO: So case C-203/15 is not **Digital Rights**, it's the current one?

MR. GALLAGHER: It's the current one, it's the Swedish case I think. 14:10

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: I'll just go back.

MS. JUSTICE COSTELLO: When you said *"in this case"* I wasn't too sure whether you were referring to **Digital Rights**. 14:10

MR. GALLAGHER: I am terribly sorry. You will see 203/15 is the Swedish case.

MS. JUSTICE COSTELLO: I should have known from 15, sorry. 14:10

MR. GALLAGHER: Yes. And the UK case is the other one. So it refers to it in that way, it's the two cases. Sorry, Judge, that was not clear and I should have made it clear.

14:10

Then if I can move to paragraph 102. So having identified, as I said, the lack of any limitations which mirrored what had already been held to be invalid in **Digital Rights**, the court continues with its analysis in 102: 14:10

"*Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime,*

provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure in relation to the Directive."

14:11

So again identifying what is capable of justifying a measure. In this case it's all about fighting crime and it is serious crime, not just any crime, it has to be serious crime.

14:11

And 103: "*Furthermore, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern of 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."*

14:11

14:11

Again back to what was held to be invalid in **Digital Rights**.

And 105: "*Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective*

14:11

pursued. It is comprehensive in that it affects all persons using electronic communications services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy." 14:12 14:12

Again **Digital Rights**.

106: *"Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical are and/or a group of persons likely to be involved, in any way or another, in a serious crime or (ii) persons who could for other reasons contribute through their data being retained to fighting crime."* 14:12 14:13

Again the **Digital** case. And then:

"107. National legislation such as that at issue in

the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by those provisions."

14:13

Judge, just one point I may have misstated yesterday. I think you asked me is public security the same as national security and I may have said 'yes'. What I should have said is public security and national security are legitimate objectives. I think public security is used in the cases in the context of crime as opposed to national security which is the --

14:13

MS. JUSTICE COSTELLO: It's a term I'm not familiar with.

MR. GALLAGHER: Yes, but they all talk about it, protecting public security, but it's in terms of the order of society.

14:13

MS. JUSTICE COSTELLO: So it's not like crowd control coming out from...

MR. GALLAGHER: Well, it's a bit more than that, I think.

14:13

MS. JUSTICE COSTELLO: I was just wondering what was it.

MR. GALLAGHER: Yes. It extends to terrorist crimes and that, so it's fairly broad. But it's a European term *"public security"*, but that is used in distinction to national security.

14:13

Sorry, in fact maybe I am making a correction that

I don't owe to the court. Ms. Hyland thinks you might have --

MS. JUSTICE COSTELLO: Getting your retaliation in first.

MR. GALLAGHER: Yes. Ms. Hyland thinks that you might have been asking me about state security which is the same as national security, but it does no harm to distinguish between public security and national security in any event. 14:14

And then if I can move to, 107 I have drawn your attention to. 108:

"*However, Article 15(1) of the Directive, read in the light of those Articles of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventative measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided the retention of data is limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted to what is strictly necessary.*" 14:14 14:14

And 109: "*In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that natural legislation must, first, lay down clear and precise rules governing the scope and application of such a data measure and imposing minimum safeguards,* 14:15

so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring such a measure is limited to what is strictly necessary".

And then 110: "*Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe in practice the extent of that measure and, thus, the public affected.*" 14:15 14:15 14:16 14:16

And paragraph 111:

"*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 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. Such limits may be set by using a geographical where the competent national authorities consider, on the basis of objective evidence, that there exists in one or more geographical areas a high risk of preparation for or commission of such offences." 14:16 14:16

And 112: "*Having regard to all of the foregoing, the answer to the first question in the Swedish case is a that Article 15(1) of the Directive, read in the light of the provisions of the Charter, must be interpreted as precluding national legislation which, for the purposes of fighting crime, provides for the general and indiscriminate retention of all traffic and location data."* 14:17 14:17

So again the strictly necessary approach. And it goes on to answer the second question, and if you go to paragraph 118 on page 26: 14:17

"*In order to ensure that access of the competent national authorities to retained data is limited to*

what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of the directive, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data." 14:17 14:18

And 119: *"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 and of being implicated one way or the other in the crime."* 14:18 14:18

And it refers to some ECHR case law. And then it goes on to say:

"*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 in which it* 14:19
can be deduced that the data might, in a specific case, making an effective contribution to combatting such activities."

And again the distinction between serious crime and 14:19
national security and public security. And in paragraph 120:

"*In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the* 14:19
competent national authorities to retained data should, as a general rule, except in cases of validly established urgency be subject to or prior review carried out either by a court or by an independent administrative body, and that the decision of the court 14:19
or body should be made following a reasoned prevention, detection or prosecution of crime."

Sorry. And again that's focussed on the criminal aspect and the previous paragraph acknowledgment of 14:20
differences which all the case acknowledge with national security:

"*121. Likewise, the competent national authorities to*

whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right of a legal remedy provided for in Article 15(2)."

14:20

14:20

And again that is clearly in the context of the fight against serious crime, and you have already heard as to the distinction between notification in that context and in the context of national security and the different rules acknowledged by the Commission in the privacy decision itself and in the cases.

14:20

123: *"In any event, the Member States must ensure a view, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly requested by Article 8(3) of the Charter and constituting in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory*

14:21

14:21

authorities a claim for the protection of their data."

And over the page, finally, at 125: "*Having regard to to all of the foregoing, the answer to the second question in one case and the first question in the other is that Article 15 of the Directive, read in the light of Articles 7, 8 and 11 of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access to the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime."* 14:21 14:22

14:22

And, as you will see, it's in large part a repeat of the rationale or the ratio of the **Digital Rights** case and lack of protections in the context of fighting serious crime and this general obligation that applied without distinction to all data. 14:22

And, Judge, I then want to move, before perhaps coming back and finalising the position on national security, draw your attention to something that is very relevant which you have only been referred to in the most general terms previously and that is the evidence in this case to be found first in Book 4 of the evidence and expert reports, Book 4 of the books before the court. (Short pause) 14:22

And maybe to identify for you where you will find a document to which constant reference has been made, that is the from a Report, is in divide 11 of that and there's a page I'll come back to later, but I have referred you on a number of occasions to page 67 of that report and the judgment of the Federal Administrative Court in Germany dealt with in the left-hand column. So that's just something you might wish to note at this stage. 14:23

14:23

And then the evidence of Mr. DeLong, which is to be found in divide 14. And you will remember, as is evident from page 1 of his background and qualifications, he is a Director of Compliance or, sorry, was a Director of Compliance for the National Security Agency throughout the relevant period, 2009 to 2014, and responsible for the NSA's compliance programmes covering signals intelligence and worked alongside the NSA general counsel and NSA intelligence activities [sic]. Then from 2014 to 2016 he served as a Director of Commercial Solutions Center at the NSA and was a member of the core leadership team, senior official responsible for NSA's interactions with corporations. 14:24 14:24

14:24

He sets out his role in paragraph 4 what it involved in terms of compliance which included, but was not limited to, dealing with FISC, the US Congress, the PCLOB and the Presidential Review Group, which Prof. Swire was a

member, and the NSA Inspector General.

And in 5 he resigned from the NSA in May 2016 and is a fellow at the Berkman Klein centre for Internet & Society at Harvard University for that academic year, 14:25
and he sets out his degrees, both in physics and mathematics and in law in paragraph 6.

And, Judge, I cannot overemphasise the importance of this evidence in the context of the principles that 14:25
have been identified both in the privacy decision and in the cases in assessing what is strictly necessary and in giving focussed attention to how in practice the whole system operates. And of course the practice is, as is clear from **Schrems** and paragraph 75 and clear 14:26
from the privacy decision, vital. I don't want to delay you, but I will refer you to, if I may, the important paragraphs taking account of the fact that it's something the court will read on its own.

14:26

Paragraph 23 on page 7 just describes signals intelligence, which is what all this is about, and he says:

"*It serves a critical role in protecting the US, its* 14:26
allies and partners around the world. In signals intelligence, pertinent information in signals and information systems is extracted, analysed and provided in regulated pathways, to senior officials across the

US and allied governments in order to protect military troops, fight terrorism, combat international crime and narcotics, support diplomatic negotiations, and advance many other important national objectives. Signals intelligence is focussed on refinement at each stage of the process."

This is important: *"Only part of what is targeted is often actually collected; only part of what is collected is ultimately analysed; only part of what is analysed is ultimately shared through those regulated pathways with senior officials, military personnel and other personnel focussed on the safety and security of the US and its allies."* 14:27

Over the page in paragraph 26, he says: 14:27

"It is the nature of the communicative process - what is said and what is not said, what is responded to and what is not, who is added to the discussion and who is not, what is said to one person and not said to another - that provides value and insight that comes uniquely from signals intelligence and also what uniquely impacts liberties such as privacy. This nature is precisely the reason for added protection above and beyond other intelligence areas to be sure that information is specifically evaluated for relevant knowledge at each stage and also minimises extraneous information of anyone - not just United States persons 14:27 14:28

- in relation to the foreign intelligence focus of the activity."

And 28: "*The United States takes an all-of-considerations approach to signals intelligence - evaluating protections for safeguarding liberties, reviewing programs for efficacy and efficiency, allocating resources, discussing economic impacts when applying risk management, and focusing on least intrusiveness. This is, again, necessitated by the goal of achieving all aims laid out in the United States Government's fundamental charter (its Constitution) which contemplates the possibility of assessing one goal (individual privacy) alongside another (collective security and safety). This comprehensive approach provides for the inclusion of all proper considerations to the exclusion of none, at the core of proportionality."*

14:28

Over the page, Judge, at the last paragraph on that page he says that:

14:28

"*Each agency's adherence to its targeting and minimisation procedures is subject to extensive oversight within the executive branch, including internal oversight within individual agencies as well as regular reviews conducted by the Department of Justice and the ODNI. The Section 702 programme is also subject to the FISA court, including during the*

14:29

annual certification process and when compliance incidents are reported to the court. Information about the operation of the programme is reported to congressional committees. Although there have been various compliance incidents over the years, many of these incidents have involved technical issues resulting from the complexity of the program, and the Board has any not seen any evidence of bad faith or misconduct."

14:29

14:29

At 31 --

MS. JUSTICE COSTELLO: When it says *"the board"*, is that a quote?

MR. GALLAGHER: The board is the PCLOB board. Yes, it is a quote.

14:29

MS. JUSTICE COSTELLO: Is that a quote from the PCLOB?

MR. GALLAGHER: It is, Judge. And in fact it begins on paragraph 29 and it is saying what the board found and it is giving you the page of the report.

14:30

Then at 31: *"The term foreign intelligence is defined in various parts of United States law. NSA generally applies the definition in Executive Order 12333, as amended, as 'information relating to the capabilities, intentions or activities of foreign governments or elements thereof, foreign organisations, foreign persons or international terrorists'. In my experience, the inclusion of the phrase 'foreign persons' tends to be misinterpreted to mean 'ordinary*

14:30

persons'. In practice, the inclusion of the term 'foreign persons' serves to catch, for example, sub-government actors - who are involved in specific, predefined issues - such as weapons proliferation or cyber interpretation - that do not at first impression fit into a tight definition of 'foreign governments' or 'foreign organisations'.

32. Even from a purely resource and effectiveness viewpoint, there is little license for and no tolerance of NSA of intrusions into ordinary matters of people that do not involve foreign intelligence. During my time at NSA my various supervisors held me accountable to the production of useful foreign intelligence performance reviews. There was no benefit to focus anywhere else - and in fact there was a well known substantial cost to focussing elsewhere.

33. NSA personnel who deviate from this core purpose are held accountable."

And it gives examples in that respect.

35: "*The PCLOB, an independent oversight body, noted in a detailed review of the 702 programme that 'the limitations do <u>not</u> permit unrestricted collection of information about foreigners'. The regulation, value, purpose, and additional safeguards around the 702 programme have been widely reviewed and discussed."*

And he refers to the report.

And if you would be find enough to move to page 13 and paragraph 40. He says:

14:32

"As the President's Review Group noted: 'Intelligence is designed not only to protect against threats but also to safeguard a wide range of national security and foreign policy interests, including counterintelligence, counteracting the international elements of organized crime, and preventing drug trafficking, human trafficking, and mass atrocities'. And as the President of the United States noted directly in a speech on signals intelligence, 'We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications, whether it's to unravel a terrorist plot, to intercept malware that targets a stock exchange, to make sure air traffic control systems are not compromised or to ensure that hackers do not empty your bank accounts.

14:32

41. In addition to the direct safety and security of both people and systems, the United States intelligence community is asked to provide information and insight across a range of issues. While there is of course a heightened focus on protection from terrorism and other issues like cyber security, there are a number of additional areas where intelligence adds significant

value. For example, the United States National Intelligence Council's list of unclassified reports covers a diverse range of critical issues, many of which - if not addressed smartly in an informed manner - have the capacity to substantially interfere with human liberty and human flourishing across the globe.

42. While the span of these issues is sometimes surprising, as it covers issues not normally discussed such as terrorism or cyber security, such information leads to better, more informed, policy making and mutual security among and within nations, even beyond that of a particular intelligence service. It does not follow, however, that every intelligence need of the United States and its allies can or should be satisfied through signals intelligence. 14:33 14:33

43. In the US, these needs for information are expressed, in practice, in a framework of requirements named the National Intelligence Priorities Framework. 14:33 *And, not surprisingly, the theoretical demand routinely outpaces the realistic supply - both in terms of capability and resources. So, the priorities are further refined and allocated among the different intelligence options. In certain cases, signals intelligence is the last method one would use to gain information, often because it may be too costly, too imperfect, too risky in terms of diplomatic blowback or creates a substantial risk to life."*

MS. JUSTICE COSTELLO: Diplomatic blowback, what does that translation mean?

MR. GALLAGHER: Obviously an Americanism. I think diplomatic ruckus, I suppose, if you put it in our terms or kerfuffle. 14:34

MS. JUSTICE COSTELLO: What the British might call an incident.

MR. GALLAGHER: An incident, exactly. Then 45, Judge:

"*With respect to signals intelligence the US has focused the span of entities that can conduct such activities in the first place and further limited the degree to which it can be shared outside of that tight set of organizations. This makes it easier, from a view across the Atlantic, to understand and to know who can make such assertions. In addition to limiting the span of entities that can conduct signals intelligence activities, US law and policy further restricts the use of the digital information obtained through such activities.* 14:34

46. Signals intelligence information must be handled in accordance with procedures that are approved by the Attorney General of the United States. Not even the Director of the NSA has the discretion to set the hard limits and specific procedures that regulate the NSA. Such procedures - including specific limits and requirements for targeting, collection, retention, data protection, and use of signals intelligence information

- are approved by the highest-ranking attorney in the US Government, and are additionally reviewed and approved by FISC when required by FISA.

47. Signals intelligence is not just valuable in theory; it has demonstrated its value consistently over time. For example, PCLOB noted that 'over a quarter of the NSA's reports concerning international terrorism [many of which are shared among international partners] include information based in whole or in part on Section 702'." 14:35 14:36

And at 48 he refers to an example identified by the board following a full review of the 702 programme as to how a terrorist atrocity was avoided. I don't intend to read it out. 14:36

"*49. In my experience and knowledge, this is just one of many similar outcomes not just from 702 collection, but also from the range of signals intelligence activities conducted by the NSA. In that same vein, although drawn from a UK report, the public case studies referenced in the David Anderson QC report regarding UK signals intelligence activities - those include protecting Northern Ireland, catching a prosecuting attackers, and thwarting mass casualty attacks against aviation - are essentially equivalent (in type of outcome if not in exact type of collection or substance) to those worked every day by US signals* 14:36 14:36

intelligence personnel."

David Anderson was, I think prior to the new Act that was passed in November, he was the person who reviewed the activities of the intelligence activities GCHQ in the UK. He is a QC and he was the independent overseer, and he has produced a very detailed report as to how it operates and the justification for this intelligence, including bulk collection, and Ms. Hyland will refer you briefly to his findings. 14:37

"*50. And in many situations, demonstrated outcomes of signals intelligence provide safety and security far outside the borders of the United States. When reviewing examples involving 702 collection, the Privacy and Civil Liberties Oversight Board noted that approximately fifteen of the cases we reviewed involved some connection to the United States, such as the site of a planned attack or the location of operatives, while approximately forty cases exclusively involved operatives and plots in foreign countries. In short, the vast majority - almost three quarters - of the counter-terrorism outcomes from US signals intelligence activities, in particular the 702 program, directly benefited the United States' allies, including a substantial number in the European --"* 14:38

MS. JUSTICE COSTELLO: I think that's US allies.

MR. GALLAGHER: *"Allies, excuse me, including a substantial number in the European Union."*

Then in 51: "*Before diving too deeply into the specifics of intelligence activities, it is worth highlighting again the substantial partnership between US and European Union intelligence functions for mutual purposes (which are at times greater in sum than the individual nation-state focused purposes). While at times in public there appears to be confrontation, there is far more collaboration than not. And while not discussed often in order to not belabor an obvious point, there is a material difference in the size of US and European Union state intelligence activities. If the US was not in a position to help the European Union and its individual states with a range of their national security and mutual security priorities, such as the provision of lead information in counter-terrorism, it would be challenging for the European Union and its member states to provide an adequate level of security and safety. There is no question that European Union members and the safety of their citizens benefit from intelligence.*" 14:39

And at 52: "*NSA has over 30 direct partnerships with other signals intelligence services around the globe and the partnership partnerships are mutual.*"

14:39

And he describes that. At 54:

"*The partnerships are far more regulated than might be imagined*" and he explains that.

Then over the page at 58 he deals with the scope and scale of signals intelligence. And he says:

"*58. For example, in 2014 - and you have these figures - and that is an effective rate of 0.000031 of the internet users, the 3 billion internet users. Using the same visual analogy - I'm not sure it will help everybody in court - (albeit applied in just the 702 program context), this impact would fit within one of the small one-meter quarter circles at the corners of the football pitch.*" 14:39 14:40

And that's an American football pitch. And: "*Even if one views impacts as not just including that of the properly targeted individual but also others that communicate with that targeted individual, perhaps adding a factor of ten the impact is still limited. That tenfold increased impact would still fit within the space taken by all four small quarter circles at the corners on the football pitch.*" 14:40 14:40

Over the page at 62 he explains the targeting and bulk collection in practice:

"*62. Up to this point this report has not distinguished between target collection and bulk collection because the safeguards discussed thus far apply generally to signals intelligence activities, regardless of the label one chooses to assign. No* 14:40

matter where one draws the lines around those labels, there is no authority in the NSA of a generalised basis for access to and use of information. In that vein, I agree with David Anderson, as stated in his review of certain UK intelligence activity, that any 'legal system worth its name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data is not given on an indiscriminate or unjustified basis'.

14:41

63. In addition, given the totality of the limitations and overlapping safeguards in place, and the limited scope and scale of NSA collection, the 'bulk collection' of signals intelligence is not 'indiscriminate' and not appropriately labeled as 'mass surveillance'. Executive Order 12,333 and Presidential Policy Directive 28 specifically require that signals intelligence activities use the least intrusive methods."

14:41

And he refers to the particular provision which you have already seen.

"*64. This focus on using the least intrusive means is not just a theoretical matter. It is implemented in practice. In 2011, the NSA ceased on its own initiative a major bulk collection program related to electronic communications metadata. (To avoid confusion, this bulk program had been previously shut*

down for non-compliance reasons but was then restarted on a firmer footing.) I was one of the officials directly involved in that decision-making process and believe it is a sound example of the practical application of the overlapping requirements of Executive Order 12,333, FISA, and recently reiterated in PPD-28. Signals intelligence activities are carried out in the least intrusive way possible, taking into account a range of a factors involved in proportionality, which sometimes simply means not continuing a program anymore. NSA made and defended this decision to cease the program to its various overseers in 2011, when there was no public or international pressure to do so; it was simply the right decision to make based on an informed analysis of a variety of factors." 14:42

He continues in 65 that I'll skip.

MS. JUSTICE COSTELLO: Is that the programme that was referred to as the 215 programme? 14:43

MR. GALLAGHER: No. That was abandoned in, with the...

MS. JUSTICE COSTELLO: That was struck down, wasn't it?

MR. GALLAGHER: Yes. That exceeded the provisions of the PATRIOT Act and was discontinued by the USA FREEDOM Act. You will remember in 2011 there was a problem at 14:43 that stage with the MCTs and Judge Bates' decision and he held that he hadn't got all of the information and stopped that programme.

So I think it was an aspect of that, it wasn't the MCTs which continued, but it is separate from the 215 programme, it was a separate programme, and that was stopped.

MS. JUSTICE COSTELLO: So, I just want to get it straight in my head, so then there are four programmes we know about: There is Upstream, PRISM, 215 and then this other one, it stopped? 14:43

MR. GALLAGHER: Which was discontinued in 2011.

MS. JUSTICE COSTELLO: Yes. Thank you. 14:43

MR. GALLAGHER: "*NSA constantly adjusts its activities in light of new architectural changes.*"

Sorry I was just directing you to that.

MS. JUSTICE COSTELLO: Yes. 14:43

MR. GALLAGHER: "*69. While there is naturally a lot of focus on Section 702, an equally important set of safeguards (and not as often referenced in discussions about governmental access to information) apply to certain companies in the US.*" 14:44

Refers to 18 USC 2702: "*Which specifically regulates the type of company involved here - an electronic communication service provider - provides for numerous limitations on interaction with the government. It is quite notable that in a section of United States law titled 'Voluntary disclosure of customer communications or records' the first section of legal text starts with a prohibition on sharing content with any entity*

subject to specific exceptions."

Refers to 2703 and the other provisions which you are familiar. That I should have said is in a context of corporate and governmental interaction and restrictions on the companies itself. 14:44

MS. JUSTICE COSTELLO: Mm hmm.

MR. GALLAGHER: And he says that's an important part of the system as is recognised in the Privacy Shield. And at 76, he says: 14:44

"*Furthermore, US companies play an important role in ensuring that compelled production of customer data or information is conducted according to lawful process. This role of the private sector can be net privacy protecting, as it inserts additional checks and balances that might not be available if a government were to directly collect against a targeted individual. In my experience, many companies act in the best interests of all of their customers, not just those with a particular region or those with a particular nationality. Beyond safeguards and incentives found in rules and oversight, companies have taken a number of steps to increase technical security through architectures, cyber security best practices, and other added security efforts.* 14:45 14:45

Internal NSA Privacy, Civil Liberties and compliance.

79. Persons, regardless of nationality or location, are protected by NSA's core focus on 'foreign intelligence'. In addition, NSA follows specific safeguards in Attorney General approved minimization procedures and PPD-28. NSA now has a dedicated Civil Liberties and Privacy Office which focuses on the protection of fundamental liberties and transparency. This office, in addition to providing sound privacy and data protection inputs internal to NSA, has published three detailed, public reports over the last two years, 14:46 *which have been widely recognised and used in numerous forums"* and he identifies those.

"*80. Internally, the NSA has a substantial compliance program focused on keeping NSA signals intelligence activities verifiably consistent with the laws and policies designed to protect privacy, including PPD-28. This compliance program's workforce numbers over three hundred people. NSA has a Director of Compliance which was established in 2009 and, as required by statute, is appointed by the NSA Director. As such, the position is itself a safeguard established in law."*

At paragraph 85 on page 26 he identifies: "*Specific instances of compliance adjudication have been* 14:47 *misunderstood in the public discussion. For example, a so-called 'compliance audit' reported on in late 2013 revealed 2776 'incidents' had been dutifully recorded, addressed and reported. A full three quarters of those*

instances, however, were examples of NSA acting in compliance with the law, not the alleged non-compliance. Those recorded reflected NSA's meticulous attention to (and recordkeeping about) turning off collection under the 702 Program when a specifically and properly targeted individual travelled into the United States. Those instances were not examples of incorrect collection. Instead, they were instances of the compliance system working - a target that was lawfully collected under 702 appeared to enter the US, and therefore the collection was terminated because new legal requirements were triggered."

There is a provision in the Act you were referred to but you couldn't, I think, possibly remember it there were so many provisions. You can use 702 in respect of a foreign person, but when a foreign person enters the US you turn off the 702. This is what he is referring to here. These are incidents where it is turned off but it was turned off in compliance with the law and for legal reasons. 14:47 14:48

On page 27 he deals with minimisation procedures and the scope of protection, retention limitations and data protection. And he says that: 14:48

"87. While a comprehensive accounting of how all of the safeguards in law and policy are applied in practice and further reinforced by the internal

compliance programme is beyond the scope and length of the report, there are two particular safeguards."

To which he draws attention.

14:48

88: "*First, the actual protections, in practice, for all persons of greater than one might extract from the individual rules that in many cases focus on US persons and people within the US. While certain minimisation procedures have been written with US persons in mind,* 14:48 *and now with all persons in mind due to PPD-28, once written the oversight and compliance processes focus on the totality of the procedures and, for example, in practice non-US persons also benefit from access and retention restrictions."* 14:49

That's a reference to the PCLOB report, a point you have already heard.

"*The focussing effect of 'foreign intelligence' on the* 14:49 *relevant material provides substantial protections for all persons who do not fall in the narrow intersection of the overlapping safeguards. Furthermore, non-compliance is addressed, corrected and reported across the board for all persons, and no external* 14:49 *request - either from an oversight body or even the affected individual - is required or needed to correct non-compliant activity. While PPD-28 is extremely notable for its elevation of many de facto protections*

into de jure protections, protections for all people have been put in place more than has been widely understood or accepted or even adequately described to the public. Even with that reality, it is very meaningful that the new top-level policy directive (which has the effective force of, if not ultimately the full stature of, a Congressional law) specifically covers signals intelligence. This means there are no general or specific 'signals intelligence' exemptions available, as could be imagine in a régime with a general directive for privacy and data protection that does not specifically mention - and specifically regulate - signals intelligence and activities directly.

14:49

14:50

89. Second, access restrictions and retention limitations are at the core of signals intelligence activities. Each and every piece of information in a database comes with a default legally applicable retention requirement. Access to specific databases is limited to personnel who have both the required training (and testing), the required knowledge and experience, and the need to actually access such information to conduct their specific foreign intelligence responsibilities. In many cases the data retention limit is up to five years and in other cases, for example, based on the sensitivity of that information, it is two years or even one year. While those are the standard outer-limits of default

retention periods, it would be incorrect to assume that all data is kept up to those limits, as based on priorities and resource allocations the practical limits are often tighter than even those provided by law. 14:51

90. At first impression, five years can seem a longer time than might be expected to retain signals intelligence information, but the purpose of intelligence is to uncover and produce useful knowledge about plots, about plans, and about networks that may evolve over many years. What might seem unimportant today (or to one analyst) may very well be critically important in two years (or to a different analyst even today). The modern communication environment does not alphabetize or put perfectly in time-order the communications that move around it, and as stated before the NSA's reach into that space is objectively very small. As such, analysts must conduct their efforts - piecing together a specific terrorist network, or finding the pathways used by human traffickers, or predicting the evasive actions of an un-principled state seeking to sabotage a coalition of principled nations with a set of incomplete and unordered set of information. 14:52

91. It's a bit like having a small subset of puzzle pieces from hundreds of different puzzles, without always knowing upfront which pieces go with which

puzzle in the first place. And this reality is the same for targeted and bulk collection. As such, substantial access and use restrictions on the retained information provide the safeguards necessary to properly balance the intrusion into liberties of some, for the provision of safety and security for all. 14:52

92. The NSA Office of General Counsel is also involved in conducting oversight and reviewing compliance with laws and policy, as are operational level management. Compliance is, in essence, built into the process of targeting, collecting, analyzing and disseminating foreign intelligence information. 14:52

93. In addition to these components within NSA, I specifically wish to highlight the role of the NSA Inspector General. The Inspector General has substantial authority, resources and investigative abilities. In my experience, the Inspector General provides a strong and effective blend of both internal and external oversight in a single entity. The Inspector General has an independent budget, broad power to order and compel the production of documents, and reports to the head of NSA and to Congress." 14:52

14:53

And 94: "*In that sense the NSA Inspector General is very responsive to the concern expressed by the Article 29 Working Party that 'some knowledge and understanding of the workings of the intelligence*

community seems to be required in order to effectively fulfil the Ombudsperson's role, while at the same time indeed sufficient distance from the intelligence community is required to be able to act independent'. The Inspector General is one of a network of Executive Branch Inspector Generals that provide a pre-existing and interacting set of oversight bodies. The NSA Inspector General is able to receive, and as appropriate act on, complaints and allegations from any person." 14:53

And of course the comments of the working party, the DPC is a member of the Article 29 Working Party comprised of the DPCs and they did comment on the draft, as you know, of the Privacy Shield and knew, as I say, what was coming. 14:53

96: *"Aside from DOJ and ODNI there are outside oversight bodies."* 14:54

You have been referred to those. 97:

"*Outside the Executive Branch",* it refers to the FISC. And moving then to 32, page 32, paragraph 101, dealing with individual remedies and mechanisms in practice: 14:54

"*The United States has provided various redress opportunities and remedies, in particular in the context of an actual or suspected incident of*

non-compliance. These remedies and redress mechanisms seek to integrate a number of procedural and substantive concerns that stem from the practical considerations mentioned in this report, and they reflect realities and lessons learned that have been developed and adjusted over time.

102. While it sounds tautological, what was communicated is simply what was communicated, so the concept of 'correcting' information in a signals 14:54
intelligence repository is not as applicable as it might be in a regulatory framework or voluntary framework where an individual has submitted information and, perhaps, there is an updated set of information from that information in the course of a government directly providing some service to the individual, on an individualized level. At times, the most important signals intelligence information is that which exposes differences of action and word, or involves the evolution of and changes in plans over time, or involves different aspects of a person than might be otherwise presented to the public or to other people. In fact, the core purpose of intelligence runs counter to the idea that information should be 'corrected' or
'erased' - outside the context of clear non-compliance 14:55
or technical error -as the integrity of collected information is apparent."

That's an important point obviously which

differentiates it from other public authorities that might hold information about you that's incorrect or that's not up to date. What you are collecting is the communications that the person made and the differences of later communications etc. can in and of itself be of huge importance has been identified here. 14:56

103: "*Furthermore, the question of whether an agency like the NSA generally 'has information on' a specific person is not dispositive or directly answerable in full, even on top of valid classification and other prudential reasons not to answer such questions.*" 14:56

This is dealing also with an aspect of notification which hasn't received highlighting and it's a particularly important paragraph. He says: 14:56

"*Sometimes information about a person is collected because it was contained in a communication that was collected for a different valid reason. In some cases, a third country may be the potential target of hostile actions by the targeted parties in communication and in that case the intelligence may be shared and used, if permitted by law, to protect that third person from harm. In some cases that third person bears no importance to a foreign intelligence purpose in which case that third individual is not focussed on due to rules-based safeguards, resource limitations, and the focus of those conducting the intelligence activities* 14:56

on the highest foreign intelligence priorities.

104. Taking all of the above into account, a comprehensive analysis of whether NSA, for example, has information on an individual would require that individual to provide NSA with all other e-mail addresses, telephone numbers et cetera in order to even attempt to comprehensively look into NSA's databases. Such as an inquiry would itself generate substantial additional records across the US government. 14:57

105. Such specifics allow the inquiry to be scoped appropriately to provide a focussed analysis and then redress, as necessary. Generalised and non-particularised claims of impact are not able to be redressed in a way a regulatory agency might be able to move quickly look into a fully organised database, perhaps by name or known identifier, and provide a response. The modem communications environment does not alphabetize or organize the information it transmits into neat personal files prepared for every external redress or remedy without a particularized instance and scope. 14:57

106. And, incidents of non-compliance are proactively addressed and corrected internally, subject to external oversight, often in advance of any external request. Again, this is not to say that such internal proactive correction is a full substitute for external oversight, 14:58

only that the existing intelligence oversight and compliance mechanisms provide substantial remedies, such as the proactive deletion of non-compliant data above and beyond what is found with only independent external oversight. In particular, non-compliant collection of (or even querying of) information on a person is remedied even in advance of any external inquiry, whether from a government or private individual.

14:58

14:58

107. During my prior time at the NSA, I was generally aware of the developing Ombudsperson role, but I was not involved in any specifics of the role or its functioning. Therefore, my comments in the paragraphs that follow are based on my understanding of the role from public documents, informed by prior experiences in interacting with oversight entities. For example, when the Privacy and Civil Liberties Oversight Board rapidly accelerated its look into certain collection programs in 2013, NSA was prepared as it had already been providing detailed information for the range of other oversight bodies it interacts with (and of course generated additional information to respond to the specific questions from that particular oversight board). NSA has a long history of detailed interaction with overseers generally, and certainly specifically with respect to questions and inquiries ranging from the specific to the general.

108. And although the Ombudsperson role was developed in the context of the Privacy Shield specifically, I understand the role extends to the facts of this context, specifically transfers using SCCs. In my opinion, the Ombudsperson role will benefit from 15:00
leveraging many of the existing external and internal oversight and compliance entities - which he mentions - and compliance - sorry, to give a meaningful answer to a proper inquiry, showing that in most every respect the available pathways are substantial and the 15:00
Ombudsperson role, while adding an additional pathway, will likely in practice heavily rely, to positive effect, on the existing set of investigative and oversight bodies who bridge the internal and external oversight pathways." 15:00

And perhaps I'll allow the stenographers change.

Judge, if I can ask you to turn to paragraph 36 and -- page 36 and paragraph 115. He's talking about the 15:01
Snowden disclosures, which, he begins his analysis, I should've drawn your attention to the previous page, sorry, 111. But perhaps going to 115:

"*In my opinion, the asymmetry in information publication led to the incorrect assumption that the accuracy of many of the initial stories was not in dispute. For example, in some situations in which I was involved, a partially incorrect allegation was*

presented and the government simply responded that 'it followed the law'. In some of those situations the governmental response was misinterpreted to mean that the partially incorrect allegation was both fully correct and would in fact be lawful as presented. This misinterpretation was unfortunately the exact opposite of what was intended by the governmental response, while certainly a foreseeable misinterpretation in hindsight.

116. Internal documents of the NSA tacitly assume, at times, substantial knowledge and experience. While the United States has only officially acknowledged a subset of the leaked documents, as a general matter they were written for internal consumption and contain numerous shorthand terms. Such documents assume a substantial amount of training, knowledge, experience gained over many years. They use shorthand and jargon as activities for what would be more proper explanations" --

15:02

MS. JUSTICE COSTELLO: I think that's "*substitutes*".

MR. GALLAGHER: "*Substitutes*", sorry, "*for what would be more proper explanations of dense concepts. At times they may reflect an accurate view of only a small subset of the NSA, often in a specific context, that does not apply generally to the NSA. As such, they are in many ways less relevant source material - especially when publishing on an aggressive timeline while exploring a bulk collection of documents - for a full*

understanding of the value and safeguards in signals intelligence activities. In short, in such documents it is easier to see (or imagine) the risks than learn the safeguards or the value."

And he then deals with that over the next number of pages, I don't want to take the court's time with it, I draw attention to it. And his conclusions, on page 39, I would draw specific attention to paragraphs 125 to 128. 15:03

I just want, Judge, to go back to just one matter, if I can locate it quickly. And if I can't, I'll leave it and give you the reference later. I think it's perhaps better if I leave it and give you the reference later. 15:03

If I could refer you very briefly to the PCLOB report in this context and just a few references that you mightn't have. And I think that's to be found in five, I think 14. 15:03

MS. JUSTICE COSTELLO: That's in the US book?

MR. GALLAGHER: It's the US materials, yes. Sorry, it's 14/4 in mine, but it's divide 56 of the US materials.

MS. JUSTICE COSTELLO: Thank you. I do have it, yes. 15:04

MR. GALLAGHER: You've been through much of this, Judge, and I don't want to delay at the moment, I'll just give you some references that are of particular importance. Pages seven and eight describe the PRISM

and the two programmes operated under Section 702 by way of summary. Paragraph -- or page ten, the second last paragraph deals with the "about" communications and a point that *was* referred to but not in any detail, but it's important: 15:04

"*With regard*", it says in the second last paragraph, " To the NSA's acquisition of 'about' communications, the Board con" --

MS. JUSTICE COSTELLO: Sorry, page ten did you say? 15:04

MR. GALLAGHER: Page ten, sorry. The second last paragraph.

MS. JUSTICE COSTELLO: The second last paragraph, yes.

MR. GALLAGHER: "*With regard to the NSA's acquisition of 'about' communications, the Board concludes that the practice is largely an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets. Because of the manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate 'about' communications from its collection without also eliminating a significant portion of the 'to/from' communications that it seeks. The Board includes a recommendation to better assess 'about' collection and a recommendation to ensure that upstream collection as a whole does not unnecessarily collect* ['about'] *communications.*"

And over the page at 11, the first full paragraph, the reference to the worth of what is being done.

MS. JUSTICE COSTELLO: In which particular -- the first paragraph there?

MR. GALLAGHER: Sorry, Judge, I was just asking Mr. Kieran to look at something. It's the next page and it's the first full paragraph: 15:05

"*Overall, the Board*" - page 11 - "*finds that the protections contained... are reasonably designed and implemented to ward against the exploitation of information acquired under the program for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits. But the applicable rules potentially allow a great deal of private information about US persons to be acquired by the government. The Board therefore offers a series of policy recommendations.*"

Upstream collection is -- the PRISM collection is looked at in detail in page 33 and following. In page 35 you'll see Upstream collection referred to and how it operates. And it's worth just looking at that. It says: 15:06

"*The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because*

the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit. The collection therefore does not occur at the local telephone company or e-mail provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs 'upstream' in the flow of communications between communication service providers.

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA's minimisation procedures. CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems."

There *has* been some change to that, as you saw in the agreed report, but they have to follow and sign up to all of the systems and procedures and precautions of the NSA. And I'll give you that reference later. 15:07

"*The upstream acquisition of telephone and Internet communications differ from each other, and these*

differences affect privacy and civil liberty interests in varied ways. Each type of Section 702 upstream collection is discussed below."

15:08

And if you go to the next page, "*Upstream Collection of Telephone Communications*":

"*Like PRISM collection, the upstream collection of telephone communications begins with the NSA's tasking of a selector. The same targeting procedures that govern the tasking of an e-mail address in PRISM collection also apply to the tasking of a telephone number in upstream collection. Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-US person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorised under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition. The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are*

merely 'about' the tasked telephone number."

And then "*Upstream Collection of Internet*":

"*The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-US persons by tasking specific selectors to upstream Internet transaction collection. And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an e-mail address), and may not be key words or the names of targeted individuals.*

Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet Communications, what is referred to as the 'Internet backbone'. The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702 tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture

only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases."

And that's important, Judge. As you know, it was an issue touched in evidence as to how it's collected. So there are two screening filters and it's only the information that passes the two screening filters that is subsequently ingested into the government database. And you did raise the issue that a wider body of data is obviously screened for this purpose and of course, whenever you use selectors, that follows as a matter of course - the whole purpose is that you use it. But you don't get access to that wider body of data; what's ingested onto the databases is the product of using the target selectors. But if you are to avoid bulk collection, you must use targets. And if you use targets, they have to be applied to a larger body of data, that's how it operates. 15:10 15:11 15:11

Then it goes on:

"*Upstream collection acquires Internet transactions that are 'to', 'from', or 'about' a tasked selector. With respect to 'to' and 'from' communications, the sender or a recipient is a user of a Section 702 tasked selector. This is not, however, necessarily true for an 'about' communication.*"

And he describes how the "about" communication works. And I think you've heard that, but that is the description. And over the page, Judge, at 38, halfway down, last paragraph:

"*In order to acquire 'about' communications while complying with Section 702's prohibition on intentionally acquiring known domestic communications, the NSA is required to take additional technical steps that are not required for other Section 702 collection. NSA is required to use other technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.*"

And he gives an example of that. Then over the page he deals with the MCTs and explains how they function at 39 and on over to page 40. And I don't intend reading all of that out, much of it you've got, but that is the important reference to it. But I would just like to 15:13
draw your attention to some of the numbers. Under the heading "3. Upstream collection", the second paragraph: "*The NSA-designed upstream Internet collection.*" And it draws the distinction in the second last sentence between communications which are referred to as single 15:13
communication transactions and then the multiple communication transactions. And in the last paragraph on the page it says:

"*If the acquired MCT is a transaction between the Section 702 target (who is assessed to be a non-US person located outside the United States and is targeted to acquire foreign intelligence information falling under one of the approved certifications) and a server, then all of the discrete communications acquired within the MCT are also communications to or from the target. Based on a statistical sample conducted by the NSA, the FISC estimated that as of 2011 the NSA acquired between 300,000 and 400,000 such MCTs every year (i.e. MCTs where the 'active user', was the target him or herself).*"

Then it goes on:

"*When the acquired MCT is not a transaction between the target and the server, but instead a transaction between another individual and a server that happens to include a... tasked selector... and may have no relationship, or no more than an incidental relationship to the [tasked] selector. These non-target MCTs break down into three categories. Based on the NSA's statistical study, the FISC estimated that (as of 2011) the NSA acquired at least 1.3 million MCTs each year where the user who caused the transaction to occur was not the target, but was located outside the United States. Using this same statistical analysis, the FISA court estimated that the NSA would annually acquire an additional approximately*

7,000 to 8,000 MCTs of non-targeted users who were located in the United States, and between approximately 97,000 and 140,000 MCTs each year where NSA would not be able to determine whether the user who caused the transaction to occur was located inside or outside the United States.

The NSA's acquisition of MCTs is a function of the collection devices it has designed. Based on government representations, the FISC has stated that the 'NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which are to, from, or about a tasked selector.' While some distinction between SCTs and MCTs can be made with respect to some communications in conducting acquisition, the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a Section 702 selector. This is due to the constant changes in the protocols used by Internet service providers and the services provided. If time were frozen and the NSA built the perfect filter to acquire only single, discrete communications, that filter would be out-of-date as soon as time was restarted and a protocol changed."

And he goes on to explain that. Then the last paragraph in that section:

"*Because of the greater likelihood that upstream collection of Internet transactions, in particular MCTs, will result in the acquisition of wholly domestic communications and extraneous US person information, there are additional rules governing the querying, retention, and use of such upstream data in the NSA minimisation procedures.*"

And there is a figure, I can't just put my finger on where it is stated, but it's already been given in evidence, that Upstream is less than 10% of the -- the *entire* of Upstream is less than 10% of the Section 702 programme. 15:16

Judge, if I can just ask you to briefly refer to 98. And it speaks of existing protections for non-US persons' privacy. And in the last paragraph it mentions a point mentioned by Mr. DeLong, that: 15:17

"*The first important privacy protection provided to non-US persons is the statutory limitation on the scope of Section 702 surveillance, which requires that targeting be conducted only for purposes of collecting foreign intelligence... The definition of foreign intelligence information purposes is limited to*

protecting against."

And he describes it. And he says:

"*Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and approved by the FISC.*" 15:17

Then he goes on in the next paragraph: 15:17

"*The second group of statutory privacy protections for non-US persons are the penalties that apply to government employees who engage in improper information collection practices.*"

Then the next paragraph; the third privacies are the criminal prosecutions under 1806. And just a paragraph, the second paragraph, first full paragraph on page 100: 15:18

"*Finally, as a practical matter, non-US persons also benefit from the access and retention restrictions required by the different agencies' minimisation and/or targeting procedures. While these procedures are legally required only for US persons, the cost and difficulty of identifying and removing US person information from a large body of data means that typically the entire dataset is handled in compliance*

with the higher US person standards."

Page 103 and following contain a policy analysis. And on page 104, under the section of "The Value of the 702 Programme", that has been assessed. And the conclusion is: 15:18

"*The Section 702 program makes a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition. Section 702*" --

MS. JUSTICE COSTELLO: Where are you reading?

MR. GALLAGHER: I'm terribly sorry, 104 and under the heading "Value of the Section 702 Programme". 15:19

MS. JUSTICE COSTELLO: Oh, the first paragraph. Sorry, I beg your pardon.

MR. GALLAGHER: Yeah, the first paragraph, Judge. Then that's all I want to draw your attention to in that. If I can briefly ask you to go to 59. That's where the FISC rules of procedure to which reference has been made are contained. And page four of that, the provision in Rule 11 relating to where novel issues arise and looking for assistance in relation to novel issues. And over the page, Rule 13, the government obligation, if it discovers something, to make a submission to the court, which was specifically referred to in the Privacy Shield. 15:19 15:19

That also contains the Brown report, which I'm not going to open, in divide 66, which Prof. Swire referred to, Judge.

If I can then refer you to a different report, if I can just hopefully lay my hands on it. It's a Council of Europe report and I thought I had it -- 15:20

MS. JUSTICE COSTELLO: Take your time.

MR. GALLAGHER: -- handy. I'll find it in a moment, Judge. 15:20

MS. JUSTICE COSTELLO: No, no, take your time so you have a proper look.

MR. GALLAGHER: Thank you very much. I can move on without delaying it --

MS. JUSTICE COSTELLO: No, no, find it if you want. 15:20

MR. GALLAGHER: -- and I'll come back to it. As luck would have it, I can't just put my finger on it. I'll move on, because I won't be derailed. But I'll bring you to it in a moment.

15:20

If we go back to book four, which I was looking at, there's the evidence of Herr Ratzel, the former Interpol Chief, to be found in divide 17. And I'm not going to delay on that. The submissions of the DPC say 'Well, he just gives some examples'. And of course, 15:21 that is so. It's very clear that these examples give a clear justification for the signals intelligence and explain the importance of it. And the purpose of the examples is just that - to show how it is used in

protecting safety and the importance of this objective, being a core objective obviously of a sovereign state.

So I draw your attention to it. Mr. Collins summarised it. And it *is* worth reading the entire. As I say, we make an apology, with no disrespect to Mr. Ratzel, that the English is just slightly less fluent than we would - and I hope he doesn't read this transcript - than we might do it. He declined any assistance of a translator and clearly *speaks* fluent English, but the English is written perhaps as you might expect it to be written by a non-English speaker. 15:21 15:22

The third piece of evidence in this context that's *very* important is in book five of these books and it is the affidavit of Michael Clarke. And he is the professor who comments from a European perspective on the sort of issues that are addressed by Mr. DeLong. And you'll see in his report, in the first page he sets out his credentials. He is a Professor of Defence Studies. He was a Director General of the Royal United Services Institute - a think tank. And he occupied various other posts. 15:22 15:23

In March 2014, he says at the bottom of the page, he was appointed by the Deputy Prime Minister to chair an independent surveillance review at RUSI, which reported in 2015 and dealt with a democratic licence. The Report of the Independent Surveillance Review was 15:23

published as part of the public discussion around the Interception of Communications Bill, which was due to be enacted in December 2016, *was* enacted in either November or December, and I've referred to it.

15:23

In paragraph -- or page three, he just gives a definitional note and he distinguishes between what he calls in the first paragraph surveillance by the security and intelligence agencies, SIAs or the law enforcement agencies, LEAs. And you'll find those 15:24
acronyms throughout his report.

At page five he deals with the necessity for a level of electronic surveillance. And of course, this is important, because the movement away, obviously, from 15:24
the individualised authorisation that existed in the old FISA - obviously a different situation arose where people made individual phone calls and had individual communications - to a situation of mass communication that we have now, even those changes have been enormous 15:24
since 2006.

I remember myself, when on circuit in 1995, people queued up at the phone box in the courthouse to make calls. That's how we communicated. And of course, 15:25
those could be tracked and intercepted and authorised. But when you've three billion internet users making enormous numbers of communications on a daily basis, billions of communications, you're in an entirely

different environment. And Prof. Clarke explains the challenges that this poses, both in terms of serious and organised crime and national security.

In paragraph six he says: 15:25

"*These changing patterns of terrorism and crime as they affect EU countries - more serious and organised criminality; more well organised and lethal terrorist attacks - are believed to be at least partly facilitated by the revolution in internet-based communication and accessible high level computing capacity. Such developments and the deepening reality of digital societies throughout Europe have created many new potential platforms, opportunities and modes of operation for individuals and groups involved in criminal and terrorist activities. Such developments have similarly affected the potential vulnerability of modern, digital societies to industrial and foreign-based espionage.*"

Then he gives the necessity analysis. And at eight:

"*'Digital society' refers to the phenomenon whereby the power of the internet, allied to powerful computing capacity, penetrates the lives and activities of individuals and organisations throughout society, creating unprecedented levels of dependence on electronic communication and generating equally*

unprecedented levels of data about individuals and organisations. The potential to harvest new data is also immense, since modern data analytics can identify correlations within billions of otherwise unrelated pieces of information."

And he identifies what we would know, the economic and social benefits. And then the proliferation of communications platforms. And in paragraph 11 he says:

"*For most of the Twentieth Century, until the late 1980s, the only way most individuals or organisations could communicate was via postal services, telephone or telex lines, or through meetings. In the digital society, however, there has been an explosion in the applications of internet-based communication. More than two million apps are currently available for almost anyone in the world to download. As of June 2016 Microsoft Android offered 2.2 million different apps available for download; Apple offered just on 2 million. Apple's portfolio of available apps grows by more than 1000 per day. In 2009 around 15,000 apps every month were being offered to Apple; by 2015 it was being offered around 40,000 apps per month. All of these apps and filesharing arrangements are potentially capable of being manipulated for malign purposes. Beside the overwhelmingly legitimate uses of such technologies, therefore, criminals, terrorists and foreign agents have been able to diversify their modes*

of communication to make detection, or evidence gathering, by the SIAs/LEAs significantly more challenging."

He identifies the growth of encryption. And then in 13: 15:28

"*The internet is intrinsically transnational and by the turn of the Twenty-first Century this inherent quality was recognised to have created significant new challenges for all western SIAs/LEAs, not just from international terrorism but also from transnational organised crime. This was recognised by the US National Security Council as a generically novel threat both to the United States itself and more generally to international political order. In more recent years new transnational challenges have also emanated from the evident efforts of autocratic governments that are deemed to pose security challenges to western societies.*"

And he gives examples of implications of terrorism and crime, paragraph 16:

"*In the three months from December 2014 to February 2015 one commercial terrorist monitoring organisation recorded a leap in ISIS-related twitter postings from around 100,000 per day to 1.2 million per day, some of which - estimated to be a low proportion - created by*

botnets, but most reflecting direct personal connectivity."

He describes botnets and the likes later, I don't think we need to delay on it, it's just the scale. In paragraph 20, over the page, he refers to the UK's Home Office assessment of cyber crime as: 15:29

"*A tier 1 threat to the UK's national security. Malware, ransomware attacks and the targeted compromise of UK networked systems, particularly from criminals based overseas, are an increasing threat. Cyber techniques are used by organised criminals to commit fraud against government departments, businesses and the public. Firearms, drugs and other illegal commodities are traded on the internet, including the 'dark web', using virtual currencies. We are seeing an expansion of cyber crime 'as a service', with some instances of organised crime groups hiring cyber experts.*"

If you go to page 11, paragraph 24, he sets out the benefits of electronic surveillance. And in paragraph 25:

"*One benefit is that the inherently international nature of internet communications may allow SIAs/LEAs to gain access, through legal means in their own domestic environments, to material in networks*

operating in foreign jurisdictions. In cases submitted by the UK's GCHQ to the David Anderson review of bulk access, it was repeatedly shown that between 2009 and 2013 access to data and communications inside the UK had linked the authorities to wider terror networks in the Middle East, or to active international paedophiles involved in child... exploitation. In particular, the nature of the internet offers the authorities the capacity to perform at an international level, some key tasks in information handling; not just in intelligence gathering and investigation, but also in the more specialised areas of forensic data preservation and recovery and in the authentication of digital evidence.

A second benefit is that it's cost effective in terms of resources, in 26 he says. And then 27: 15:31

"*A third benefit is that the vulnerabilities of the digital society for the law-abiding public when facing criminal and terrorist activity are also potential vulnerabilities for criminals and terrorists.*"

And at paragraph 28 he identifies a fourth benefit, which is:

"*A fourth benefit is that electronic monitoring is* inherently *able to uncover networks of connected individuals and organisations if SIAs/LEAs choose, and are legitimately able, to pursue extensive linkages.*

This is of particular relevance in combating current trends in international jihadist terrorism as they have developed in the last twenty years. Classic terrorist [activity] *has traditionally operated in cell structures, where networks of groups and individuals were intended to be anonymous or not to exist at all. From the 1970s to the 1990s European SIAs and LEAs could only effectively penetrate the terrorist networks that threatened Europe through big investments in*" - that's human intelligence - "*to reveal their connectedness. Since the advent of the Al Qaeda threat to Europe and the western world in the late 1990s, however, international jihadism has been distinguished by its highly networked and barely concealed structures; and in the case of Islamic State, by its public acknowledgement and celebration of such structures as part of its attempt to build international momentum behind the appeal for a Caliphate. In contrast to most previous terrorist organisations that have been based around tight cadres of specialised individuals, Al Qaeda and IS have attempted to develop from their inner cadres elements of a mass movement, largely mobilising determined amateurs who make little attempt to keep their identities or intentions secret. The friends and family links between would-be terrorists involved in plots as far removed as the 9/11 attacks, terrorism in the UK and guerrilla warfare in Yemen, for example, can be well documented from public sources.*"

He identifies then the response of SIAs and LEAs and, on page 14 at paragraph 35 and following, deals with the rules of interception. And he says that:

"*Given the exponential growth in the volumes of data and communication available on the internet, the reality for SIAs and LEAs is that all surveillance has to be targeted. In the UK, untargeted searches, or simply 'trawling' for information is not lawful and would be a very uneconomic use of resources if it were. Typically, SIAs/LEAs seek access to information that requires different levels of intrusion on the basis of different targeting requirements. They can be defined in the following way:*

36. Communications data."

And he describes what that refers to. And I think you've had much of that already. And over the page he gives figures. And in paragraph 37: 15:34

"*The overall proportions are said to be similar in cases heavily involving the SIAs. In 2013 it was reported by The Guardian that senior intelligence officers had revealed that, 'Every single major international terrorism investigation has involved the interception of communications ... It matters because terrorists have to communicate'. In 2014 the UK Home*

Secretary told Parliament, 'Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade. It has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service'.

38. Though communications data is far and away the form of access most frequently required by the SIAs/LEAs, the necessary authorisation requires a degree of targeting dictated by the cases to which it is being applied. In the UK the rationales for authorisation are audited annually by an independent commissioner and staff. In the case of foreign-based CSPs from whom communications data has to be obtained, requests can be denied or targeting rationales challenged."

He deals with content data, because it's more intrusive obviously. And in 40:

"*Bulk Data and Bulk Interception. Bulk data has emerged as one of the most controversial aspects of the debate around privacy and security. There is a misunderstanding in the term itself. Bulk interception refers to the interception of large volumes of data. Bulk data, in itself, refers to information that exists in bulk form, though it may be intercepted very simply. Bulk data interception and access is also commonly regarded as 'untargeted', but this too is a*

misunderstanding. Bulk data interception and access draws large amounts of material into its searches, the vast majority of which will be of no interest to the authorities. In that respect it is distinguished from 'targeted' access to communications or content data, for example. But the sheer volume of material now generated on the internet means that bulk searches have to be 'targeted' to the extent that they have to be directed to those areas, or limited timeframes, that the search and filter technologies available to the SIAs are capable of handling".

MS. JUSTICE COSTELLO: Can I just understand what he's saying there? He's sort of saying "bulk" is a sort of a larger target, but not indiscriminate?

MR. GALLAGHER: Exactly. The phrase "bulk" has been conflated with "indiscriminate", and it's a distinction that's drawn in PPD-28 as well. "Bulk" is not indiscriminate, you still use discriminants. And you have to do that (A) because you just couldn't handle the volume and it wouldn't be effective; and (B), in any event, under PPD-28 the focus is, as you know, on targeted interception. So he's clearing up some misapprehensions whereby "bulk" is just conflated with "indiscriminate" and that you access everything. That's not so. 15:37

In 42 he says:

"*For western SIAs there are two main operational*

purposes for intercepting data in bulk. The first is to reconstitute split communications, given that the internet breaks messages down into packets to transmit them and then reconstitutes them at the destination. For the SIAs" - the intelligence agencies - "*a targeted message or flow of information may have to be intercepted at multiple points to recover the whole message. It is in this sphere where enhanced encryption makes the task significantly more challenging for the SIAs. The second is for 'target discovery' to identify individuals of particular interest to the security services or; to identify potential but as yet unknown threats to national security. The UK's Parliamentary Intelligence and Security Committee summed it up:*

'GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in those communications are sometimes already known, in which case valuable extra intelligence may be obtained (for example, a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.'

43. In his special report, reviewing the operational

utility of bulk powers, David Anderson accepts most of the arguments of the SIAs in favour of this type of interception. It is particularly effective, he concludes, in combating cyber-crime, even though he acknowledges that its utility in the overall intelligence picture in the future may be diminished by the evolution of internet technologies. For the present, however, he is clear that bulk interception of data and communications has fed directly either into ongoing investigations or else into prioritising areas for future investigations into the most serious threats to national security. It offers the SIAs the possibility of keeping up with the agility of terrorists and criminals to create fast-moving threats to national security, operating across many different areas of the internet. In these functions bulk interception, by several different means that he reviews in his report, is either acting on a targeted basis, or else is helping to establish a targeted basis for further investigations. In David Anderson's view,

'The bulk interception power has proven itself to be of vital utility across the range of GCHQ's operational areas, including counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations.

The power has been of value in target discovery but also in target development, the triaging of leads and

as a basis for disruptive action. It has played an important part, for example, in the prevention of bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks'."

And it goes on in more detail. And then the summary is on page 20. And in paragraph 49:

"*It is my belief that with such a range of activities being conducted 'on line' it would be impossible for the SIAs/LEAs to try to counter their operations 'offline'. It is also my belief that intercepting the communications of criminals, terrorists and espionage groups through electronic means is, in principle, necessary insofar as this is a modern day equivalent of traditional policing techniques such as legitimately tapping a telephone or trailing a suspect to ascertain with whom they communicate. As patterns of electronic communication activities have evolved for all in the digital society, so, it is my belief, it is necessary that security and policing agencies should be able to operate in the same space.*

50. Throughout EU member states data collection, interception and processing by the SIAs/LEAs must be conducted on the basis that such activities are deemed lawful, necessary and proportionate. As the foregoing has shown, however, the implied intrusion of the SIAs/LEAs both into the depth and width of the

electronic fabric of a digital society as they go about their work is necessarily great. It is my belief that of the three pre-conditions, the advent of digital society across the EU makes the judgement of what is proportionate *in any given operation significantly more difficult to determine.*

51. Civil liberties issues are not trivial and I have not tried to encompass them in this report. I have tried to deal with what is technically possible and what I believe to be current practice; not how to weigh a judgement between security and privacy. That must rest on a balance that weighs the intrusions of the SIAs/LEAs into the lives of EU citizens against the 200 plus real or attempted annual terror plots against European targets or the 3,000 active, organised crime groups believed to be operating in and through the continent."

I don't think I drew your attention to page four and paragraph three, which says that: 15:42

"*The most recently available figures from EUROPOL record 211 terrorist attacks either 'completed, failed or foiled' in 2015 against members of the EU. All sources of terrorism as defined by the EU are included in these figures, including jihadism, right and left wing extremism and national separatism. The completed attacks caused*" --

MS. JUSTICE COSTELLO: Sorry, I didn't quite find, where were you?

MR. GALLAGHER: It's paragraph three on page four.

MS. JUSTICE COSTELLO: Thank you. Sorry. "*The completed attacks*", yes. 15:43

MR. GALLAGHER: Yeah.

"*The completed attacks caused 151 fatalities and seriously injured more than 360 people. Some 103 of these 211 cases were recorded in the UK. EUROPOL also records the arrest of 1077 individuals across the EU on terrorism-related charges. Of these, 44% were arrested on suspicion of membership of a terrorist organisation, and 23% on suspicion of attack-related activities (up from 13% in 2014). EUROPOL also pointed to a 'notable increase in arrests of individuals of Russian origin in the EU'. Court proceedings were completed against 514 individuals on terrorist-related charges in 2015.*"

So that is the evidence on the legitimacy of the objective, which is recognised, and the necessity for the type of intrusion that does take place in relation to the data. And I want to try and -- 15:44

MS. JUSTICE COSTELLO: You just might help me a little bit with one -- there seems to be a little bit of tension between some of the evidence there. 15:44

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: Obviously I think, I can recall specifically the PCLOB report; they were talking about

the tiny percentage, I think it was 0.000031 of the internet traffic.

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: And that seemed to be suggesting that really this isn't too bad, to put it at a very crude high level. Then we have here Prof. Clarke saying that he refers to the intrusion of the SIAs and the LEAs both in depth and width of the electronic fabric of a digital society is *necessarily great*. 15:44

MR. GALLAGHER: Yes. 15:45

MS. JUSTICE COSTELLO: So I'm just wondering, I know neither of them are purporting to do the balance between --

MR. GALLAGHER: No.

MS. JUSTICE COSTELLO: That you're talking about. But you're talking about the assessment of -- that has to be conducted -- 15:45

MR. GALLAGHER: Exactly.

MS. JUSTICE COSTELLO: -- as little as necessary.

MR. GALLAGHER: Yeah. I think it's a frank acknowledgment. Mr. DeLong acknowledges the privacy concerns. Obviously many people would regard that as great - they don't want any intrusion. What they're saying, it *is* great in that sense, but it is not mass, it is not undifferentiated, it is not indiscriminate, it is not taking all of the information and ingesting it onto your servers. I think they would be doing a *disservice* to what's involved if they said this isn't significant. It is. And what they try to do is 15:45 15:45

justify the significance of it.

And those are very powerful, uncontradicted witness statements as to (A) how they operate and why they *do* use means for limiting and safeguarding the task in which they're engaged and, in particular, the extent of the interference with data and limiting the amount of data that is ultimately collected by using the filtering processes. Obviously what's relevant of particular concern in this case is the process used in the US. And Mr. DeLong gives detail in relation to that process, whereas Prof. Clarke is dealing with it more on an overview and emphasising its importance. But he does acknowledge that this is significant and nobody is down down-playing that. 15:46

But the one thing that *does* emerge from the uncontradicted evidence is the relevance of the safeguards and the limitations. And the description given by Mr. DeLong, which of course is consistent with that in the PCLOB report, shows that it is very much a targeted and focused interference with data, it's not indiscriminate, it's not mass surveillance in any sense. And the rules and regulations that are now in place are designed to maintain that. 15:47

That, of course, is the approach taken by the Commission, that had access obviously not to Mr. DeLong, but had access to the people in the US and

to the PCLOB report, and they took the view that this was a legitimate objective and that the intrusion went no further than was strictly necessary.

But of course this court isn't being asked to decide that. That would be an assessment of the necessity which would be very difficult for *any* court to do and a very significant margin of discretion is, in any event, given to countries in that area and to tell a country it can't do a particular type of surveillance that it says is necessary for all these important objectives would be a very serious matter. But it points out that this is the task that needs to be *undertaken* before you *conclude* that the law of the other Member State is not *adequate*. Because the adequacy is judged from the perspective of the peculiar aspect and special aspect of national security. It's treated in a different way, it is accepted that it's an interference with the rights, and, therefore, you apply the strictly necessary analysis.

15:47 15:48 15:48 15:48

As I say, that is wholly missing from what was done in this case and you cannot possibly reach a conclusion as to adequacy without conducting that.

15:49

Paragraph 75 of **Schrems** which I did refer to - it's not necessary to open it - talks about examining, and I quote:

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

I did draw your attention to 25(2) when you asked me that this morning. The rules and the practice are vital. Of course, many of the rules identified by Mr. DeLong are legislative. All of these oversight bodies are grounded on statute. And then the more specific detailed rules are what one would expect in any situation - administrative rules that have a legal effect, because they have legal consequences. But they're not statutes obviously, and that's recognised in the ECHR as being rules and regulations that can be taken into account. And for very obvious reasons, while there is provision for targeting and minimisation and for all forms of certification and oversight in directives, the *detail* cannot be disclosed, because that would negate the very purpose of the whole national security regime and there is no requirement to do that. 15:49 15:49 15:50 15:50

So the Commission looked at all of those matters, took all of those matters into account. And we say you

couldn't have *any* doubts about the adequacy of the regime without conducting such an exercise, which was never conducted here.

But it also emphasises another matter that is of significance and I just want to spend a short period of time on it - it's connected with this, and it won't be long - and that is you have to have a holistic approach. Nobody, in *any* of the cases -- the CJEU, in any of these cases, just picked out the remedies and said 'Let's look at what the remedies are here and see whether they're adequate'. They looked at the contours of the national security issues, the access which was had to the data, looked for limitations and safeguards and assessed strict necessity on that basis. That is precisely what the European Commission did. 15:50 15:51 15:51

And of course, it's done not just because national security has to be treated in that way given its particular and peculiar status, but also because national security involves necessarily a limitation of the rights. And when you're looking at the limitation of the rights, you must assess them in terms of what is the extent of those, or what is the extent of those limitations, what protections and safeguards are there to ensure that the limitations go no further than is strictly necessary? They recognise, as does the court in **Schrems**, that the *remedies* can be limited. And the court, remember, in **Schrems** talked about the essence of 15:51 15:52

the right being implicated or being denied where there was no possibility for an individual to pursue legal grounds. In paragraph 96:

"*Likewise, legislation not providing for* any *possibility for an individual to pursue legal remedies in order to have access.*"

So it recognises that there will be limitations on those remedies. And Article 47 itself recognises that. 15:53

So you can't start with the remedies and say there are limitations and say that *because* there are limitations, that means they're not adequate. Because (A) it begs the question as to what you're comparing it to, but 15:53
(B), in national security, by definition there are going to be limitations on the remedies. That matter was not addressed at all by the DPC. And if you go to the Charter, which is in divide one of the first book of EU materials, that is apparent from an examination 15:53
of 52 in particular. Firstly, you will see Article 47 is:

"*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... [before an] *impartial tribunal*", that's a separate matter. But it's the rights and freedoms guaranteed by the laws of the Union. And Article 52 tells us that limitations can exist on those. So:

"*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 recognised by the Union or the need to protect the rights and freedoms of others.*"

So the possibility of limitations on the exercise of all rights, which of course includes 47 and 7 and 8, is provided for in 52; you must respect the essence of the right, you mustn't negate the essence of the right. And subject to that, of course, there is an assessment with regard to necessity and proportionality. 15:55

So that's not much different from the approach of the ECHR. But taken at its height from the DPC's point of view, if you apply the Charter, that's the sort of analysis you need to engage in - that's what was engaged in in **Schrems**, **Digital Rights** and in **Watson** - and you make the assessment on that basis. That is the assessment, as I said, that the Commission has done, but not the DPC. And therefore, any assessment of

adequacy is, for that reason, in and of itself invalid.

I do want to refer you then to -- or before moving to that, just to say this; remedies, as we say in our written submissions, are an accessory right. They are a remedy where there is a breach of the law. If the law -- or where you want to *assert* a breach of the law. Where the law is, or the legal rights are limited, as they are in the area of national security, to assess and evaluate the remedies, you must, of course, evaluate substantive law in the first place and you must look at the limitations on that law and in that overall context make the judgment. 15:56 15:56

If you go, Judge, to the Directive for one moment, this ties in with the question of Article 26, which I will be coming to shortly and the difference between 25 and 26. But the Directive is in divide four of that first book, that same book. And the adequacy of the level of protection -- or, sorry, the principles in Article 25 which underpin this, 25(1): 15:56 15:57

"*The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive*" - again the reference to the national provisions - "*the*

third country in question ensures an adequate level of protection."

Then 25(2), to which you've been referred, tells you about how that adequacy is to be protected. And Article 6 provides for the Commission assessing that adequacy in the context of Article 31(2), it's a very formal procedure. And if you go to Article 31(2) you see the procedure by which it makes its decision. 15:57 15:58

Then if you just go back to Article 29 you see the Working Party. And Mr. Collins opened that to you and what *its* role is. And you'll see in Article 29(2): "*The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established*" by the government institutions and other bodies. 15:58 15:58

So the DPC was part of that. The adequacy must be done in accordance with the case law, it must be done in accordance with a particular procedure and while she is entitled to question that in the context of a decision, it must be in that context and there isn't room for her to conduct the truncated exercise which she conducted which *doesn't* recognise the special position of national security, *even* within the context of the 15:59

Charter.

So I do want briefly tomorrow to just draw your attention to the Council of Europe report which I just couldn't lay my hands on just now to update you. I've taken a little bit longer than I thought going through that evidence. I will try and finish by lunchtime - the other issues are net and a lot of what I have said here, I'll be able to apply them to the other issues and then Ms. Hyland will start. I suspect she won't finish tomorrow, she'll go into the Thursday, so there is a bit of slippage, Judge, for which I apologise. 15:59 15:59

MS. JUSTICE COSTELLO: And then, Mr. McCullough, I think you were about a day, is that right?

MR. McCULLOUGH: Yes, Judge. Hopefully less, Judge, but that's what I should allow. 15:59

MS. JUSTICE COSTELLO: Yes. So, Mr. Murray, so we look like you might be up on the Friday, is that right?

MR. MURRAY: That sounds like it, Judge, yes. Mr. Collins was hoping to be back here on Friday, so we'll divide the reply between the two of us, Judge. But I think it's likely to take -- I have to hear the remainder of what Mr. Gallagher and Ms. Hyland will say, but it will take, I think, between a half a day and a day. 16:00 16:00

MS. JUSTICE COSTELLO: Yes. And again I'm not cutting anybody short, but I have another commitment on Tuesday of next week. So...

MR. GALLAGHER: Okay.

MS. JUSTICE COSTELLO: ... if we need to run over, it would have to be resumed *after* that other commitment.

MR. MURRAY: Very good.

MR. GALLAGHER: Thank you, Judge.

MR. MURRAY: Thank you, Judge. 16:00

THE HEARING WAS THEN ADJOURNED UNTIL WEDNESDAY, 8TH MARCH AT 11:00

B

C

D

E

F

M

N

O

P

Q

R

S

T

U

V

W

Y

Z