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 WEDNESDAY, 8th MARCH 2017 - DAY 17

17

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 WEDNESDAY, 8TH 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: Good morning, Judge. Judge, I'm going to try and go speedily through the various issues that I have left this morning. Before doing so, there are just two or three clarifications from yesterday. You asked me about the reference in the DeLong report to the discontinued programme. 11:04 11:05

MS. JUSTICE COSTELLO: Mm hmm.

MR. GALLAGHER: And I confirmed it was a different programme that had been discontinued back in 2011. It wasn't a programme under Section 702, it was under some other provision of the FISA Act, but it was discontinued then. 11:05

MS. JUSTICE COSTELLO: Hmm.

MR. GALLAGHER: The second, the analogy to the American football pitch, he corrected me and said he had actually changed his analogy so we would understand it better, to a soccer pitch. 11:05

MS. JUSTICE COSTELLO: We are talking about the circles, but the corners?

MR. GALLAGHER: About the circles, yes. Judge, on page

131 of yesterday's transcript, I was opening page 35 of the PCLOB report which said: *"Unlike PRISM collections, raw Upstream collection is not rooted to CIA or FBI and therefore it resides only in NSA systems where it is subject to the NSA's minimisation procedures."*

And I said I thought that had changed. I was confusing a change that arose in relation to the 12333 that is mentioned in the expert reports, that *hasn't* changed. So the position -- 11:06

MS. JUSTICE COSTELLO: Which one hasn't changed, so I get it straight.

MR. GALLAGHER: Sorry, the Upstream explanation in page 35. 11:06

MS. JUSTICE COSTELLO: That remains as is?

MR. GALLAGHER: That remains as is. Sorry for that lack of clarity.

Judge, I have dealt at some length with the national security position and I just want to perhaps draw the threads together. We also have prepared a response to the speaking note of the DPC in relation to that which we will hand in (SAME HANDED TO THE COURT). I'm not going to go through that, but it summarises the points we want to make. 11:06 11:07

Judge, in essence our position with regard to national security, the primary position is that it's outside the

scope of the Treaty and the Charter and therefore an analysis or an assessment of the processing conducted by the national security agencies of a foreign state, in this case the US, is not subject to assessment by reference to either. That is our primary position on the basis of the section of the Treaty and the Charter that I have identified and of course also the Directive. 11:07

That approach, however, has not been adopted, as you know, in **Schrems** and by the Commission in the Privacy Shield in the sense that they have had some scrutiny of that processing by reference to the Charter. For the sake of the argument before you, we're adopting or accepting that position for the sake of the argument, reserving our position on the primary point if this were to go further. 11:07 11:08

Adopting the approach then of **Schrems** and the Commission, you do have regard and must have regard to the fact that the processing is conducted in a national security context. You must have regard to that because the Charter rights are going to be abridged or limited and national security and the associated, the foreign affairs of the US, they are legitimate objectives and they can in principle justify the abridgment of Charter rights or the limitation of Charter rights 7 and 8 and 47. 11:08 11:08

In order for them to justify or in order for the national security processing to justify an abridgment of the rights, you have to be satisfied that they haven't impaired the essence of those rights. For the reasons that we have urged on the court, the essence of the rights has not been impaired. There are limitations on the rights, but the essence is still there.

There has been no finding in the Draft Decision that the essence of the rights has been impaired. Indeed, the finding in paragraph 44 that there are remedies but there are limitations on the remedies is, in and of itself, inconsistent with a finding of an impairment of the essence of the rights. Paragraph 44 of the decision says the data subject is not completely without redress and a number of remedial mechanisms are available, and you will remember that paragraph 95 of **Schrems** talked about there being no possibility of redress.

MS. JUSTICE COSTELLO: What was the paragraph number again?

MR. GALLAGHER: 95, Judge, of **Schrems**.

MS. JUSTICE COSTELLO: Thank you.

MR. GALLAGHER: And in those circumstances, there's no question of the essence of the right, that's not a case that can now be made at this stage in an attempt to justify the position, it's in contradiction to the decision. And it's also of course inconsistent with

the approach of the Commission in the Privacy Shield which did not regard the essence of the rights being impaired and accordingly felt justified in applying the analysis that Article 52 of the Charter envisages, which I have called the strictly necessary analysis for short, but Article 52(1), as I indicated to you yesterday, says: 11:11

"*The limitation must be provided for by law or respect the essence of the rights, be proportionate, be necessary and be carried out to genuinely meet objectives of general interest or the rights of freedoms of others.*" 11:11

It's not obviously just confined to national surveillance, but that is the subject of the Draft Decision and that's what's relevant here. The Draft Decision is premised entirely on national surveillance. But law enforcement generally can do it and other considerations of general interest of the type that have been identified in the cases. 11:11

That's the analysis carried out by the Commission and it says it meets the requirements of Article 52 and that the limitations on those rights are strictly necessary. So, as I say, adopting that approach for the sake of the argument in this court and recognising the reality that this court is not going to differ from **Schrems**, the approach in **Schrems**, we say that the 11:11

failure to take account of the fact that it's within the sphere of national surveillance, to carry out the required assessment wholly invalidates the provisional conclusion which is done by reference to a freestanding abstract Article 47 right without recognising these factors at all. 11:12

It is also faulty or it's defective because it doesn't carry out the holistic analysis that is carried out by the Commission that's envisaged by Article 25, envisaged by paragraph 75 in **Schrems** - yes, 75 in **Schrems** - and it is an incorrect approach. It also fails to take account of the necessary balancing of rights. And, as the court will be familiar from our own constitution and tradition, rights are not absolute, they are always subject to limitation. And of course there are pre-eminent rights that are at stake here in terms of the national surveillance activities, the right to life, the right to security, all Charter rights recognised, ultimately the right to do business which is an important right and the fundamental raison d'être of the original Community and the continuing raison d'être of the European Union, the right to conduct trade. 11:12 11:13 11:13

A right that needs to be balanced, as will be recognised in the decision involving the European Data Protection Supervisor that I will be referring to later in the context of Article 25 and 26, an explicit

recognition by the European court that the supervisor, as it is called in that case, must balance and take into account that element of trade.

So the analysis is entirely wrong. Even starting from the premise, which the DPC would ask you to start from, there's been a failure to follow through the type of analysis that's required by the Charter and that's fundamentally defective. 11:14

I did draw attention yesterday that, in the **Digital Rights** case and indeed in the later **Watson** case, that the court did not regard the essence of the right being impaired, even though the Directive required the retention of *all* traffic data, and I stress the *"all"*, concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony, quoting: 11:14

"*It therefore applied to all - and I supervise 'all' - means of electronic communication, the use of which is very widespread, and of growing importance in people's everyday lives. Further, in accordance with Article 3 of Directive 2006/24, the Directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.*" 11:15 11:15

Paragraph 56 of **Watson**. And paragraph 57:

"*In this respect it must be noted that Directive 2006/24 covers in a generalised manner all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.*"

That was not held to destroy or impair the essence of the right. And of course, in considering that issue here, if you get to it, and I suggest you can't get to it because there has been no such finding by the DPC, but, if you thought it was necessary to consider it, those statements are of vital importance; but so also is the detailed analysis that I referred the court to yesterday as to the limitations and safeguards within the system and the fact that discriminants are used in targeting and that only a fraction of the communications are captured.

11:15 11:16 11:16 11:16

Those are very important, not only in the assessment of the validity of the limitations and in any assessment of proportionality, but they are also of vital importance in seeing whether the type of all embracing interference with data, admittedly to the extent of retention of the data, is of such a nature as to impair the right. I do acknowledge of course that in **Watson** and in Digital Rights it was the metadata rather than the contents that was retained, but it was emphasised that that was very significant. And you have the

11:16 11:16

evidence that in this case, while there is examination of content, it is done in the controlled and targeted way and limited way that is set out in detail, both in the PCLOB report, and perhaps in very great detail and by way of a practical explanation of the practice which **Schrems** requires the court to look at, or anybody carrying out an adequacy assessment, in Mr. DeLong's report. 11:17

It is important to stress the simple and obvious point that Mr. DeLong's evidence, Prof. Clarke's evidence, Herr Ratzel's evidence, none of that has been challenged in the slightest, but Mr. DeLong is in the unique position of being able to talk to what actually happens. And it is of course very significant that such evidence is before the court, directly from somebody who was involved, to correct the mistaken assumptions that underlay **Schrems** and to put before the court in a very transparent and complete way all of the relevant information that is unambiguously required by the case law and the emphasis as to how it operates in practice, the type of evidence that was missing from all of the cases, **Digital Rights**, **Watson** and everything else, and a measure obviously of how significant Facebook regard these proceedings and the importance of putting before the court a complete record. 11:17 11:18 11:18

That then, as I say, is the strictly necessary analysis which we say holds good and that in any event the court

is bound by the decision. And there is just one or two documents I want to briefly refer to in this context. Judge, the GDPR, which is the regulation that I referred to the other day.

MS. JUSTICE COSTELLO: That's the one coming in next year? 11:19

MR. GALLAGHER: Exactly, in a ham-fisted way, referring to it as a directive, but I'm glad to say that it's a regulation that you will find in that first book in divide 11 of the material. I don't want to overload the court with detail, but merely to make one -- 11:19

MS. JUSTICE COSTELLO: I think that boat sailed.

MR. GALLAGHER: Sorry?

MS. JUSTICE COSTELLO: I think that boat sailed.

MR. GALLAGHER: I was just going to say it was a bit late to express that regret, but it is genuine and it has been there since the beginning, it's not an afterthought. But I am perhaps even more conscious as time goes on. 11:19

There are just two matters, Judge, and, if you go to Article 2, just a simple point, it's on page 32. Just the material scope of this new regulation. You will see: 11:19

"1. The Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or

intended to form part of a filing system.

2. This Regulation does not apply (a) in the course of an activity which falls outside the scope of Union law." 11:20

So the exception is still recognised and the **European Parliament** case shows that the processing in the US is outside the scope of Union law, the act of transfer is not and the DPC's speaking note seek to confuse the two. They emphasise the transfer, which we have always accepted has to be governed by EU law, but they seek to ask the court to ignore entirely that the processing, which is of concern to the DPC, is a processing by the national security, it is that processing that is outside the scope of European law and it is that which dictates at the very least a strictly necessary analysis, even if one accepts, as we do, for the purpose of the argument that some analysis by reference to the Charter is required. 11:20 11:21 11:21

There is also some attempt, with the greatest of respect, to confuse matters further by suggesting that, if data is being shared by the US, which it is as you know in the uncontradicted evidence, that it's being shared by the Union under the common foreign and security policy provisions of the Union. That's wrong in the evidence. It's clear from Mr. DeLong and Prof. Clarke that it's shared with individual Member 11:21

States. But I draw attention to paragraph 2(b) which in any event makes it clear that the Regulation does not extend to Member States when:

"*Carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU.*" 11:22

Those are the specific provisions on the common foreign and security policy that are now part of the European Treaties, and a fundamental part of them. So even if that were so, it is excluded. 11:22

MS. JUSTICE COSTELLO: I just want to get clear in my head. You were talking about the, obviously there is two types of data processing, I think it's agreed by anybody. 11:22

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: There's the transfer from Facebook Ireland to Facebook Inc., were you accepting that that's not in the context of national security? It's the potential processing of personal data of EU citizens when Facebook Inc. is in receipt of it. 11:22

MR. GALLAGHER: Absolutely.

MS. JUSTICE COSTELLO: That you are arguing is governed by the national security?

MR. GALLAGHER: Absolutely, Judge. 11:22

MS. JUSTICE COSTELLO: I just want to get that clear.

MR. GALLAGHER: Yes. And we did make, and it's something that I did want to emphasise again. We did say it in our submissions. We couldn't obviously say

anything other than all, and our whole case is premised, all the evidence of Prof. Meltzer is this data is transferred for economic reasons, trade reasons, and nobody could contend that, in the light of Article 25 and 26, that the fact of processing of making it available is not caught by the Directive.

MS. JUSTICE COSTELLO: Mm hmm.

MR. GALLAGHER: But what is critical and what is elided in the DPC's submissions is that the objection is not taken per se to a transfer to Facebook Inc. in the US, the objection is taken because of the separate susceptibility to processing by the national security agencies in the United States. It is that separate processing that is outside the scope of the Treaty. The European Parliament makes that clear, specifically deals with it in the context of security processing, and in any event the wording of the Treaty.

So, therefore, if you are looking at the intrusions in the rights, you must look at it in the context that you're not dealing with intrusions in the private sphere, there's no complaint that the private law doesn't restraint private actors from abusing, if I can use that term, the data. It's that the public law governing the state doesn't specifically provide remedies. But you cannot look at that in the abstract by reference to Article 47, you have to take account that that is national security which inevitably involves an abridgment of Charter rights, so that is

the very important and fundamental distinction.

The last document that I want to refer you to in this context, having I am afraid found it struggling yesterday, it's in my fourth book of the EU agreed materials, it's divide 61 which I think is of more relevance -- oh, no, it's not. I have made the same mistake. Just one second, I do have it today. It's 53, I think, sorry. This is getting a bit too much. Yes, 53, sorry. 11:24 11:25

It is the same book - well, sorry, for me it's the same book, I'm sure it's not for you.

MS. JUSTICE COSTELLO: Oh it is, sorry.

MR. GALLAGHER: There is a reference to the Council of Europe - Prof. Swire talks about it - report, but you haven't actually been asked to look at it. I do want to ask you to look at it briefly. 11:25

If you'd be kind enough to just go to the first page, you will see it's: *"Democratic and effective oversight of national security services of council of Europe members."* 11:25

And if you go to page 7, *"National Practices in Council of Europe Member States"*, item 3. And the second paragraph of that: 11:25

"*It is emphasised that there is no Council of European*

of member state whose system of oversight comports with all of the internationally or regionally recognised principles and good practices discussed in this issue paper."

11:26

And then: "*There is no best approach to organising a system of security service oversight. Nevertheless, this issue paper seeks to highlight particular approaches or practices that offer significant advantages from a human rights perspective."*

11:26

And over the page, next page, you will see under the heading "*Independent Oversight Institutions*" that:

"*Expert security/intelligence oversight institutions play an increasingly prominent role in the supervision of security services. This issue paper adopts the view that they are fundamental to enhancing the efficacy of oversight and improving human rights."*

11:26

So oversight is critical. Then the *"Judicial Bodies"*:

"*Judicial bodies are primarily discussed with reference to the authorisation of intrusive surveillance measures. Attention is drawn to the fact that very few states require judicial authorisation for <u>bulk</u> surveillance measures, access to communications data or the use of computer network exploitation."*

11:27

And it says: *"This area of law lags behind developments in surveillance measures."*

And at the bottom, *"Internal Controls"*: *"Although the internal controls within security services are not a focus of this issue paper, it is essential to note that it is individual members of security services that play the most significant role in ensuring the security service is human rights compliant and accountable. External oversight can achieve little if the security services do not have an internal culture and members of staff that respect human rights."* 11:27 11:27

And the evidence you have on that comes from Mr. DeLong but also from Prof. Swire who carried out the classified review and confirmed he believed it and the PCLOB report that I referred you to yesterday, the sections where they didn't believe that there was -- sorry, the section quoted in Mr. DeLong's report where they didn't believe that there was deliberate evasion of controls. 11:27 11:28

MS. JUSTICE COSTELLO: And this is a 2015 document?

MR. GALLAGHER: This is a 2015 document. Those are very important, those are things that some witnesses sought to dismiss, but they clearly are critical. Mr. DeLong identified in great detail the extent of the compliance culture, the sanctions for people if they don't comply with it. Of course in that context you saw that the FISC rules, that I drew your attention to 11:28

yesterday, Rule 13, noted in the Adequacy Decision requires the NSA to disclose to FISC any non-compliance that is identified. There are now reports of non-compliance incidents, as Mr. DeLong explained.

MS. JUSTICE COSTELLO: I forgot to ask, what happens, does the FISC court then review the orders or what does it do? 11:29

MR. GALLAGHER: The FISC court then reviews, and obviously it can review the authorisation. It can identify whether the directives are being compliant with the authorisation and, as you saw, the FISC court ultimately can direct, as it did in the 2011 Bates opinion, to direct that a programme be discontinued. So those are very significant powers. Of course it is secret in the sense that it's not open to the public. It would be astounding and contrary to the whole purpose if it were. 11:29

But, on any assessment, the extent of the transparency between the court and now the reports that are published with regard to targeting procedures, compliance, oversight, there's been no suggestion that anybody else does better than that, and that goes as far as can consistently be gone in protecting the efficacy of the surveillance. 11:29 11:30

And of course the court will realise that, contrary to seriou7s crime, which has its own problems, and organised crimes as Prof. Clarke explained, you are

dealing with very sophisticated state actors, hostile countries with enormous IT ability, that even information that ordinary people might regard as not very disclosing of intelligence methods would be of immense value to them in undermining the effect of these programmes and in carrying out their own objectives. 11:30

So you are dealing in an area that is completely different from the enforcement of crime where, notwithstanding the sophistication of the organised gangs, it doesn't even approach what hostile states or terrorist groupings can marshal in terms of the ability to do damage in the form of the hostile actor described by Prof. Swire. 11:30 11:31

On page 32 you'll find at the bottom of the page:

"*The court has long recognised that the concept of effective remedy cannot carry the same meaning in the context of secret intrusive measures because the efficacy of such measures depends upon their remaining secret. In view of this, the Court has accepted that, as long as secret surveillance measures are either ongoing or cannot be revealed to the subject for other legitimate reasons, remedies need only be as effective as they can be given the circumstances. However, the Court has held that the fact that a person cannot be informed as to whether or not they are under* 11:31 11:31

surveillance or have been under surveillance should not preclude them from being able to raise a complaint with an oversight body. Such a body should be able to conduct investigations to ensure that any measures are being used in accordance with the law, without informing the complainant one way or the other. Once measures are known to the subject, as a result of a legal requirement to notify him/her, or they are otherwise revealed, he or she must have recourse to a body that can provide an effective remedy." 11:31 11:32

That's of course why the Ombudsperson procedure is regarded as so important because it is properly understood in the relevant context.

11:32

And then, Judge, on page 41 chapter, 4 what was in the summary *"there is no Council of Europe state"*, the last paragraph:

"*Whose system of oversight comports with all of the internationally or regionally recognised principles and good practices.*" 11:32

MS. JUSTICE COSTELLO: Sorry, I missed the page.

MR. GALLAGHER: Sorry, 41.

MS. JUSTICE COSTELLO: 41, thank you. 11:32

MR. GALLAGHER: And the last paragraph.

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: "*Equally it must be emphasised that there is no one best approach to organising a system of*

security service oversight. Diverse constitutional arrangements, legal and political systems, and historical contexts necessitate a range of approaches within the Council of Europe area. Accordingly, caution should be exercised when considering any wholesale importation or copying of examples from other states. There is, however, no doubt that there are models or practices that can be regarded as more effective."

11:32

11:33

And those examples are discussed.

If you go to page 46 at the bottom you'll see that they deal with the oversight committees in the form of parliamentary committees. And, at the top of page 47, it says, in the first line, first sentence, complete sentence: "*Beyond these committees with niche mandates, many parliaments have other committees whose remits cover aspects of service policy or activity.*"

11:33

11:33

So that's a recognised form of oversight. Judicial bodies are dealt with on page 52 and it says:

"*Although the courts may scrutinise and adjudicate on the action and output of security services in many contexts, this section will focus on the role of judicial bodies in authorising intrusive surveillance.*"

11:33

And then you see *"Complaints Against Security*

Services":

"*Regarding claims against security surveillance, most Council of Europe states offer the theoretical possibility of an individual bringing an action to seek a remedy. Bringing an action may be more straightforward when a person wishes to challenge an arrest, interrogation or detention. However, as mentioned, there are often significant obstacles to litigating against service services. Using the courts to challenge security service surveillance or data use is even more complex because, in most cases, an individual will not find out about such infringements of their rights.*" 11:34

11:34

And they quote the Venice Commission, and you remember Prof. Swire quoted that.

"*Challenges are only likely to be brought if an individual finds out about such measures through some form of notification requirement, by accident, from a whistleblower or through some other legal proceedings. There are sometimes explicit restrictions on persons seeking to challenge secret surveillance in ordinary courts before they have been notified of their having been targeted.* 11:34

The UK has created a special body."

And that's the Investigatory Powers Tribunal. And over the page at the first paragraph:

"*Although the types of measures requiring external authorisation vary, they commonly include the targeted interception of communications (where the person/organisation whose communications are to be intercepted is known at the outset), search and seizure of property and the installation of recording devices in dwellings. By contrast, in most states judicial authorisation is not, for example, required for information collection using human sources, untargeted bulk surveillance, computer network exploitation, searching pre-existing data banks.*" 11:35

Now on any version that report of the Council of Europe States has to be, even if the comparator is not the Member States, it has to be of major significance in assessing proportionality and the limitation and the acceptability of the limitation on the rights and perhaps put to bed, if I may say so, something that has taken a lot of the court's time in this case, this whole issue about the limitation on standing, which I will deal with briefly, and on redress as if this is some sort of US invention that exists nowhere else and that it is, in and of itself, creates a problem. It's not, it is standard and one has to assume that all of these Council of Europe States are presumed to be in compliance with the Convention. But, even if that were

not so --

MS. JUSTICE COSTELLO: The report you are saying?

MR. GALLAGHER: The report is obviously, but states are presumed to comply with the law and their international obligations. And, even if that were *not* the case, 11:36
clearly this is a vital matter to be taken into account and clearly taken into account in the approach of the Commission.

So finally then with regard to the approach in national 11:36
security, apart from all of those criticisms it was a wholly selective approach focussing on one aspect of the regime remedies for which there is no warrant or justification in the cases, it gave a distorted view of the position, it was taken out of context, it didn't 11:37
look at practice, it didn't look, even in the context of remedies, of non-judicial remedies, and while, by definition, a non-judicial remedy is not a judicial remedy, it is relevant in assessing the limitations on judicial remedies. And, most of all of course, it 11:37
failed to take into account the Ombudsman procedure which is regarded as vital and clearly is part of best practice.

There is some fairly lame, if I may say so, attempt to 11:37
make some mild criticism of it in the submissions, something that they are not entitled to do because it wasn't part of the decision. There is no suggestion on the part of the DPC that there is anything wrong with

the Commission decision or any basis for challenging it, and that is not something that they are entitled to do now.

I want then to move quickly to Article 25 and 26 of which you have heard much, and I have only one or two points to add to what is there. They are perhaps obvious to the court already, but they are a slightly different emphasis from, and I think important emphasis, difference in emphasis from the submissions you have heard already. 11:38 11:38

One thing is absolutely clear, Article 26 - and you'll find the Directive in...

MS. JUSTICE COSTELLO: I have it. 11:38

MR. GALLAGHER: Or, sorry, the decision, excuse me - the Directive is different from Article 25 in its approach, we know that, on any view, leave aside any linguistic analysis. There are just two aspects of Article 26(2) and (4) that I want to refer to. 11:38

Firstly 26(2) specifically addresses in the fifth line *"where the controller adduces adequate safeguards"*. In opening I said that was very important because, by definition, it could not be envisaged that the controller is going to address national security or public law or achieve a complete answer to any issue that might arise in that regard. 11:39

That is absolutely clear. Whether you use the word, adequate, sufficient or anything else, nothing could be clearer than that. And it's reinforced by 26(4) where the Commission is tasked, and there is no challenge to the Directive: "*In accordance with the procedure referred to in Article 21(2) that certain standard contractual clauses offer sufficient safeguards.*"

So what is to offer the sufficient safeguards? It's the contractual clauses. We know the contractual clauses can't change public law. So to conclude, as the DPC did, that you don't even look at the standard clauses because they don't change public law is, as you heard many times now, fatally flawed. But, more importantly in the context of what I'm now going to say, it just is inconsistent with any approach in the context of Article 26 that requires an adequacy of the law assessment.

11:39

11:39

11:40

Article 26 requires the controller to adduce the safeguards. They do actually address issues with regard to the mandatory provisions of the foreign law where the importer is unable to carry out the instructions of the exporter and a claim can be brought against the exporter in this jurisdiction, and Ms. Hyland will deal briefly with those.

11:40

So they do deal in part with it, but of course, even if they never dealt in any part with it, the answer is

that the solution lies within the terms of the SCC decision itself. And that's to be found in divide 10. You'll remember there is a recognition in the footnote in page 12 of that - sorry, not page 12, just one second - yes in page 12 under Clause 5, *"obligations of the data importer"* and the reference below to which I drew your attention to *mandatory* requirements, a recognition that you have all of these protections in place but they are of course subject to mandatory requirements of the third country. 11:41

And how do you deal with the mandatory requirements of the third country? As I said in part they are dealt with in the content of the model clauses, but in truth the solution is both clever, effective and obvious when you pause for a moment's reflection. 11:42

If you go back to Article 4 of this decision, which is the embodiment of the decision or the substantive part of it, on page 8 you see the answer. It says: 11:42

"*Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to the Directive, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing.*" 11:42

So if, notwithstanding the model clauses that are adduced to provide or introduced to provide the sufficient safeguards, specifically under the wording of 26(2) and (4), they don't work in the case of a third country, then the answer is you can suspend in respect of that country. Why is that there? It is there to give extra protection in the sort of situation that is now envisaged, but it also recognises, as I think Mr. Collins certainly said in passing, that the SCC decisions govern all third country transfers. You are being asked to invalidate, well not you because you can't do it, but... 11:43 11:43

MS. JUSTICE COSTELLO: It's only in relation to the US, not in relation to all those countries.

MR. GALLAGHER: No, but you see that's what they say. 11:43

MS. JUSTICE COSTELLO: Yes.

MR. GALLAGHER: They say it's only in relation to the US, but it cannot be invalidated only in relation to the US, it applies to everybody. So it's a complete misconception. And the reason it cannot be invalidated, because one country's laws don't meet the requirements, is because it contains within it the basis for addressing that: You suspend the flow to that country. But this is the extraordinary thing, and Mr. Murray shot up at one stage, 'it's only in the US' and in the statement of claim they say it's only in the US, but it's a complete misunderstanding; the SCC decisions, as you can see in their terms, relate to transfers to *all* third countries. 11:43 11:44

So the court, the European court couldn't be asked on the basis of concerns about the US to invalidate. It would mean the stopping of flows to all countries. And why would you do that when you look at the provisions of 4(1), if you are not meeting the requirements of the Directive, you suspend the transfer to that country. Who does that? The DPC, the person who **Schrems** says has all of the powers and, in paragraphs 41 to 45, it emphasises the importance of the role of the DPC, and in the **European Data Supervisor** case, that I will be coming to, it emphasises that. So let's see what the DPC can do. 11:44 11:45

So in order to protect individuals with regard to the processing, where? And this is the condition: It is established, so it must be established, not a well-founded concern: *"That the law to which the data importer process is subject imposes upon him requirements to derogate from the application data protection law - that's the law in Ireland - which go beyond the restrictions necessary in a democratic society as provided for in Article 13."* 11:45 11:45

So you remember Article 13 applies for restrictions that can be imposed on the entities within the Member State, this in a sense is an analogue; if the laws of the US or anywhere else require the person to go beyond or who require the person to do something which go beyond the restrictions, then the DPC intervenes, so it 11:45

has to be established that it does that, it hasn't been established here. And then you go on: "*Where those requirements are likely to have a substantial adverse effect on the guarantees.*"

11:46

So it's not just to show that they go beyond the restrictions necessary, there is a further condition: They have they have to have a substantial adverse effect on the guarantees provided by the applicable data protection.

11:46

So that's the solution. It is simple, it is coherent, it is neat, it provides the entire answer to the case, and it's amazing the DPC didn't have regard to the very powers which she has, but, you see, that would have required her to go through these steps and establish, but what she can't do is ask this court to lend its aid to a reference that is misconceived because it seeks an invalidation of the SCC decision, the SCCs decisions, in respect of third countries, because that would be its consequence, without dealing with the, without dealing with the powers that are conferred on her.

11:46

11:47

In a sense it's the opposite to **Schrems**. In **Schrems** the complaint was the DPC had powers which he never exercised. Well, this is the same thing, it is seeking this court's imprimatur that it goes off. And the court somehow somebody says 'well you don't have to go through that step and satisfy me that that step doesn't

11:47

stop'. If it is established you stop it. And that's why that's there. And the extent of this, there was some reference to the fact that Nasscom, which is an Indian trade body sought to be joined as amicus, they were too late and McGovern J refused it, but they recognised and everybody recognises than an invalidation of the SCCs stops their use for everybody. 11:48

And of course the effect of that would be catastrophic, it was something that was never intended. These were carefully introduced to allow for dealing with countries where there was no Adequacy Decision, because they are not required where there is an Adequacy Decision, but it also had an inbuilt protection if that country's laws overstepped the mark. And what's interesting and what is critical is the test is: Do the restrictions go beyond what is necessary in a democratic society, the very test that I have spent the last day and a bit explaining was the relevant test in the context of national surveillance and not the test applied by the DPC. 11:48 11:48 11:49

So that, as I say, is the answer in relation to that, and I want to hand in the decision in **European Commission -v- European Data Protection Supervisor**. We do have, I think, the folder for you now, Judge. Is the index agreed? It's been handed up, so at least you have something to put it into. There is just one statement here that elucidates -- 11:49

MS. JUSTICE COSTELLO: I think it was four volumes.

MR. GALLAGHER: Sorry?

MS. JUSTICE COSTELLO: I think it was four more volumes.

MR. GALLAGHER: Oh, I am sorry. Well, it is still better to have them, I suspect, in some as is all I can say lamely. 11:49

MS. JUSTICE COSTELLO: Put it this way: Mr. Kavanagh is busy putting my marked-up ones in.

MR. GALLAGHER: Thank you, and thank you Mr. Kavanagh. The decision, Judge, it really related to, the Commission complained that the European Data Protection Supervisor in Germany, it was against the German government, the intervenor was the European Data Protection Supervisor, but it complained that the supervisor in Germany wasn't sufficiently independent, it was subject to some parliamentary scrutiny, I think, with regard to the cost of the office and it was felt that the interference would be inconsistent with the importance of the position conferred on the DPC. 11:49 11:50 11:50

And if you go to page 1908 under the findings of the court you'll see the scope of the requirement of the independence of the supervisory authorities. And, skipping to paragraph 20, where it says: 11:50

"*In the second place, concerning the objectives of Directive 95/46 it is apparent from the third, seventh and eighth recitals in the preamble thereto that,*

through the harmonisation of national provisions on the protection of individuals with regard to the processing of personal data, that directive seeks principally to ensure the free movement of such data between Member States, which is necessary for the establishment and functioning of the internal market within Article 14(2)."

Then 21: "*However, the free movement of personal data is liable to interfere with the right to private life - that's recognised.*

22. For that reason, and as is apparent from the 10th recital, the latter seeks not to weaken the protection guaranteed by existing national rules, but on the contrary to ensure, in the European Community, a high level of protection of fundamental rights."

And then 23: "*The supervisory authorities provided for in Article 28 are therefore the guardians of those fundamental rights and freedoms, and their existence in the Member States is considered, as stated in the 62nd recital to the Directive, as an essential component of the protection of individuals with regard to the processing of the data."*

And then it goes on to 24: "*In other to guarantee the protection, the supervisory authorities must ensure a fair balance between, on the one hand, observance of*

the fundamental right to private life and, on the other, the interests requiring free movement of personal data."

So that is a very important aspect, as I have urged on the court, that trade aspect. It is a recognition of the power given to the supervisor. Article 4 of the SCCs is entirely consistent with that. That doesn't involve abandoning standards, it imposes a different approach to Article 25, but it reinforces the explanations you have already had as to why Article 25 test is not, could not and never was the correct test and that, to the extent that the standard contractual conditions cannot provide adequate protection in a particular case as against mandatory provisions of the third country law, there is a focussed, an individual, a targeted measure that the DPC can adopt that doesn't affect other third countries that are not party to these proceedings, whose laws haven't been examined and who may suffer from no such deficiency, if a deficiency were established and approved. And of course no such deficiency has been established or approved.

11:52
11:52
11:53
11:53
11:53

And can I, in the context of that, refer you just for one moment to the report of Prof. Meltzer which you will find in Book 4 of the court papers. I don't intend to delay on this, I would ask the court, as undoubtedly it will, to consider his evidence which again isn't challenged. Mr. Collins drew your

attention to the key expert opinions on page 2 as to the consequences, but also I think of interest in understanding this is page 17 which sets out the economic importance for the EU of cross-border transfers of personal data and sets out the relevant figures that arise in that context. 11:54

And then in 11.2 at the bottom of the page it refers to the US and EU economic relationship with the US: "*Is the most important trading partner outside the EU, accounting for 27.5% of the all exports and over 31.7% of all EU imports are from the US.*" 11:55

And then: "*United States investment in EU employs approximately 3.7 million Europeans.*" The transatlantic data flow, this is dealt with on page 18. In page 22 there is a section dealing with *"EU digitally deliverable services trade"* and the importances of the transfer of data in that. Page 24 deals with opportunities and *"the global internet"*, it says at 11.10: 11:55 11:55

"And cross-border provide a particular opportunity for SMEs to be engaged in the international economy."

And it is important, as I did emphasise when opening, that this materially concerns SMEs, small medium enterprises, and not just the giants that have been referred to here. This catches them all. The

explanation of course is even apart from, as he explains in the previous section to which I briefly referred, even apart from the IT companies, every US company that has a subsidiary or an associate in Europe and vice versa, they are trading data all the time, transferring data about employees and about people, about customers. It's just such an integral part of trade nowadays, as Prof. Meltzer explains, that it's difficult to conceive of trade without it. At page 28 he gives the quantitative effect and on page 31 a summary of what would happen if this transfer of data was interrupted. 11:56 11:56

So the importance of that again is not contested and, in fairness to Mr. O'Dwyer in that opening affidavit as I drew attention to, I think it was paragraph 107, he identified the Commission report which identified the enormous impact on GDP of Europe. 11:57

So that's Article 25 and 26. I then want to deal briefly with the position of the adequacy of US law, not because - briefly - not because it is not important, we very much contend that it is adequate, but because I think what's relevant to the court in making that determination can be summarised in a convenient way. And part of my submissions on this, I have mentioned to Mr. Murray, neither party is handing in further speaking notes, but I have said that I am going to hand in this document. It is just a 11:57 11:57

summary for the court of the sections, a table, so that you have them because it is mesmerising trying to remember the various provisions to which reference was made.

MS. JUSTICE COSTELLO: Thank you very much. 11:58

MS. DONNELLY: Judge, I just want to reserve our position.

MR. GALLAGHER: Oh, absolutely, they need to.

MS. JUSTICE COSTELLO: Thank you.

MR. GALLAGHER: I had given a copy, but I had meant to send it earlier and they haven't had an opportunity of looking at it. But it's just meant to be hopefully helpful to the court to help memorise the relevant provisions. 11:58

But can I just look at one thing first, this idea of standing that has taken so much time, and we say the resolution of the standing issue is simple, without doing any injustice to the learned witnesses who gave evidence, and really resolves or revolves, resolves itself into one issue or revolves around an issue and that is ultimately the question of knowledge that you have been the subject of surveillance. You will see or have seen in the Council of Europe report it is recognised that most people don't have that knowledge and therefore, as it says, have no possibility of challenging in the courts which is one of the reasons why the other procedures of oversight are so important. 11:58 11:59

That's recognised. But you have been treated, as I say, to an analysis of that with great particularity and great learning but that really was premised on an unspoken assumption that this was somehow extraordinary, had no mirror image anywhere else, that was unique, and certainly the Draft Decision creates that impression and fails to recognise the context. 11:59

If I can summarise very briefly what the court has heard, and this, I say, is on the *uncontested* evidence. **Lujan**, and as we know **ACLU -v- Clapper**, said that there are three elements of standing which the experts have actually agreed in their common report. And the first, as you know, is injury-in-fact; the plaintiff must have suffered an injury-in-fact, an invasion of a legally protected interest which is (a) concrete and particularised and (b) actual or imminent, not conjectural or hypothetical. 12:00 12:00

Then the second pillar is causation. There must be a causal connection between the injury and the conduct complained of. The injury has to be fairly traceable to the challenged action of the Defendant and not the result of the independent action of some third party not before the court. That's a concept you are familiar with and not one that generated any controversy; and, three, redressability. Third, it must be likely as opposed to merely speculative the injury will be redressed by a favourable decision. 12:00 12:00

That didn't generate any controversy. You did, Judge, ask, I think, during the course of some of the evidence on this whether somebody who did not have a Fourth Amendment right would satisfy the redressability prong of the standing analysis and you posited that or you asked the question whether a EU citizen, because they lacked standing on the Fourth Amendment, would not be able to establish that. 12:01

That is answered in the following way: The redressability prong asks only if the nature of the injury is such that it would be redressed by a ruling in the plaintiff's favour. It's independent of the cause of action in that sense. Obviously you have to have a cause of action. If you are an EU citizen, it's not under the Fourth Amendment, it has to be under the statute or the APA or whatever, but you just ask 'well if you establish your case is it capable, is the court capable of redressing it'. The answer to that was undisputed, it is; the court will stop the harm if it's continuing, make a declaration where that's appropriate, grant damages. So redressability is not the issue. 12:01 12:02

And in terms of injury-in-fact, the issue has really revolved on whether they can establish that there is an actual or imminent interference with the protected rights. If there is an abuse of data, of their data, that is sufficiently concrete and it is sufficiently 12:02

particularised and that was accepted by Prof. Richards and Mr. Serwin. Sorry, I'll leave the stenographers change.

And the actual or imminent, as opposed to conjectural or hypothetical, as you know, revolved around whether somebody, in the first instance, could sufficiently *plead* they were the subject of surveillance - if they didn't, they were struck out on the facial challenge, the initial dismissal - and if they did plead it, there could be an application for summary judgment on the basis that they didn't ultimately have sufficient evidence to support the pleas. 12:03 12:03

In the interval between the motion to dismiss on facial grounds - I suppose similar to our striking out because on the face of the pleadings there's no cause of action - if you survive that, you got your discovery. Obviously issues might, depending on the circumstances, arise with regard to state privilege, as they would anywhere, but you get your discovery and you get a chance then to produce the evidence that supports the pleas. And if you're unable to do that, you are then the subject of an application for summary judgment, as happened in **Amnesty -v- Clapper** and your case is struck out. 12:04 12:04 12:04

If, of course, you have evidence, as you might have, that you *have* been the subject of surveillance, if you

have the type of evidence that they had available in **ACLU -v- Clapper** then you can produce evidence to show that you are somebody who is particularly affected in a concrete way. The problem is having that evidence. And obviously there are significant constraints and being able to establish that unless you have notice that you were subject to surveillance.

Now, Prof. Vladeck gave evidence - and there is *some* disagreement, but no *fundamental* disagreement - that there are ways around it; you can, as they did in **ACLU -v- Clapper**, without direct evidence, have sufficient evidence by virtue of the leak and the extent of the meta-data programme to satisfy the court that they actually were affected. Prof. Vladeck said in the light of the Snowden disclosures that it's much easier now to establish the type of facts that they were unable to establish in **Amnesty -v- Clapper** at that initial stage before the disclosure.

But whether or which, if you have notice then you meet the standing criteria. If you don't have notice then you have difficulties, but no stranger difficulties or no more onerous difficulties than you'd face in Europe than you face anywhere in the context of national surveillance, as recognised in the Council of Europe decision.

So, far from being in and of itself some major

objection to the adequacy of the remedies, it is an inherent feature in this area, something recognised explicitly by the Commission in the Adequacy Decision, where it refers in the body of it - I just can't remember the paragraph for a moment, but I'll come back to it, give it to you - the body of the Commission decision, that standing is in issue and that can be raised and can create difficulties. That is what the DPC recognised, went no further *than* that. And in fairness, none of the experts go any further. 12:06 12:07

So the standing, which was the major objection to the adequacy of the remedies, resolves itself into the question of notice. And the question of notice is something inherent in this activity -- or lack of it is inherent in the activity - something that we now know is neither strange nor unusual - but an inherent part of the limitations that must exist if the objective is to be achieved and, therefore, acceptable. 12:07 12:07

It is worth reminding the court, if I may, of what was said with regard to the standing which supports that simple proposition. First, and from our evidence - and I'll deal with the concessions made by Prof. Richards and Mr. Serwin in a moment - Prof. Vladeck put it lucidly at day 12, page 63 where he stated: 12:08

"*Right. So I mean, again I think if the claim is that an EU citizen* believes *that their data has wrongly been*

collected by the US Government from a firm like Facebook, that's concrete. The question is not proving that that harm was concrete, the question is proving that that harm actually occurred. And so all of the pressure in that context is going to be on the actual or imminent prong of standing doctrine, not the concrete particularised prong."

"*Because I think there's just no dispute in US law that government data collection is a concrete harm whether it's lawful or not.*"

So proving the actual or imminent is the issue. And that, of course, relates to notice. And Prof. Richards, on day eight, at page 45 said: 12:09

"*... certainly in the private sector, somebody interferes with your e-mails and gets access to your e-mails, that's something which in and of itself is a harm that would sustain a claim, isn't that correct?* 12:12
A. Assuming the other elements of standing were -- injury in fact were met, yes.
Q. Well, I mean, there would be injury in fact if somebody accessed your e-mails and looked at the content, isn't that correct? That would be an injury in 12:13
fact. And it would be particularised as well, Professor.
A. I believe that's correct."

Now, that's in a private context. And you heard Prof. Vladeck explain that actually, in a government context that is even more the case. Similarly, on day nine, under re-examination from Mr. Murray, Prof. Richards accepted the following. He was asked: 12:09

"*Mr. Gallagher put to you and I think you agreed with him that*" --

MS. JUSTICE COSTELLO: Do you have the page reference, sorry?

MR. GALLAGHER: Oh, that one I'll come back to you. 12:10 It's just missing from my note. I do have it. On day nine, under re-examination with Mr. Murray, Prof. Richards accepted the following:

"*Mr. Gallagher put to you and I think you agreed with him that the interception of the contents of an e-mail or a telephone conversation, access as it were to the contents of the communication, was likely to be found to be concrete and particularised?* 11:08

A. That's correct." 11:08

At day eight, page 90, the following interaction with Prof. Richards occurs with respect to **ACLU -v- Clapper**:

"*Q. It's the court interpreting **Amnesty** and stating what it understands **Amnesty** to mean?* 14:26

A. Yes.

*Q. And therefore **Amnesty -v- Clapper** does not prevent standing where somebody can show that their data has*

been collected?
A. Yes.
Q. And --
A. As they were able to show in this particular case.
Q. In that particular case. And if that can be shown, 14:26
as it was shown in that particular case then there is an entitlement to relief?
A. If that can be shown, the injury [in] *fact element of standing has been satisfied and one would move on to the causation and redressability elements of standing."* 14:27

At day eight on page 126 he's accepted the following with respect to title 23 of ECPA and he says:

"*Yes. If you establish the* unlawful *use, you would* 15:22
have standing --
Q. You'd have standing.
A. - under this provision.
Q. So there's no issue about standing under the ECPA if you establish that somebody has unlawfully used or 15:22
disclosed the information?
A. I think you would have to prove that it was your information and that it -- but yes. I believe you're referring to the injury in fact requirement again?
Q. Yeah. 15:22
A. But yes, it is my belief that a violation of the unlawful use or disclosure provisions of the Electronic Communications Act broadly defined would suffice for stand -- if proven, would suffice to satisfy the injury

in fact requirement, yes..."

"*Q. And there's no complexity or difficulty or doubt about that, is there?*
A. With respect to the information covered by ECPA, no." 15:23

And at day eight, page 127 he also accepted:

"*If a person can prove that the contents of their communications certainly have been unlawfully intercepted, the injury in fact requirement, if they could find - and of course, notice remains a problem here - but if they find out about it and if they can prove and establish proof, then no, in those circumstances standing would be satisfied.*" 15:23 15:24

That was his answer, that was what he accepted. And the question then says:

12:12

"*Yeah. And it's not just the injury in fact, but the other two components would be satisfied as well, isn't that correct?*
A. The injury in those cases would be caused by the unlawful act of the defendant and the injury would be redressed by the deposition of the statutory damages." 15:24

That probably should be "*imposition* of the statutory damages".

"*Q. So there's no issue about standing at* all *there if you can do that?*
A. Under those facts, if proven, of course not.
Q. And is that stated anywhere in your report? 15:24
A. No."

At day eight, page 132, the following interaction with Prof. Richards occurred:

12:13

"*Q. I take it that you agree in the context of Section 1810 of FISA that if there is unlawful use or disclosure in* that *context and somebody can establish that, there is no difficulty about standing?*
A. If someone learns about it and is able to use the 15:31 *facts that they have learned about the secret acquisition of their data by whatever means and that it was unlawful under US law then it is my belief that standing would be able to be satisfied in that case, that is correct.*" 15:32

Importantly, on day eight, at the bottom of page 132 and top of page 133, the following interaction occurred with Prof. Richards:

12:13

"... *in those circumstances, standing is not complex or difficult to establish under those three statutory provisions that I've referred you to.*
A. In those circumstances, however factually unlikely,

it is my belief that standing can be satisfied, yes."

And the last three statutory provisions that are referred to in that question are ECPA, APA and 1810 of FISA. But clearly it applies to them all. The question is: Have you notice? If you *have* then the injury-in-fact element of standing can be satisfied. And there is no element of causation and redressability, because it's caused, the wrong is caused by the government surveillance or interception and it *can* be redressed either by damages or declaratory or injunctive relief. 12:14 12:14

At day ten, pages 31 and 32, in the context of a discussion of **ACLU -v- Clapper**, the following interaction with Prof. Serwin occurred: 12:14

"*Q. They are just there at the top. Sorry, just when you keep on going in the next column, when you go to the next column, top of the page: 'If the telephone metadata program is unlawful, appellants have suffered a concrete and particularised injury'?*
A. They are hitting all three elements of standing there. What they are saying is concrete and particularised injury, then they are hitting causation and they are hitting redressability.
Q. Yes, absolutely.
A. I think what they have done is kind of collapse the -- they are hitting all three elements of standing. 11:40 11:40

I will say they do not talk about actual or imminent in that paragraph. There is three elements of standing.
Q. Yes.
A. There is injury-in-fact, causation and redressability."

And I think it is fair to ask the question as to *why* this became such an issue when the *real* issue is the question of notice? And if there is notice then you can prove that you get over the actual or imminent, there's no doubt it's particularised or concrete, the causation doesn't arise and redressability doesn't arise, they're all fulfilled. And it's no different to our own rules; this is something the courts haven't had to grapple with in the context of data protection here. But normally a plaintiff has to --

MS. JUSTICE COSTELLO: In **Digital Rights** wasn't the mere possession of a phone sufficient?

MR. GALLAGHER: Absolutely. And I was going to deal with that

MS. JUSTICE COSTELLO: So that there was an inference, in effect?

MR. GALLAGHER: Oh, yeah. But, sorry, it didn't even require inference. It was an established fact. And the court notes that - you have the phone. The evidence, as I referred you to --

MS. JUSTICE COSTELLO: It was automatic for all...

MR. GALLAGHER: Everything. All. *All* communications. So it was on your data had been interfered with.

MS. JUSTICE COSTELLO: So that was like the Verizon...

MR. GALLAGHER: Exactly. So *everything* was caught. And *that's* why the court in that case didn't have any issue. But nobody has produced *any* case which deals with a situation of the type that is produced in the US. 12:16

I've referred a number of times and Ms. Hyland will refer you to it, because there's another aspect of it, but in the from a report, page 67 to which I've referred, I'll just read out the passage, I won't ask you to look at it. It's in my book four of 13 and it's in divide 61. But the passage is sufficient: 12:16

"*A judgment of the Federal Administrative Court in Germany illustrates the difficulties individuals face when confronted with strict procedural rules on providing concrete evidence to prove their victim status. In this case, a complaint was lodged against strategic surveillance of communications under Section 5 of the... Act by the Federal Intelligence Service (BND), after it was reported that 37 million communications were caught in 2010 by the dragnet search, mostly e-mails, of which only 12 were considered 'relevant'.*"

This is German intelligence.

"*The complainant argued that it was very likely that he*

was affected by the dragnet search because of his frequent international e-mail communications as a professional lawyer with contacts abroad; hence, he requested a statement that the BND acted in a disproportionate manner and violated his right to privacy of communications. The Federal Administrative Court, however, held that the complaint was inadmissible since complaints against strategic surveillance of telecommunications under the relevant domestic law were only admissible if it was evident *that the complainants had been affected. The court added that the right to an effective remedy does not mean that the burden of proof must be eased on the ground that the individual is not informed when the data collected through the search terms are immediately deleted.*"

So that was in Germany. And *no* intelligence agency says 'Actually, we confirm you are...' It would very easy to pick, to actually inter -- or to actually track 12:18
the approach of the intelligence agencies; lots of people put in requests, they're told *they're* not surveyed and it doesn't take the people who are engaged in this sort of business very long to establish patterns, to establish likelihoods of modes of 12:18
conveyance, timing, sectors that might be subject to surveillance.

So to confirm, not deny is something that is

recognised, particularly in the sophisticated agencies; I don't say that's so in every country, but it *is* something that is recognised in the Council of Europe report, it is something that the German court recognised. Obviously in other countries which don't have the sensitive national surveillance that perhaps the larger countries, things are different. But it's something that needs to be put in context.

But you can leave aside whether **Spokeo** -- and certainly the preponderance of the cases before you established that **Spokeo** *didn't* change the law and the judgment of the majority said they were only identifying the difference between particularised and concrete, which was already, they said, clear from earlier decisions. But in a sense, why were you bothered with all of that when it is accepted that there is a limitation in terms of your ability to be able to prove that depends on notice? But that is a limitation which, if it's not common to every national surveillance system, is common to many. And in this case there was undisputed evidence to justify it from Prof. Swire - he wasn't cross-examined on it - by Mr. DeLong, who wasn't cross-examined on it, and even Prof. Vladeck, who has a view about all of these things that he described as an outlier on the other side in terms of criticism, said he understood.

So that really was the standing. And then you look at

the substantive provisions. There's no great criticism of those. Those are extensive by any version, as you see from what's put before you. There are remedies that can be obtained. It *is* very noteworthy that Section 702 was omitted entirely from any analysis, 12:21
very significant. Everybody must, who is looking at the remedies in the focused way that Mr. Serwin was doing and Prof. Richards, should have adverted to it. A declaration and an injunction are very important remedies, even if you have to establish certain proofs 12:21
to get the declaration and injunction. It's not perhaps to --

MR. McCULLOUGH: You mean the APA, I think.

MR. GALLAGHER: Sorry?

MR. McCULLOUGH: The APA, I think. 12:21

MR. GALLAGHER: The APA. Oh, what did I say?

MR. McCULLOUGH: Sorry, it's a different section, 702 might not --

MR. GALLAGHER: Oh, it's Section 702 APA, sorry. There's the two sections. Sorry. And obviously you 12:21
don't get a declaration perhaps in quite the same circumstances you might get it here, it seems to be a bit more limited. But undoubtedly, if the matter is continuing, you'll get it. If it's not continuing, you'll have established the breach, you'll have got 12:21
redress because the illegality will have been established, you don't need a particular remedy.

The Section 18 USC 2712, or 18 USC 2712 ECPA, we've set

out in the table the remedies. It *is* willful violation. But as I said, that is not something that is unusual in actions against the state, and particularly in terms of damages. And indeed you did ask, Judge, in the context of the European Community, whether actions could be brought against - I should say Union - Union institutions for damages. And the basis for non-contractual liability is Article 340 of the TFEU, where the institutions must make good damage caused in the performance of their duties. But the case law - the Treaty doesn't say it - the case law says that it must be willful. 12:22 12:23

So that's not an uncommon requirement. And even **Schrems** says the laws don't have to be the same, the remedies don't have to be the same. And the interposition of that is understandable. And it's accepted that 2712 is a waiver of sovereign immunity, as APA waves it as well. 12:23

Then 18 USC 2707 ECPA; any intentional or wilful violation of the stored communication. And again we've set out sovereign immunity there applies to claims against the US, but officer suits are possible. 12:23

And 18 USC 2520; it provides persons whose wire, oral or electronic communication is intercepted, disclosed or intentionally used - the Wire Tap Act - damages, including punitive damages, sovereign immunity, and

references to what Mr. Swire notes.

Over the page, 1810, we've set out the position there - the Judicial Redress Act and Privacy Act. And it is acknowledged that in the context of the surveillance by 12:24
the NSA that's not of much use, it's not *actually* part of the Privacy Shield and Adequacy Decision. It *is* of use against other departments that might get it; Homeland Security, Department of Commerce, Secretary of -- or the Department of State - I think that's for 12:24
the foreign affairs - those are all subject to it, as are the Department of Justice. So it is of *use*, but it doesn't cover everything and there are limitations, as you know, and the issue with regard to covered documents. 12:24

Then Computer Fraud and Abuse Act and the Right to Financial Privacy Act.

So those are remedies. The problem, to the extent that 12:24
it exists, is, in standing, in establishing the actual element of standing, something that is a frequent provision in legal systems, something that can *actually* be got around. And Prof. Vladeck said something very important; he said if you plead your case properly -- 12:25
he said the posture of the case was so important, meaning the state of the case. Firstly, if it's pleaded, they won't get a dismiss. Then you get your discovery. And very often, he says, there can be a

settlement at that stage for all sorts of reasons.

So it's true, as Mr. Serwin said, defeating a motion to dismiss isn't a remedy. Of course it isn't, no more than defeating such an application here or defeating some attempt in the proceedings to constrain your case. But it's *part* of the remedy, it's part of the process and it *can* yield dividends. And of course, the existence of these remedies are very important constraints. 12:25 12:26

And what we haven't included there, but you'll remember, is that under FISA itself, directives can be challenged by the corporations and are being increasingly challenged or queried - you've the evidence of Facebook, very detailed and complex and comprehensive procedures that they engage in in dealing with these directives - and those companies can plead constitutional rights, can challenge, they clearly have standing. And in that process, you *can* get a determination of constitutionality that you wouldn't, of course, get by a challenge by a foreign national. But that limitation on the right to challenge the constitutional validity of a law is again a feature of many legal systems and all of the systems differentiate between the position of foreigners and citizens to some degree. 12:26 12:26 12:26

So Mr. DeLong also --

MS. JUSTICE COSTELLO: But is that the comparator, or whether an EU citizens here in the EU could challenge the provisions of a -- relies on the Directive?

MR. GALLAGHER: You're absolutely right. I alided the distinction between two separate things. You're looking at the remedies *available* to the EU citizen. But, Judge, when looking at the *limitations* on those, that's a factor that you can take into account, the proportionality, the fact that that is something that exists. But I shouldn't have allided both. 12:27

So, Judge, obviously I could spend a great deal of time on the US law - it wouldn't be fair to the court to do so at this stage and the task presented by some of the witnesses to the court of some minute analysis of the decision is not one we say the court ought to engage in; even on the *uncontested* evidence, the agreed evidence, there are substantial remedies and the limitations are not such as to make this inadequate, if that were the test, and it's not. They, looked at in the round with all of the other remedies, are very substantial. The standing has been overemphasised, as Prof. Vladeck said. And it really comes down to a question of notice. And if you analyse it in terms of notice, the complexity of the US law disappears. And it's clear there *are* adequate remedies and the question of proof doesn't make them inadequate in any real sense in the area of law in which we are talking.

So they are *only* inadequate in this notional abstract assessment of remedies, which in truth, though not stated, is done by way of a comparison with the remedies that might be available against a *private* actor. Constraints are inevitable in claims against the state and, as Ms. Hyland will briefly advert to, there are standing constraints in EU law and standing constraints in Irish law with regard to challenging. 12:28

The Article 4 amendment is a bit of a red herring. Let's take it that it's unlikely that a foreign citizen with no close connection with the US can rely on it -- 12:29

MS. JUSTICE COSTELLO: You mean the Fourth Amendment to the Constitution?

MR. GALLAGHER: The Fourth Amendment, sorry, excuse me. 12:29

MS. JUSTICE COSTELLO: There's a lot of articles. I want to keep straight.

MR. GALLAGHER: Yeah, sorry, the Fourth Amendment. Thank you, Judge. I've made that mistake before.

MS. JUSTICE COSTELLO: No, I want the transcript right so I can make sense of it. 12:29

MR. GALLAGHER: No, I did, I made it before and I was corrected, with an element of horror, by Prof. Richards, who said there is no Article -- well, there *is* an Article 4, but not this one. The Fourth Amendment. 12:29

The Fourth Amendment goes to the merits, it's a cause of action if it's available to you. You've heard from

Prof. Vladeck that even in terms of US citizens this right for damages, the **Bivens** right, isn't of much use. But they have other remedies. And it may well be that the courts will develop, in the case that's to be decided - is it the **Hernandez** case? Not the **Hernandez** case, the never -- I can't pronounce it, the ver-something case that's to be decided shortly about the shooting across - it is **Hernandez**; it's the defendant I can't pronounce - shooting across the border, whether it applies in that case. 12:30

And as Prof. Vladeck explained, there was an injury-in-fact there - the unfortunate boy had been shot - the Article 4 had nothing to do with standing, it had to do with the basis of the merits of the claim; 12:30 can you rely on that as part of your cause of action, which is separate from standing, or do you find some other basis for establishing a violation of your rights if that's not available? And here we have the statutory provisions that are available. 12:30

And it *is* significant when you're assessing the legal position to take account not only of the failure to adequately deal with this in the decision, but also to just reflect, if I may ask the court to do so - and 12:31 it's, of course, a matter entirely for the court - on what Prof. Vladeck said, his initial reluctance to get involved and then his willingness to do so because he thought they were material deficiencies in the analysis

of the adequacy. Mr. Murray tried to suggest that these were somewhat an academic oversensitivity. I don't believe they were anything of the sort, not least the APA. But it does show the dangers of engaging in the sort of partial exercise that the DPC engaged in, apart from anything else in that context. 12:31

So, Judge, standing is not the problem, with respect, it's been made out to be and shouldn't cause the court to conclude that there are well founded concerns with regard to the remedies and extensive remedies that are available in this context. 12:32

There was also the rather curious issue of Rule 11 raised by Mr. Serwin and quickly backtracked from and his subsequent memorandum and Prof. Richards making an attempt to suggest what he said didn't really say -- didn't really mean what it conveyed to the ordinary reader. But Rule 11, I think, is no different from our own obligation not to make wild accusations in pleadings, to have *some* belief that they *can* be substantiated, as Prof. Vladeck said, by reference to evidence or whatever - he said that he has never even heard it *discussed* in this context as an inhibition. And Mr. Serwin did, in fairness to him, admit that it had never arisen, he wasn't aware of it arising in any case. 12:32 12:32

But it shows the danger of proceeding, as the DPC did,

on a memorandum from an expert who had no knowledge or experience or expertise in national surveillance law raising an issue that's not an issue at all, achieving a prominence in her report. It's not even regarded in the Adequacy Decision - rightly so - because it is just ultimately so irrelevant. It's no impediment at all, but much time was taken in that regard. 12:33

And it *is* remarkable, as I said before, that we were not told that Mr. Serwin did *not* have an expertise - that emerged in cross-examination - and it does show the dangers of the exercise in which the DPC engaged in getting her own report, showing it to nobody, putting forward well founded concerns to the court, engaging in an expensive process that has involved us all and involved court time, ignoring the submissions of the US Government and indeed not giving Facebook any opportunity to comment on it that has led us to this position. 12:33 12:34

Then I want to come to the next item, Judge, and that is the court's concern, or the issue raised by the court as to whether -- sorry, whether -- the issue raised by the court as to whether, if the court had concerns, a reference could be justified on that basis. And the answer to that, we say, is emphatically no and is to be found unambiguously in **Schrems** in paragraphs 64 and 65. But also -- that's book two of 13 in mine and the divide is, I'll give it to you again, 36. But 12:34

also as a matter of principle.

I've drawn your attention to the passages in the Commission -v- European -- or **Commission -v- Germany**, I keep called it the European Data Protection Supervisor, 12:35
but it was about the role of the Data Protection Supervisors and its independence and the importance of that role. It's like, I suppose, the analogue we would be more familiar with here is where you have a procedure within a taxation statute or a planning 12:35
statute where there's a procedure to be followed and you then come to the court as part of that procedure. But it's not something that can be raised by the court separately, given that this is the procedure by which it's come before the court. And 64 and 65, on page 20, 12:35
draw that distinction very clearly.

"*In a situation*", 64 says, "*where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of* [the Directive]*, read in the light of Article 47... have access to judicial remedies enabling him to* challenge *such a decision adversely affecting him before the national courts.*"

That's what you're doing, you're challenging the decision of the DPC. And it says:

"*Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded.*"

So in the context that the claim is rejected as *unfounded*, the court must review that. And in that context it may decide that it's appropriate to put it forward on its own motion. Then that is distinguished in 65: 12:37

"*In the* converse *situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are* well founded*, that authority must, in accordance with the third indent of the first subparagraph of* [the Directive]*, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the... courts in order for them, if they* share *its* 12:37

doubts as to the validity."

So the distinction is drawn between the procedures. And it's understandable in the first the conclusion is that the complaint is *unfounded*. We, in our procedure, have a judicial review on that basis and in that context; when it comes before the court, the court can send it forward. The converse case, there's no mechanism provided for in the Act and in our general system where the DPC *shares* the view that the concerns are well founded. But the DPC can't declare that, that's a Commission decision that's binding on her, as **Schrems** explains, so all she can do is put it before the court, having carried out that analysis, analysis in respect of which she seeks deference to be given to her decision in her submissions. 12:38 12:38 12:38

MS. JUSTICE COSTELLO: I just want to tease that out as a matter of principle. What's the principled difference between disagreeing with the DPC's analysis of a complaint or agreeing with it? 12:39

MR. GALLAGHER: Because...

MS. JUSTICE COSTELLO: I mean, I understand what the judgment's saying there, paragraph four and five. But to draw the -- at 64 and 65. But to draw the distinction you're saying there, what's the principle distinction? 12:39

MR. GALLAGHER: Well, it seems that the principle of the decision, Judge, is that if the matter comes before the -- sorry, if the DPC has concerns that are well

founded, there is no procedure, as I said, in the law that that goes any further. The court mechanism is only engaged to *allow* it go further to comply with the obligation that it's the CJEU that must make the pronouncement. 12:39

And all the court is being asked to do in these terms is do you share the concerns of somebody who, in this instance, has carried out an investigation, who is the person, as you'll see when I go back to paragraphs 41 to 43, that is given this special position and has this special expertise? And what the court is saying is if that person has carried out the wrong analysis then you don't have any valid analysis which you can share. The procedure is the DPC will go back, will examine it again and *then* it may come forward to the court. But what is envisaged in the normal way by this procedure is that the analysis be done by the DPC. And therefore, all the court is being asked to do is to *share* those doubts by reference to what the DPC has done. And in the normal way, where somebody who is in a statutory position - as it would be under Irish law - has failed to carry out the proper analysis of the decision is not effective, then you say it goes back, there's nothing to stop the DPC looking at the matter again, taking into account criteria that the court has identified and the court explaining why it doesn't share the doubts. 12:40 12:40 12:40 12:41

But the court is not being asked in this context to do some freestanding analysis. This is meant to be a fairly simple and straightforward procedure. But the court is not being asked to do its own freestanding analysis. And what is clearly envisaged is, in those circumstances, the court should say the DPC, who is the person who is given the statutory function, should look at it afresh. That's what would be done normally in our system and it seems to be the distinction that's being drawn here. As a matter of principle that's not unusual, because the person that *is* given the statutory task, if they don't do it properly what is normally done is they're asked to *do* it properly. 12:41 12:41

So the court doesn't go to the second stage, the court looks and says 'Are those doubts well founded? Do I share they're well founded?' If the court says 'No, I don't' then it doesn't go to the second stage of saying 'I have other and separate doubts'. What is appropriate in that instance is a proper analysis is done by the DPC and then it comes forward. So that is an important distinction. 12:42 12:42

Judge, if you look at paragraphs 40 -- 39 really to 46, those are the paragraphs, and 40 perhaps to -- sorry, 40 to 45 on page 17. What the court is trying to do in those instances is to identify - or the CJEU - is to identify the importance of the role of the DPC. It is *enshrined* in the Directive, it is *enshrined* as a 12:42

consequence in the legislation and it is the DPC that is given this role as guardian. The court's role is of a supervisory role and the court will look at the decision and see if it's well founded. And if it's not then that's not something that the court transmits to Europe - that's not envisaged - the procedure is it goes back to the person who has the duty, the primary duty of carrying out the analysis. And it may come forward again in those circumstances if, having looked at the matter in the light of the court's directions, the Commissioner forms a similar decision. 12:43 12:43

So I think the principle is rooted in the special position of the DPC and the fact that these analyses, Judge, are envisaged as happening at DPC level as opposed to somebody coming to court and bypassing the DPC. And that is why, if there is an inadequacy, the appropriate step for the court to take is to afford the DPC an opportunity of addressing that inadequacy, carrying out the - when I say "inadequacy" there, I should say defect in the decision - carrying out the proper analysis. 12:44 12:44

And it is noteworthy, Judge, that the court does draw that distinction very much. It uses the words of its own motion in the context of paragraph 64 and clearly doesn't use it in the context of -- 12:44

MS. JUSTICE COSTELLO: 65.

MR. GALLAGHER: -- 65. And that is --

MS. JUSTICE COSTELLO: But in the sense where you're saying where the court's role is supervisory and it's the situation where the DPC has refused or rejected the complaint and the complainant brings, in our system, a judicial review, or maybe it might be to the Circuit Court, it's not confined to the analysis of the DPC in rejecting it -- 12:45

MR. GALLAGHER: That is --

MS. JUSTICE COSTELLO: -- or the arguments put forward by the complainant -- 12:45

MR. GALLAGHER: That is true.

MS. JUSTICE COSTELLO: -- as to why she was wrong.

MR. GALLAGHER: That is true.

MS. JUSTICE COSTELLO: The court, of its own motion... So is that a bit more than supervisory? 12:45

MR. GALLAGHER: Well, I don't think so. I agree with you, sorry, it's *not* confined in that way. And the *reason* it's not confined in that way is if the court is *lending its name* - because that's what the court is being asked to do - then the court has an independent obligation under EU law to ensure that all of the appropriate information is put before the European Court. That is something that's inherent in the Article 263 process. And of course, the court *cannot* ask the EU to pronounce if it finds there are all sorts of matters not considered by the DPC that are relevant. 12:45 12:46

So that's why you're not confined. But that doesn't lead to the next step, that having looked at that

evidence, as you *must* do in deciding whether you share the doubts and, if so, make a reference, that you embark on some analysis of your own and say 'I am now not putting forward the DPC's doubts', which is what the court seems to envisage, 'I'm actually putting forward my own doubts in the matter'. That doesn't *appear* to be envisaged. 12:46

I can't say that you could never, in theory, have such a situation that the principle is one that could never embrace that, but the principle as recognised by the court here does draw that clear distinction. And the reason why you go further than the DPC is for that overriding obligation in relation to EU law. And certainly, even if you had an *entitlement*, Judge, there is no obligation to do so, you still have a discretion, it's not *necessary* to determine this case. In this case you can determine it by saying the Commissioner's are not well founded. That disposes of the particular difficulty and it goes back in the normal way and is addressed. 12:46 12:47 12:47

I suppose there's another reason, Judge, while one should be slow in those -- or, sorry, there *are* the other reasons which I've indicated to you why one should be very slow as a matter of discretion to put it forward here, given the process that does exist, which won't exist in all cases and didn't exist back at the time of **Schrems** of where this issue is now going to be 12:47

determined by the institution that is given the *obligation* of looking at adequacy under Article 25. So in this particular case, adequacy isn't the test under Article 26. The Commission carries out the adequacy assessment and that is going to be carried out in July. 12:48

MS. JUSTICE COSTELLO: I know I'm jumping around here, but just seeing as you mentioned that there, one of the things that I want to stand back and make sure I don't get lost in the labyrinth and just playing forward; if the Standard Contractual Clauses were to be declared 12:48 invalid by the Court of Justice if a reference were made, is the data permitted then to be transferred pursuant to Privacy Shield under Article 25?

MR. GALLAGHER: Oh, yes.

MS. JUSTICE COSTELLO: So is that one of the reasons 12:49 you're saying this is a moot? Because even if these are struck down, vis-à-vis the US...

MR. GALLAGHER: Yes, absolutely. And of course, I'm not jumping back --

MS. JUSTICE COSTELLO: Because I know you were talking 12:49 about it being a collateral challenge to Privacy Shield. I was wondering whether you envisaged somehow that being implicated in any decision of the CJEU or whether it was still going to stand. Because --

MR. GALLAGHER: Yeah, it's very difficult to see that 12:49 the CJEU would even *embark* on an analysis --

MS. JUSTICE COSTELLO: Possibly I'm asking to you do a moot. But anyway.

MR. GALLAGHER: Yeah. No, but just to answer your

question, the CJEU will embark on an analysis of adequacy in the context of the SCC decisions, not just because that's not the test, but because the court would recognise that an assessment of adequacy involves a level of complication and detail that the *Commission* is *specifically charged* to conduct. So you would wait to see what it says after its review. That would be what you would challenge, if you were challenging *anything* at this stage. It's after the review whether its says it's right. It would be an entire and utter moot. 12:49 12:50

If the SCCs were declared invalid - and it's difficult to see how they could *ever* be declared invalid if the Privacy Shield had made a *finding* and which was never challenged that the law was adequate, because the *ground* is *inadequacy*; that's misconceived because of Article 4, as I have said - but then you just transfer, in any event under, the Privacy Shield, because that covers everything. I mean, if you have your finding of adequacy under Article 25, you'd need -- 12:50 12:50

MS. JUSTICE COSTELLO: Oh, yeah, you're under 25, you don't need 26. Yeah.

MR. GALLAGHER: Exactly. That's exactly it. But if the SCCs, contrary to all our submissions, were declared invalid on the basis of *inadequacy*, that would pose a real problem. Because you have the Privacy Shield saying it's adequate; whether the court would be prepared to embark on that, I don't conceive that it 12:50

would be, I think it would have to address in that instance or postpone it until the adequacy issue was dealt with in the context of Article 25. There are two challenges in respect of that, as you know. But in any event, it's difficult to see anything being done until the further review takes place. And you have the input of all of the various bodies, including the Article 29 Working Party and the other people who were inclined to do it -- or who were entitled to do it. 12:51

The decision that I wanted to refer you to, Judge, on mootness at a European level is at divide 27 of book two, it's the **Gasparini** decision. And it is a decision that looked at the principle of ne bis in idem, the fundamental principle you can't be tried twice for the same matter. And it involved the courts in Spain interpreting a judgment of the superior courts in Portugal that evidently wasn't very clear as to what it meant. The facts, I needn't go into, but if you go to page 9259 at paragraph 38 you'll see: 12:51 12:52 12:52

"*The third question is based on the premiss that the criminal courts of a Member State declare that it has not been established for the purposes of the offence of smuggling that the goods are from outside the Community.*"

In other words, the premise that the person was entitled to an acquittal. Then 39:

"*Such a premiss is inconsistent, however, with the facts of the main proceedings as described by the national court and reproduced in paragraphs 16 to 18 of the present judgment.*

40. Admittedly, the majority of the defendants in the main proceedings allege that the national court has misread the judgment of the [Supreme Tribunal in Portugal]."

I needn't continue with that. Then if you go to 42:

"*In the light of the national court's reading of the judgment of the* [Portuguese court], doubts arise as to the admissibility of the third question.

43. On such a reading, the premiss upon which the third question is founded, namely the acquittal of the defendants because there was no, or insufficient, evidence that the goods were from outside the Community, is not present.

44. According to the Court's settled case-law, while the Court is in principle bound to give a ruling where the questions submitted concern the interpretation of Community law, it can in exceptional circumstances examine the conditions in which the case was referred to it by the national court, in order to confirm its

own jurisdiction. The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of Community law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer."

So the hypothesis principle. And just to go back why you couldn't do it of its own motion here. Supposing, Judge, I were wrong in my interpretation of **Schrems** 64 and 65; well, that's irrelevant, because you *can't* do it here. And the reason you *can't* do it here is you're bound by the Adequacy Decision, as I identified in the other passage in **Schrems** where the court is bound by the decision. And as I have said, that has *not* been challenged. Even *now* the DPC doesn't say that was wrong. She was a member of the Working Party that was consulted in relation to it. And you saw, Mr. Collins put in the press release of the Working Party at the time. They will be consulted in the new process. But where it's not under challenge, then you just can't do it on the facts of this case. 12:54 12:54 12:54 12:55

As I said at the beginning, apart from that being a principle of EU law, of the binding nature of the decision, there is, of course, the fundamental aspect that it would be an injustice in terms even of our own

procedures that you would, as I said, through a side wind or collaterally, put in issue something that was not put in issue in the pleadings, that if it had been might well be addressed differently, other issues might arise, issues of evidence etc. So it cannot *be* introduced in that way or any issue arising in relation to it. 12:55

And you'll see in paragraph 52 of **Schrems** where it says the organs are bound by it. So in this case, I don't think that issue arises for your consideration. 12:56

I want to try and finish, Judge, so unless there's another question on that --

MS. JUSTICE COSTELLO: No, not at all. Thank you. 12:56

MR. GALLAGHER: -- I'm going to move to the next two matters very quickly, really one matter I think that I have to deal with -- two matters that I want to deal with very quickly.

12:56

EO12333. I would remind the court that, as Mr. Collins said on day two, page 69, line 19, that:

"*I think as a broad principle one can say that actual intelligence activities that take place outside the US I think are conducted pursuant to EO12333, with which we are not really concerned. Because we are only concerned with what happens to date when it goes to the US and how it is processed or accessed within the US.* 12:56

So we're not actually concerned that much with EO12333."

And we say that's correct. We're looking at the laws of the US as they apply in the US to data transferred and stored in the US. That's what was assessed in the decision. 12:57

In any event, the matter is dealt with in the Privacy Shield with a recognition that different rules apply to what is conducted outside the US and there is no holding that there is any lack of adequacy because of the existence of 12333. In fact, all of the constraints, and in particular PPD-28, were regarded as very important in bringing an Executive Order, which is, of course, a species of law - not the same as a statute, but is nevertheless binding and has legal effect - that those constraints were sufficient to satisfy the Commission. And also there is the fact in paragraph 75 of the Commission decision noting that there is no acknowledgment of the use of -- 12:57 12:57 12:57

MS. JUSTICE COSTELLO: Did you say 75 or 95?

MR. GALLAGHER: 75. Of the Adequacy Decision, sorry.

MS. JUSTICE COSTELLO: Yes, I have that.

MR. GALLAGHER: Of the Adequacy Decision. No acknowledgment of the use of 12333 in the manner speculated on. And the -- that that obviously applies. 12:58

Sorry, I'm helpfully passed just a note on the matter

that I was missing, Judge, the reference on day nine to Mr. Richards' evidence. And it was page eight. You'll remember --

MS. JUSTICE COSTELLO: Thank you. Yes, I'll put it in my notes. 12:58

MR. GALLAGHER: Yes, page eight and line five. The other matter that I want to just very, very briefly deal with, if you go to the book of submissions - I'll be about five or six minutes on this and I'll use the two minutes before lunch, if I may - and just look at 12:58 the Plaintiff's submissions. As I say, we didn't have these when we filed our submissions, but there's one or two stand-out items that I just want to draw attention to; I think we've dealt with most of what we say are the errors. 12:59

But if you go to page six there's the extraordinary submission in paragraph 14:

"*It is apparent*" - this is referring to 65 of **Schrems** - 12:59 "*that the making of the reference is **required***", they say, "*where two elements are present.*

*(1) First, the Commissioner must **'consider'*** that the objections are *'well founded'; and*
(2) Second, the Court must 'share [the Commissioner's] doubts'.

*15. The first element is clearly a **subjective***

requirement which, as is evidenced by the Draft Decision, has already been fulfilled."

That seems to be an assertion of some protection from scrutiny, which would be unique, I think, in our system. Of *course* she has to consider - so there's the subjective element - but *even* if it is demonstrated that the subjective consideration is based on an incorrect legal basis, is based on a failure to take account of relevant considerations and is objectively -- sorry, or excludes principles or material that ought to have been taken into account and adopts the incorrect methodology, the court isn't bound by that. The court would say 'You did arrive at a subjective consideration, but you arrived at that through a way that was incorrect in law'. 12:59 13:00 13:00

The only other matter is to ask the court to decide whether it shares the doubts. And they say that's straightforward. And as you know, the drum beat, or beaten at the very beginning is 'There's an easy way out for this, Judge. Just look at this and say "This locks horrendously complicated. I *undoubtedly* share the doubts. I have, I've found a doubt and I can send it".' Well, it's not the -- 13:00 13:01

MS. JUSTICE COSTELLO: I think the answer is get behind me Satan. But anyway.

MR. GALLAGHER: Exactly. It's *not* the approach actually that *is* the easiest - you can't do that - but

it would be a formidable task to prepare a reference that could share doubts that are manifestly wrong, but even if you got over that hurdle, that would identify all the material that would have to be sent to the court to determine something of such momentous importance, not just to the parties before this court, but to everybody else.

And for all of the reasons, as I said, the idea of the court sending a reference and saying 'I share the doubts, because that's what paragraph 65 tells me, and I have a few of my own, of the Ombudsperson' -- or, sorry, 'of the DPC, even though the DPC didn't do what she's obliged by law to do, take account of the decision' - the answer that she didn't want to wait for it is not an answer - 'even though the Commission has found this, even though she hasn't addressed the material in the Adequacy Decision' and send that off, that's not a cost-free exercise or an easy or appropriate thing to do.

Judge, I'll leave it there. I'll be five minutes, if that's okay, and then that's it.

13:01
13:01
13:02
13:02
13:02

(LUNCHEON ADJOURNMENT)

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

MS. JUSTICE COSTELLO: Good afternoon.

REGISTRAR: Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 14:05

MR. GALLAGHER: Judge, on Book 12 at paragraph 21 page 10, just for a moment.

MS. JUSTICE COSTELLO: 10, yes.

MR. GALLAGHER: At paragraph 32 in particular: "*The Draft Decision is unassailable*" it is said because it correctly applies the Directive. It doesn't. "*It correctly identifies the criteria against which the adequacy of US law is to be assessed.*" It doesn't. "*It correctly identifies the standard of protection against which the adequacy of US law is to be addressed.*" It doesn't. "*It correctly understands the requirement of Article 47 of the Charter.*" It doesn't. "*It correctly assesses US law and the preliminary view expressed therein is supported by the evidence filed in the proceedings*" and we say it's not, and I just want to deal briefly with some of those points. 14:05 14:05 14:06

If you go to page 27, they identify the correct understanding of the legal requirements of Article 47, most of the other points I have dealt with to date. But they say: 14:06

"*(i) An aggregate assessment is required.*

78. The Commissioner does not dispute - contrary to FBI's suggestion - that remedies ought to be assessed in aggregate, and while the Commissioner is criticised for concluding that the remedies are 'fragmented', it is manifestly obvious from the Draft Decision that she both reviewed the remedies in aggregate and that her conclusion that they were 'fragmented' could only have been reached as a result of an 'aggregate' analysis."

Well, she didn't look. Firstly she didn't identify the proper standard of Article 47, and we very much adopt Ms. Barrington's submissions in that with regard to what is required by Article 47. The fragmented conclusion was based on the Directive which doesn't apply. There was not a proper aggregate review, as we contend. 14:06 14:06 14:07

Then the next heading is *"Exclusions will Render the Remedy Ineffective"*. This is an extraordinary proposition. What's quoted is paragraph 95 of **Schrems**: 14:07

"*Likewise, legislation not providing* ***for any possibility*** *for an individual to pursue legal remedies in order* ***to have the 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****."* 14:07

That supports the proposition that if there is no

possibility for an individual to pursue a remedy the essence is not respected.

The paragraph is adverted to but it is misconstrued. It is now authority for a proposition that exclusions from relief will fail to satisfy the requirements of Article 47. There is no authority for that proposition whatsoever. 14:07

Then the next statement: "*Unjustified Immunities will Render the Remedy Ineffective*". And it then says: "*A remedy which precludes a 'procedural disadvantage'.*" Sorry: "*Requires an effective remedy which precludes a 'procedural disadvantage'.*" 14:08

As a matter of law that's incorrect, as Ms. Barrington has pointed out in her submission. The next contention is:

"*A remedy that imposes an Excessively Difficult Burden is not Effective*" and the **San Giorgio** case in a tax context is referred to, which of course doesn't address the issues that arise in this context at all, a common thread or failure on the part of the DPC. 14:08

The next proposition is: "*A remedy that requires the law to be broken to test it is not effective*", and they rely on **Unibet**. Well, **Unibet** supports our contentions with regard to Article 47, as Ms. Barrington has shown. 14:08

The fact that there are criminal offences during which the surveillance may be disclosed is not a remedy that is dependent or requires the law to be broken. It is a due process protection in a criminal context independent of and in additional to the civil remedies. 14:09

Then: "*Access to an independent authority is required*". They refer to the Advocate General in **Schrems**. Well, there are independent authorities, there's the court and there's of course also the FISC court. 14:09

"*Notification of processing is required*". This again is a failure to reflect the position in the decided cases in the Council of Europe. There is a reliance on **Watson** which self-evidently relates to criminal proceedings and the distinction between those proceedings is specifically adverted to in the footnote to which I drew your attention yesterday by the Commission that, criminal proceedings once they are over or during the course of them because they involve an individual, you can notify, they are completely different to surveillance in a national security context. 14:09 14:10

And then it says: "*Standing must be available to those within the scope ratione personae*". That's not correct as stated therein and it ignores in any event that the alleged difficulty with standing derives from the lack 14:10

of notification, and Ms. Hyland will deal with standing in any event.

Then the next proposition, not one reflected in the analysis of the DPC but now plucked out to justify it retrospectively: "*The essence must be preserved before balancing is considered*". That's true, but there is no such analysis conducted by the DPC and nothing to suggest or support a proposition the essence has been impaired. 14:10

And 92 just asserts that the exercise of the right, the *essence* of the right has been impaired without establishing a basis for that.

14:11

And then if you would go to page 34 and 99: "*The legal remedies that are available are not complete.*"

There is some criticism of the Privacy Act and the Judicial Redress Act. That is not essential to the adequacy of the remedies as the Privacy Shield discloses. In any event they don't have to be complete. 14:11

The next heading on the next page is *"Unjustified Immunities"*, that state immunity is unjustified. Well, you have seen the limitations on that, the ways around that. But how it could be suggested that the presence of State immunity in respect of certain remedies where 14:11

other remedies are provided derives somebody of an adequate remedy under Article 47 is difficult to understand.

Then again repeated at 36 "*Remedies that imposes excessively difficult burdens*", and that is a statement that is then supported by the wilfulness requirement which is not an excessively difficult burden and, if it is, then EU law, as I have indicated to you, is defective in terms of the remedies it provides. Again there's an expansion of the remedies that require the law to be broken on the next page. 14:12 14:12

On that page, 37, at 110: "*There will be no guarantee of access to an independent authority, even after the implementation of the Privacy Shield.*" 14:12

Well, this is remarkable. The DPC didn't consider it. She can't through submissions make any such point, it's not in issue in the proceedings. And in any event it's a misunderstanding of the significance of the Ombudsperson procedure, and you will see they attempt to make this point realising the significance of that in the next number of paragraphs. 14:12

The standing position is then dealt with in 116, and I have said much on that. And then in 120, it is said: 14:13

"*It is Commissioner's provisional view, as set out in*

the Draft Decision, that this host of frailties is such that the US law impairs the essence."

As I say that's not justified by anything in the decision. 14:13

In 124, they say: *"Given the lack of knowledge noted above of unlawful processing, and in the absence of proof of same, the remedy contemplated by Clause 6 may not be available to a complainant like Mr. Schrems in any event, because the relevant data controller would unquestionably contend that it could not be shown that it had even breached the SCCs, such as to trigger a remedy under the SCCs."* 14:13

Again that's a misunderstanding of the position at law in terms of the notification and the constraints on that. It's a misunderstanding of the rights that are given where you can prove that your data has been intercepted, which may arise in many instances, and in any event the issue of what level of proof you require in that regard would be a matter for Irish law because the proceedings would be brought in Ireland against the exporter claiming that there had been a breach. So there's a failure to distinguish between the substantive remedies given in the SCC that are specifically governed, as you know under the model clauses, by Irish law and the jurisdiction of the Irish court and there is also a mediation process. 14:14 14:14

And in 125, it says: "*In any event, there is a certain tension in the position adopted by FB-I, DE and BSA: anxious to highlight the inadequacies of the systems of protections in the Member States, while claiming that remedies for breach of the SCCs in national courts pursuant will address any concerns.*" 14:14

There is of course *no* inconsistencies, and that's a misunderstanding of the SCCs. The SCCs provide their *own* remedies as a matter of contract, independent of the legal system. And that just demonstrates, with the greatest of respect, the level of confusion on the part of the DPC with regard to the SCCs. 14:15

Moving to page 48, paragraph 148, it says that: "*The processing powers in respect of which the remedies are inadequate extend beyond the national security context. For example, FBI's own expert, Professor Swire, accepts that the relevant processing occurs beyond the national security context, noting that 'when the US government conducts a wiretap or otherwise against access to personal data in the US, the investigation within the US is governed primarily by either foreign negligence of **criminal rules'**. The remedial deficiencies arising are no less pressing in such situations.*" 14:15 14:16

Again a remarkable proposition. There is nothing in the decision that deals with the criminal law, it just doesn't address it. It is explicit in addressing

national surveillance. Process Prof. Swire, in giving a complete account of the law, drew attention to criminal enforcement and that is *now* stated to be some basis for supporting the concerns in relation to national surveillance. And of course, in any event, excludes any consideration of the protections in a criminal law sphere which haven't been even considered and the recognition in **Watson** and **Digital Rights** that criminal law enforcement can, in and of itself, provide a justified basis for a curtailment of the rights. 14:16

And two final points. When I was dealing with standing in the context of the US law, I did of course urge that it really came down to the question of notice. What I neglected to mention to you was there was another what I would call, with respect, not meaning to be in any way derogatory about the position, but there was a confusing factor, this question of **FAA -v- Cooper**, and the decision that, in the context of the Privacy Act, as you will remember it said the court had interpreted damage as requiring it to be pecuniary damage. 14:16 14:17

Firstly, the Privacy Act isn't relevant for the reasons that we have said, or of any prime importance is perhaps a better way of putting it, but in any event that only speaks to the type of remedy, you can't get damages, it doesn't preclude other remedies. And, as the submissions on Article 47 demonstrate, damages do not always have to be available. 14:17

The nature of the remedy is not a standing point in any event, it deals with the merits; what remedy do you get if you succeed, but there was no suggestion in **FAA -v- Cooper** you couldn't get another remedy, it was just a requirement for the damages. 14:18

And the final matter, subject to you, I, having spoken with Ms. Donnelly, agreed to defer. We, Judge, are very concerned about what was said with regard to the evidence of the experts and the criticisms that were 14:18 made that we believe are *wholly* unjustified. It's not something I'm going to get into now, we have delivered the affidavits. I'm going to hand into you a book that contains all of the correspondence and the affidavits because we would be very anxious that you would see 14:18 them. We are awaiting a response, they were demanded by lunchtime on Friday, we gave them til Friday. We haven't a response yet, but we are evidently expecting a response and if and when something arises I do want to reserve the right to deal with that shortly. 14:18

It's, I think, the only going to arise if there is some criticism of the witness as opposed to anything more substantive, but obviously it was of very significant concern to us that there be a criticism that we believe 14:18 is wholly unjustified. I don't want to say anymore or take anybody short at the moment. I did mention to Ms. Donnelly that I would just preserve my position on it and I think the Commissioner would prefer that we

have the response and deal with it in those circumstances, if it needs to be dealt with. That's subject to you, Judge.

MS. JUSTICE COSTELLO: Thank you.

MR. GALLAGHER: Thanks. 14:19

MS. JUSTICE COSTELLO: Ms. Hyland?

SUBMISSION BY MS. HYLAND:

MS. HYLAND: Yes, Judge. Judge, you have heard a great deal about the US and what happens in the US, and the question of the comparator has been mentioned but not, I think, dealt with in any detail. Judge, it seems that a useful exercise that I might now do is to give the court some material to consider how similar issues are treated in Europe by way of comparison. 14:19 14:19

Because I think sometimes one could have been forgiven for thinking, listening to the discussion that it was only in the US that (a) this type of surveillance took place and (b) these type of restrictions were in existence, and that is far from the case, Judge, and I hope that the material that I'm going to open to the court will show you a number of things. 14:19

14:20

First of all, Judge, I hope it will show you that surveillance takes place in Europe also, both traditional and bulk surveillance, and often on a very significant scale. I hope to show the very similar

issues, or in fact the very same issues arise in an EU context as in a US context in relation to matters such as the conditions under which surveillance should take place, the controls, the oversight provisions, both internally and externally, the question of the inherent limitations on notification to the subject of surveillance, the remedies to the persons affected and the particular role of oversight having regard to the limitations on notification. 14:20

The court knows that the Data Protection Directive does not apply in this national surveillance area because of the national security exemption. And however one characterises that, and there has obviously been various submissions made to the court, and the court has to make a decision on that, but however one characterises it, it is quite clear that the Data Protection Directive itself does not apply squarely in the area of national security for very obvious reasons. 14:20 14:21

In those circumstances one turns to the Member State law, the law of the Member States. Because all of the Member States are signatories to the Convention on Human Rights, and because the Convention on Human Rights does deal with this area, it does come within its scope, there is important and significant Convention jurisprudence, so I will look at that. 14:21

I will also look at a document that I think is very

helpful to the court. It's a report on surveillance in the Member States commissioned in 2015 from an agency called the Fundamental Rights Agency. And I have to admit that I was not aware of that agency until this case, but in fact it is an agency that was set up by a EU regulation and it is specifically charged under the EU structure with providing research and assistance on human rights. They carried out a report at the request of the European Parliament following the Snowden revelations. 14:21 14:22

It is a report which is done by way of a questionnaire format to all 28 Member States. There is also representatives of the from a in the various Member States and there was the assistance of experts. So it's a very authoritative report and it does what I think probably no individual expert before this court could do, it identifies a position in each of the 28 Member States in this area. So I think that will give the court a very helpful basis upon which to evidentially understand what is the position in respect of surveillance in the Member States. 14:22 14:22

Judge, I'll also take a closer look at the United Kingdom and Ireland because they are jurisdictions that this court is familiar with, not in huge detail, but I think it's no harm for the court just to hone in on what it looks like in two particular Member States. I'll also briefly then look at Article 47 itself and 14:22

particularly in respect of remedies and standing in an EU context. Because the court may be familiar with the fact that in fact the standing rules before the General Court and the Court of Justice, insofar as direct actions are concerned; in other words, if a person is seeking to challenge the legality of an EU measure, are in fact extraordinarily restrictive for individuals. Institutions of the communities are entitled to do that and Member States are entitled to do that, but effectively individual challenges can only go through the national courts and a reference if that is ultimately decided. 14:23 14:23

There's effectively no direct access unless a decision is addressed to you, like a competition decision or something of that kind, but, absent that, if a person is simply trying to challenge a piece of EU law they really cannot do it by way of a direct action, and I think that's relevant in this discussion of standing. It's more restrictive I think than anything we have seen in the US context. 14:23 14:24

And I'll finish then, Judge, by just dealing with the SCCs, and I will not repeat what the court has heard about the SCCs. There is a few discrete points I want to make, but apart from that I won't go over old ground. 14:24

So, Judge, I'm going to ask the court to look at some

of the case law of the Court of Human Rights, and it is going to be a gallop through it because in a sense I'm trying to do in an afternoon what we have spent a number of weeks doing in respect of the US but this time in respect of, if you like, various different Member States. But nonetheless I think one can get a flavour from the case law of the court about a number of points. I'll just identify you the themes, if you like, that one will see when we look at the case law. There's a number of themes that I think are relevant having regard to what you have been hearing on the US side. 14:24 14:24

First, the notion of prior judicial authorisation in respect of a surveillance measure. It's been stated by the court - and when I say the court now I'm referring to the Court of Human Rights - it's desirable but it's not mandatory. In respect of notification to a person who's been surveilled, the court accepts that notification cannot be given during surveillance as otherwise the purpose of the surveillance is likely to be defeated. 14:24 14:25

The court has identified that it is desirable to give notification once surveillance is finished, but only if that is possible. It recognises it may not be possible and it accepts that in certain instances other remedies may substitute for the notification obligations, and there are other ways of ensuring control over the 14:25

exercise of surveillance powers apart from notification and direct judicial actions by individuals.

In that context the court has noted that oversight by both what it describes as internal and external bodies is absolutely crucial, and one sees the court giving some considerable time and weight to the manner in which a Member State has set up their oversight controls. And when one understands that in the surveillance context often a person cannot be notified, it becomes clear why it is so important that the control must come in a different way and that is through oversight. 14:26 14:26

The court tends to treat evaluation of the substantive right and the remedy in a holistic way. It doesn't separate them out in a formalistic way. So when the court is looking to see whether or not there's been compliance with Article 8 of the Convention, which is how all of these cases come before the court - and the court will be aware that Article 8 is effectively very similar to what the court has been looking in the context, this court has been look at in the context of Charter, 7 and 8. 14:26

MS. JUSTICE COSTELLO: Hmm. 14:26

MS. HYLAND: And the court then also looks at the entire picture from start to finish, if you like, when considering if there's a breach of Article 8. It will look at the nature, the scope, the duration of

measures, the grounds required for ordering them, the authorities competent to authorise them, the carrying out of them, the supervision of them, the remedy provided; in other words, the whole picture will be looked at from start to finish. There won't be one aspect, if you like, of the exercise hived off and considered in isolation. When an Article 8 breach is asserted the court will look at the whole picture. 14:27

In relation to standing, standing is - I suppose there is two points to be made. First, there are the courts own rules about standing. And obviously they are not, if you like, the direct comparator here because any individual who is complaining about surveillance has to exhaust domestic remedies. As the court will be aware that's a requirement of the Convention, but nonetheless it is of some importance, I think, how the court treats standing. And essentially the court has dealt with standing is as follows, there's two different approaches. If actual interception is alleged, if a person is coming to the court and saying they have been the subject of interception, then the court has held that there must be a reasonable likelihood that surveillance measures were applied to the applicant. 14:27 14:28 14:28

On the other hand, if the individual is simply challenging an interference with Article 8 on the basis of the legislation in question, i.e. let us say there is a particular legislative structure which permits

secret surveillance measures and in that situation the court will exceptionally allow a person to challenge the particular legislation even if they haven't been able to show that they themselves have been surveyed.

14:28

If the national remedies will make it effectively impossible for a person to challenge at domestic level, it's a somewhat involved test, but what the court will do is it will look at what happens at domestic level, it will see whether it's possible to bring a challenge 14:29 and if it's not possible at domestic level then the court has said there's a greater need for scrutiny and in those circumstances one sees the court giving standing to people in that situation.

14:29

And I wonder, Judge, could I start by asking the court then to look at Book 13, and the tabs that I'll be looking at, Judge, are from Tab 39 onwards. And there's about, I think there's six cases.

MS. JUSTICE COSTELLO: 39 onwards? 14:29

MS. HYLAND: 39 onwards, exactly.

MS. JUSTICE COSTELLO: Just a moment. Yes, I have it.

MS. HYLAND: Well, they are all together in my book, they may not be in the court's book. So the first case, Judge, I'll spend a bit of time on this one 14:29 because, although it's a case from 1978, in fact it's still being relied upon by the court today. It's still the foundation of much of the court's case law, so I will spend the most time on this case because one

sees the findings being repeated over and over again right up until 2016.

This was a case where there was five German citizens that had launched the challenge to the relevant German legislation and they asserted that it was a breach of Article 8. Just in relation to this whole standing point, if I could ask the court to look please at page 4 of the decision. You'll see there at tab or paragraph 13, I beg your pardon, they say there that they claimed that they had been subject to surveillance measures. They didn't know whether the G10 had actually been applied to them and in fact the government made a statement saying that in fact they had not been the subject of surveillance measures. 14:30

And if I could just ask the court then to turn on please to page 14, you'll see there the comments of the court in respect of whether or not they had the necessary entitlement to bring the case. 14:31

You'll see there the top of page 14: "*The question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, owing to the secrecy of measures objected to, he cannot point to any concrete measure specifically affecting him. In the Court's view, the effectiveness of the Convention implies in such circumstances some possibility of*

having access to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious.

The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures." 14:31 14:31 14:32

And the court then goes on to consider whether or not Article 8 is to be infringed.

And asking the court then to turn over, Judge, to page 16 you will see the test and the test that they identify here is a test that is then used throughout all of the cases that we will see. There is a quote there at paragraph 39, top of page 16, of Article 8 of the Convention, and I think the court is probably 14:32

familiar with that.

You'll see at subparagraph 2 the test whereby:

"*There shall be no interference with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country.*" 14:32

14:32

And, Judge, I can tell the court that much of the discussion is not so much about whether or not it's in accordance with law, because once something is published in a statute or in some other identifiable provision it's treated as being in accordance with law. 14:32 The justification is not usually at issue in these cases either because usually there is a national security justification and the court accepts that.

The real, if you like, I suppose, issue between the 14:33 parties tends to be whether it's necessary in a democratic society, is it the minimum required in order to advance the aims sought to be achieved, and that's where one tends to see the discussions.

14:33

Judge, can I ask you then, you'll see then at paragraph 40 there was various restrictions under Article 10 of the basic law and of a law known as the G10 and this permitted surveillance. Paragraph 41, the first

question was whether the contested legislation constituted an interference with the exercise of the right.

And you'll see, going on down the page: "*The Commission expressed the opinion that the secret surveillance amounted to an interference with the exercise of the right. Neither before the Commission nor before the Court did the Government --*" 14:33

MS. JUSTICE COSTELLO: I am sorry, I have lost you, where are you on that? 14:33

MS. HYLAND: I am so sorry, Judge. It is just about two thirds of the way down the page, where it starts with the words *"in its report"*.

MS. JUSTICE COSTELLO: Oh, yes, thank you. 14:33

MS. HYLAND: Yes. You will see that there was no contesting of the issue as to whether or not there was an interference with 8.1 and the justification was that:

14:34

"*Any of the permitted surveillance measures would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and correspondence.*"

14:34

There was then a reference to: "*In the mere existence of the legislation there was involved a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the P&T*

services and constitutes an 'interference'."

So that is the fixed position, if you like, throughout all of the cases, one sees that and one sees the discussion being about 8.2. 14:34

Then moving over the page to paragraph 42 you'll see there: "*The cardinal issue arising under Article 8 is whether the interference so found is justified by the terms of paragraph 2. This paragraph, since it* 14:34 *provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the* 14:34 *democratic institutions."*

Can I ask the court to go down please - sorry well 43 you will see there in respect of *"in accordance with the law"*, that requirement was fulfilled because the 14:35 interference results from *"Acts passed by the Parliament"*. And that's the point I just made when that requirement was considering to be complied with.

Then going to the bottom of the page, paragraph 46: 14:35 "*The Court, sharing the view the Government and the Commission, finds that the aim of the G10 is indeed to safeguard national security and/or to prevent disorder or crime in pursuance of Article 8.2. In those*

circumstances."

And the court says it doesn't need to go and look at any other purposes.

But then it goes on to say: *"On the other hand, it has to be ascertained whether the means provided under the impugned legislation for the achievement of the above-mentioned aim remain in all respects within the bounds of what is necessary in a democratic society."* 14:35

Then going on to 48, the court takes judicial notice of two important facts: *"Technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance [over the mail, post and telecommunications] is, under exceptional conditions, necessary in a democratic society."* 14:36

Then paragraph 49, this is an important paragraph because again one sees this throughout the case law:

"*As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national* 14:36 *authorities any other assessment of what might be the best policy in this field.*"

And then the court goes on to say: "*Nevertheless, the Court stresses that this does not mean the contracting* 14:36 *states enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining, even destroying democracy on the ground of defending it, affirms that the Contracting States may* 14:36 *not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*

50. The court must be satisfied there are adequate and 14:37 *effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances.*"

And this is the point, Judge, I made about, if you 14:37 like, the holistic assessment: "*It depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities*

competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."

Judge, just then moving on to the second paragraph and, sorry, the second part of paragraph 51, it's about half way down that same page. 14:37

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: You will see there, they are just talking about the conditions under which surveillance may be ordered and here they may be done by a: 14:37

"*Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the supreme land authority."* 14:37

So there is an administrative procedure in place. And then turning over to page 20 at paragraph 53:

"*Under the G10, while recourse to the courts in respect of the ordering and implementation of measures of surveillance is excluded, subsequent control or review is provided instead, in accordance with 10.2, by two bodies appointed by the people's elected representatives, namely, the Parliamentary Board and the G10 Commission."* 14:37 14:38

And the court then gives some detail about the nature of those bodies and the Minister's relationship with

those bodies. And can I ask the court then to go on down to paragraph 55.

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: "*Review of surveillance may intervene at three stages: When the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity are not to be exceeded. One of the* 14:39
fundamental principles of a democratic society is the rule of law."

And then, looking at 56: "*Within the system of surveillance established by the G10, judicial control* 14:39
and excluded, being replaced by an initial control effected by an official qualified for judicial office. The Court considers that, in a case where abuse is potentially so easy in individual cases and could have

such harmful consequences, it is in principle desirable to entrust supervisory control to a judge.

Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G10, the Court concludes that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society. The Parliamentary Board and the G10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling." 14:39 14:40

And then the court goes on to consider the issue of notification, it says: *"The Court notes in addition that an individual believing himself to be under surveillance has the opportunity of complaining to the G10 Commission and of having recourse to the constitutional court. However, as the Government conceded, these are remedies which can come into play only in exceptional circumstances."* 14:40

"As regards", I'm looking at 57 here, Judge.

MS. JUSTICE COSTELLO: Hmm.

MS. HYLAND: *"As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality.*

The applicants' main complaint is in fact that the person concerned is not always subsequently informed after the suspension of surveillance and is not therefore in a position to seek an effective remedy before the courts. Their preoccupation is the danger of measures being improperly implemented without the individual knowing or being able to verify the extent to which his rights have been interfered with. In their view, effective control by the courts after the suspension of surveillance measures is necessary in a democratic society to ensure against abuses; otherwise adequate control of secret surveillance is lacking. 14:40

In the Government's view, the subsequent notification which must be given since the Federal Constitutional

Court's judgment corresponds to the requirements of Article 8.2. In their submission, the whole efficacy of secret surveillance requires that, both before and after the event, information cannot be divulged if thereby the purpose of the investigation is, or would be retrospectively, thwarted."

And then going to paragraph 58: "*In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.*

The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the court's view, insofar as 'the interference' resulting from a contested legislation is in principle justified under 8.2, the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the 'interference'.

Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction." 14:42

And the court then goes on to say, turning over the page: "*The Court has examined the contested legislation in the light of the provision of the considerations. The Court notes that the G10 contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the court must assume that in the democratic society of Germany the relevant authorities are properly applying the legislation at issue."* 14:42 14:43

And at paragraph 60 the court then concludes that the German legislature was: "*Justified to consider the interference resulting from the legislation as being necessary in a democratic society*" and no breach of Article 8 is found. 14:43

Then, Judge, Article 13 is considered. And Article 13, you'll see at paragraph 61 there, it's the remedies and

it's the, I suppose, equivalent or at least the genesis of Article 47 that this court is considering. And you will see it says: "*Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority* 14:43 *notwithstanding that the violation has been committed by persons acting in an official capacity.*"

The court considers generally Article 13. And then asking the court please to look at paragraph 65, the 14:43 court says: "*Although the court has found no breach of the right guaranteed by Article 8, it falls to be ascertained whether German law afforded the applicants an 'effective remedy before a national authority' within Article 13.*" 14:44

And, turning over the page, Judge, you will see there at paragraph 67, which is about two thirds of the way down, you will see the second paragraph of 67 says:

14:44

"*In the Court's opinion, the authority referred to in Article 13 may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the* 14:44 *remedy before it is effective.*

68. The concept of a remedy, an 'effective remedy' in the applicants' submission, presupposes that the person

concerned should be placed in a position, by means of subsequent information, to defend himself against any inadmissible encroachment upon his guaranteed rights. Both the Government and the Commission were agreed that no unrestricted right to notification of surveillance measures can be deduced from Article 13 once the contested legislation, including the lack of information, has been held to be 'necessary in a democratic society'."

14:44

And the court then goes on to say at the bottom of that page: "*The Court has already pointed out that it is the secrecy of the measures which renders it difficult, if not impossible, for the person concerned to seek any remedy of his own accord, particularly while surveillance is in progress. Secret surveillance and its implications are facts that the Court, albeit to its regret, has held to be necessary, in modern-day conditions in a democratic society, in the interests of national security. The Convention is to be read as a whole and therefore, as the Commission indicated in its report, any interpretation of Article 13 must be in harmony with the logic of the Convention. The Court cannot interpret or apply Article 13 so as to arrive at a result tantamount in fact to nullifying its* 14:45 *conclusion that the absence of notification to the person concerned is compatible with Article 8 in order to ensure the efficacy of surveillance measures. Consequently, the Court, consistently with its*

conclusions concerning Article 8, holds that the lack of notification does not, in the circumstances of the case, entail a breach of Article 13.

69. For the purpose of the present proceedings, an 'effective remedy' under Article 13 must mean a remedy that is as effective as can be having regard to the restricted scope for resource inherent in any system of secret surveillance. It therefore remains to examine the various remedies available to the applicants under and German law in order to see whether they are 'effective' in this limited sense." 14:45 14:46

Judge, we do place particular emphasis on that paragraph because it just show that one cannot in this sphere simply pull out the notion of a remedy, ignore the difficulties in respect of notification, ignore the requirement of surveillance and identify the remedy as flawed without even looking at those issues which we say that is precisely what the DPC did. 14:46 14:46

Just going back then to the case. At paragraph 70: "*Although, according to the G10, there can be no recourse to the courts in respect of the ordering and implementation of restrictive measures, certain other remedies are nevertheless open to the individual believing himself to be under surveillance: He has the opportunity of complaining to the G10 Commission and to the Constitutional Court. Admittedly, the* 14:46

effectiveness of these remedies is limited and they will in principle apply only in exceptional cases. However, in the circumstances of the present proceedings, it is hard to conceive of more effective remedies being possible." 14:46

So, Judge, that's the case of **Klass**. As I said it still remains one of *the* most important, if not the most important case and is frequently cited by the court as the court will see. 14:47

Can I ask the court then to go on a case that I only need to spend a very short amount of time on and that's at Tab 40, it's the case of **Silver**. This was a case, a little bit different to a surveillance case, it was a 14:47 case about prisoners whose letters had been intercepted by the prison authorities and they were complaining that that was a breach of their Article 8 rights. And there is just one part of this case I would like the court to look at and that's at page 28. 14:47

In fact it's in the context, just at the bottom of page 27 you will see the heading is *"Article 13 taken in conjunction with Article 8"*, so again we're looking at the remedies. I should say that the court had already 14:47 concluded that there had been a violation of Article 8 in some cases but not in others in relation to the treatment of individual letters. And then going to the Article 13 point you'll see there that the court,

turning over the page, at paragraph 113:

"*The principles that emerge from the Court's jurisprudence on the interpretation of Article 13 include the following.*" 14:48

And then there's a number of principles. The first is that: "*Where an individual has an arguable claim to be the victim of a violation of the rights set forth in the Convention, he should have a remedy before a national authority.*" 14:48

And (b): "*The authority referred to in Article 13 may not necessarily be a judicial authority.*"

14:48

I think you have already seen that in the previous case.

And then, importantly, this is the part that I would like to draw the court's attention to: "*Although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so.*" 14:48

And the court will be familiar that one of the DPC's complaints was that there was a fragmentation of remedies, and we say that that is not problematic in the European context, an aggregate of different remedies is permissible and again in **Leander**, the next 14:48

case I'm about to come up, we see the court saying the same thing again. So there isn't a requirement under the Convention at least to have one sole unified route and remedy and it is permissible to have an aggregate.

14:49

Judge, can I then ask the court please to turn on to the **Leander** case that I have just mentioned. And again this was a case, not so much about surveillance in the sense that this court has been looking at it, but rather it was in relation to information that had been 14:49 kept about the applicant which he was not permitted to see in the context of a job application.

So just turning then to Tab 41 you'll see the case of **Leander -v- Sweden**. This was a person who had got a 14:49 job as a museum technician with the Naval museum. He was then refused permanent employment with that museum on account of certain secret information which allegedly made him a security risk. He said that the vetting that had taken place on him involved an attack 14:49 on his reputation and he should have had the opportunity of defending himself before a tribunal, and the question was whether or not there was a breach of Article 8 and of Article 13 in that respect.

14:50

And if I can ask the court just to turn please to page 15, and again we see the test that already the court is becoming familiar with, i.e. whether or not the restriction was necessary in a democratic society in

the interests of national security. And if I could ask the court to take it up at paragraph 58 at the top of page 15.

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: And he says there, I beg your pardon, the court says there: 14:50

"*The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.*

59. However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life.

There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing suitability."

And then the court notes in the next paragraph that the contested interference adversely affected his legitimate interests in respect of access to certain sensitive posts.

14:51

And the court then went on to say: "*In these circumstances, the Court accepts that the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in particular in choosing the means for achieving the legitimate aim of protecting national security, was a wide one.*

60. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse."

14:51

And the court will recognise that from **Klass**.

"*61. The applicant maintained that such guarantees were not provided to him under the Swedish personnel control system, notably because he was refused any possibility of challenging the correctness of the information concerning him.*

62. The Government invoked twelve different

safeguards, which, in their opinion, provided adequate protection when taken together:

(i) the existence of personnel control as such is made public;
(ii) there is a division of sensitive posts into different security classes;
(iii) only relevant information may be collected and released;
(iv) a request for information may only be made with regard to the person whom it is intended to appoint; 14:52
(v) parliamentarians are members of the National Police Board."

And, sorry, the National Police Board were the body, Judge, that had compiled the information and provided the information. 14:52

"*Information may be communicated to the person in question; the Government did, however, concede that no such communication had ever been made, at least under the provisions in force before 1983;* 14:52
(vii) the decision whether or not to appoint the person in question rests with the requesting authority and not with the National Police Board; 14:52
(viii) an appeal against this decision can be lodged with the government;.
(ix) the supervision effected by the Minister of Justice; Chancellor of Justice, Parliamentary Ombudsman

and the Parliamentary Committee on Justice.

63. The Court first points out that some of these safeguards are irrelevant in the present case, since, for example, there was never any appealable appointment decision. 14:53

64. The Personnel Control Ordinance contains a number of provisions designed to reduce the effects of the personnel control procedure to an unavoidable minimum. Furthermore, the use of the information on the secret police register in areas outside personnel control is limited, as a matter of practice, to cases of public prosecution and cases concerning the obtaining of Swedish citizenship." 14:53

Then they go on to say, importantly: "*The supervision of the proper implementation of the system is, leaving aside the controls exercised by the Government itself, entrusted both to Parliament and to independent institutions.*

65. The Court attaches particular importance to the presence of parliamentarians on the National Police Board and to the supervision effected by the Chancellor of Justice and the Parliamentary Ombudsman as well as the Parliamentary Committee on Justice."

And then the court identifies the involvement of the parliamentary members of the board and their participation.

And the court then goes on to say: "*The supervision carried out - two paragraphs down - the supervision carried out by the Parliamentary Ombudsman constitutes a further significant guarantee against abuse, especially in cases where individuals feel that their rights and freedoms have been encroached upon.* 14:53 14:54

As far as the Chancellor of Justice is concerned, it may be in some matters he is the highest legal adviser of the Government. However, it is the Swedish Parliament which has given him his mandate to supervise, amongst other things, the functioning of the personnel control system. In doing so, he acts in much the same way as the Ombudsperson and is, at least in practice, independent of the government. 14:54

66. The fact that the information released to the military authorities was not communicated to Mr. Leander cannot by itself warrant the conclusion that the interference was not 'necessary in a democratic society in the interests of national security', as it is the very absence of such communication which, at least partly, ensures the efficacy of the personnel control procedure.

The Court notes, however, that various authorities consulted before the issue of the Ordinance of 1969, including the Chancellor of Justice and the Parliamentary Ombudsman, considered it desirable that the rule of communication to the person concerned, as contained in section 13 of the Ordinance, should be effectively applied in so far as it did not jeopardise the purpose of the control.

67. The court, like the Commission, thus reaches the conclusion that the safeguards contained in the Swedish personnel control system meet the requirements of paragraph 2 of Article 8. Having regard to the wide margin of appreciation available to it, the respondent State was entitled to consider that in the present case the interests of national security prevailed over the individual interests of the applicant. The interference to which Mr. Leander was subjected cannot therefore be said to have been disproportionate to the legitimate aim pursued." 14:54 14:55 14:55

And, Judge, we say that that's a very important case from an *oversight* point of view. Because what one sees there is that Mr. Leander was not entitled to look at the information, he wasn't allowed to challenge it, he wanted to do that and he couldn't do that. But there were other bodies who were conducting an oversight function and in particular the court identified the Parliamentary Ombudsman, the Parliamentary Committee on 14:55

Justice and the Chancellor of Justice. And the court accepted that these controls were effective restraint on abuse and that, therefore, was sufficient so that the decision was not held to be in breach of Article 8.

14:55

We say that the reason that's so important in this context is because one cannot assume, as the DPC did, that one simply looks at one particular remedy and once that remedy, on her account, was held to be inadequate, if you like the inquiry ends there. We say that, consistent with the approach of the court in this case and in all the cases we see, you must look at the totality of the picture and that's what we see here.

14:56

Then just turning over, Judge, in relation to the Article 13 point. Again we see Article 13 being invoked by Mr. Leander. Turning over the page to page 18, just two paragraphs there. You'll see paragraph 78:

14:56

"*The court has held that Article 8 did not in the circumstances require the communication to Mr. Leander of the information on him released by the National Police Board. The Convention is to be read as a whole and any interpretation must be in harmony with the logic of the Convention. Consequently, the Court, consistently with its conclusion concerning Article 8, holds that the lack of communication of this information does not, of itself and in the*

circumstances of the case, entail a breach of Article 13."

And then there is a reference to Article 13 and whether or not there was an effective remedy. And you'll see there that the court, going to paragraph 84, concludes that: "*An effective remedy must be a remedy as effective as can be, having regard to the restricted scope for recourse inherent in any system of secret surveillance for the protection of national security.*" And the court holds there was no breach of Article 13. 14:57 14:57

And can I ask the court then to turn on please to the case of **Weber** and that's at Tab 42. Again this is another German case and it's about the same law that the court already looked at in the context of **Klass**, but that law had been amended and extended in respect of the possibilities of surveillance, and there was a fresh, and this is now in 2006, and there was a fresh challenge to that law. 14:57 14:58

Just looking at the first page of that case, Judge, you'll see there that the first applicant Ms. Gabriele Weber, is a German national, The second applicant, Mr. Saravia, is a Uruguayan national. They both live in Uruguay. 14:58

Then turning over, Judge, please, there's a description of them, but essentially they worked for, oh yes,

turning over the page to page 2 paragraph 5.

"*5. The first applicant is a freelance journalist who works for various German and foreign newspapers, radio and television stations on a regular basis. In particular, she investigates matters that are subject to the surveillance of the Federal Intelligence Service, notably armaments, preparations for war, drug and arms trafficking and money laundering. In order to carry out her investigations, she regularly travels to different countries in Europe and South and Central America, where she also meets the persons she wants to interview.*

6. The second applicant, an employee of Montevideo City Council, submitted that he took messages for the first applicant when she was on assignments, both from her telephone and from his own telephone. He then transmitted these messages to wherever she was."

14:59

And if I could just ask the court then to skip on a number of pages to page 9. I'm just going to identify a few of the characteristics of the law in question which are quite similar to what you have already seen in the US context. So, looking at paragraph 32 of that decision, you'll see there that: 14:59

"*The Federal Intelligence Service was only authorised to carry out monitoring measures with the aid of*

catchwords which served and were suitable for the investigation of the dangers described in the monitoring order. The second sentence of the provision prohibited the catchwords from containing distinguishing features allowing the interception of specific telecommunications."

A little bit like what you have already seen in the US context. And then: "*However, this rule did not apply to telephone connections situated abroad if it could be ruled out that connections concerning German nationals or German companies were deliberately being monitored (third sentence). The catchwords had to be listed in the monitoring order."*

14:59

And so one sees there that there is a different rule applying depending on whether or not German nationals are at issue or whether that's not the case. That's a little bit like some of the minimisation procedures you saw in the US context. I think the stenographers wish to change, thank you.

15:00

Then just going on with the conditions:

"*The execution of the monitoring process as such had to be recorded in minutes by technical means and was subject to supervision by the G 10 Commission. The data contained in these minutes could be used only for the purposes of reviewing data protection and had to be*

deleted at the end of the year following their recording."

So I'm not trying to draw an absolute parallel, because the detail of that would be impossible in the time, but just to show that the same kind of themes and the same kind of issues arise in the context of this legislation here as we've already been dealing with in the context of the US system. 15:01

Then, Judge, can I ask the court to skip on please and the court will see then that -- could I ask the court to look please at paragraph 114? And it's at page 26. And this was in the context of the court looking at the purpose and necessity of the interference, going back to the core question again. And starting at paragraph 114: 15:01

"*The Court is aware that the 1994 amendments to the G 10 Act considerably extended the range of subjects in respect of which so-called strategic monitoring could be carried out under section 3(1), the central provision at issue here. Whereas initially such monitoring was permitted only in order to detect and avert the danger of an armed attack on Germany, section 3(1) now also allowed strategic monitoring in order to avert further serious offences listed in points 2 - 6 of that section. Moreover, technical progress now made it possible to identify the telephone connections*

involved in intercepted communications.

115. While the range of subjects in the amended G 10 Act is very broadly defined, the Court observes that... a series of restrictive conditions had to be satisfied before a measure entailing strategic monitoring could be imposed. It was merely in respect of certain serious criminal acts... that permission for strategic monitoring could be sought."

Then there's a description of what kind of permission is required. And the permission is where there is a reasoned application by the President of the Federal Intelligence Service or his Deputy. And the decision to monitor had to be taken by the federal minister empowered for the purpose by the Chancellor - in fact a little bit like the previous provisions in **Klass** that we've already seen. 15:02

Then, Judge, turning over to paragraph 117, again we see the supervision and monitoring. Again a bit like **Klass**, there was still the Parliamentary Supervisory Board and there was still the G10 Commission, which had to authorise surveillance measures and had substantial power in relation to all stages of interception. And the court noted that in **Klass** it upheld that system of supervision and it saw no reason to reach a different conclusion. 15:02 15:03

Then again an issue that you saw in the context of the US system, paragraph 124, the transmission of data to various authorities. And you'll see here that the authority, they say the Office For the Protection of the Constitution as well as to other authorities, and the applicants contended that this was an interference with their rights.

If one turns over to page 30 and paragraph 128, you'll see there that the court analyses the decision to transfer, looks at the controls and decides the control is sufficient. At paragraph 128 the court says:

"... *the decision to transmit data had to be taken by a staff member of the Federal Intelligence Service qualified to hold judicial office, who was particularly well trained to verify whether the conditions for transmission were met. Moreover, as clarified in the Federal Constitutional Court's judgment, the independent G 10 Commission's powers of review extended to verifying that the statutory conditions for data transmission were complied with.*"

So again we're looking the an oversight body. Then, Judge, in relation to this question of notification, if I could ask the court to turn over to the next page, page 31. And there is a long quote at paragraph 135 from **Klass** and from **Leander**, which the court has already seen. And at paragraph 136 the court looks at

the situation under this legislation and notes that:

"... *individuals monitored were to be informed that their telecommunications had been intercepted as soon as notification could be carried out without jeopardising the purpose of monitoring.*"

The Court noted that:

"*The Federal Constitutional Court again strengthened the safeguards against abuse... by preventing the duty of notification from being circumvented.*"

Then just going to the bottom of that paragraph, we're still at the top -- sorry, we're top of page 32, but just towards the bottom of that first paragraph: 15:05

"*The Court finds that the provision in question, as interpreted by the Federal Constitutional Court, therefore effectively ensured that the persons monitored were notified in cases where notification could be carried out without jeopardising the purpose of the restriction of the secrecy of telecommunications.*"

Then the conclusion was that the respondent state, within what the court described as its fairly wide margin of appreciation in that sphere, was entitled to consider the interferences with the secrecy as being

necessary in a democratic society.

Then just to ask the court to turn to page 36. We see a somewhat different treatment of Article 13 which appears to be now the present approach of the court where they don't in fact have a separate analysis of Article 13 any more; once they've looked at it in the context of Article 8, they simply say that 'We have done the analysis in an overall context and we don't have a separate analysis'. And we see that here at page 36. And at paragraph 156 at the bottom of the page: 15:05 15:05

"*The Court has found that the substantive complaints under Articles 8 and 10 of the Convention are manifestly ill-founded. For similar reasons, the applicants did not have an 'arguable claim' for the purposes of Article 13, which is therefore not applicable to their case.*"

And they rejected the Article 13 claim on that basis. Then if I could ask the court to look at an important case, **Kennedy**. I suppose important from two respects; first of all, I think it's a case --

MS. JUSTICE COSTELLO: Sorry, what number is **Kennedy**? 15:06

MS. HYLAND: I'm sorry, Judge, it's at tab 44. It's just the one --

MS. JUSTICE COSTELLO: It's the next book for me.

MS. HYLAND: Oh, sorry, it's the next? Very good,

Judge. Apologies.

MS. JUSTICE COSTELLO: Yes?

MS. HYLAND: And I suppose this case, we would identify it as important for two reasons. First, it does give some considerable detail, I think, to the standing requirements of the court itself, the Court of Human Rights itself, and the level of interest a person is required to have in order to be allowed to bring their case to the court. 15:07

And it's also relevant because it identifies the situation in which a Member State - in this case the UK - where they had no notification provisions, but nonetheless their system was held to be compliant with Article 8 because there was an entitlement to make a complaint to the IPT, the Investigative Powers Tribunal, which I suppose in some ways can be analogised to FISA or to FISC; it's a court -- I will ask the court to look at a judgment later on of that court. One doesn't see -- it's certainly not as -- only in recent years one is able to see the judgments. There wouldn't be, I think, as many judgments available as we've seen in the US context. But it is not *dissimilar* in certain respects. So we say that the case of **Kennedy** is important from that point of view. 15:07 15:07 15:07

The facts of this case were somewhat strange, Judge - you can see them at page two. But essentially what had happened was the applicant had been arrested for

drunkenness, had been put in a cell and in the morning his cellmate was dead and he was charged with murder. And that conviction was quashed, he was then retried and he was convicted of manslaughter. He served, I think, some nine years. He then was released and he started a campaign for victims of miscarriage of justice. 15:08

He was running a business called Small Moves, a removal business, and he then began to experience interference with his phone calls. He said he was getting hoax calls and he was getting calls not being put through to him and he said that he was being intercepted by the police because of his history and also because of his lobbying on behalf of victims of miscarriages of justice. And it was in those circumstances he brought a case challenging the surveillance that he alleged was taking place in respect of him. And ultimately the case made its way to the Court of Human Rights. 15:08 15:08

Can I just ask the court please to look at page six of that judgment? And you'll see that his complaint -- well, sorry, I beg your pardon, could I ask the court just, I beg your pardon, just to look at page three first, just to see how it came about that he came before the IPT? So paragraph eight at page three. He made subject access requests to MI5 and GCHQ and the object of the request was to discover whether information about him was being processed by the 15:09 15:09

agencies and to obtain access to the content of the information. And you'll see he made the access requests under the Data Protection Act, which I think is the first time in this case law we see that showing up. 15:09

"*Both requests were refused on the basis that the information requested was exempt from the disclosure requirements of the 1998 Act on the grounds of national security under certificates.*" 15:09

He then lodged two complaints with the Investigatory Powers Tribunal, the IPT. Then, Judge, asking the court to turn on to page six at paragraph 20:

"*On 17 January 2005, the IPT notified the applicant that no determination had been made in his favour in respect of his complaints. This meant either that there had been no interception or that any interception which took place was lawful.*"

You'll see then, going on, Judge, that there is a reference to, at paragraph 22:

"*Under section 28 DPA, personal data is exempt from disclosure under section 7(1) if an exemption is required for the purpose of safeguarding national security.*"

Then, Judge, if I could ask the court to turn on to page 36. And one sees a detailed discussion of the standing issue. And taking it up at paragraph 122, you'll see there:

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

Then paragraph 123:

"*In cases concerning general complaints about legislation and practice permitting secret surveillance measures, the Court has reiterated the Klass and Others approach on a number of occasions... Where actual interception was alleged, the Court has held that in order for there to be an interference, it has to be satisfied that there was a reasonable likelihood that surveillance measures were applied to the applicant... The Court will make its assessment in light of all the circumstances of the case and will not limit its review*

to the existence of direct proof that surveillance has taken place given that such proof is generally difficult or impossible to obtain.

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

So this is the test, I think I described it earlier on as somewhat involved. So in other words, this is the test applicable when an applicant is challenging, if you like, an across-the-board piece of legislation. And the question as to whether or not the person is allowed to do that before the Court of Human Rights will depend on what the availability of remedies at the national level looks like and also the risk of secret surveillance measures being applied to him. 15:12

So I don't think it's correct to say that there's, if you like, an unhindered right before the Convention to challenge any legislative measure without having to take *any* steps to show whether it might be applied to you or not or whether or not you may be able to challenge it at the national level; you have to look, the court will look both at your own particular situation and also what the likelihood is at the national level for you to challenge it. 15:13

The court then does note though that where there is no possibility of challenging the alleged application at domestic level - and I would stress the "no possibility", it's a complete elimination of a possibility of doing so - in that circumstance, the court notes that: 15:13

"*Widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court.*"

So it is, I think, on a case by case basis that the court decides whether or not a person should be entitled to bring proceedings. And one sees that even more so, I think, in the **Zakharov** case and the **Zabo** case, where the court further elaborates on its test. 15:13

In this particular case you'll see, Judge, that at paragraph 126 he said that calls were not put through to him and that he received hoax calls and this demonstrated a reasonable likelihood his communications were being intercepted. The Court disagreed that such allegations were sufficient to support the applicant's contention that his communications have been intercepted and it concluded that he had failed to demonstrate a reasonable likelihood there was actual interception in *his* case. 15:14 15:14

But then at paragraph 128, on a different basis, the court decided that he *should* be allowed to challenge. He says that under the provisions of RIPA - that was the relevant legislation: 15:14

"... *any person within the United Kingdom may have his communications intercepted if interception is deemed necessary on one or more of the grounds* [identified]*. The applicant has alleged that he is at particular risk of having his communications intercepted as a result of his high-profile murder case, in which he made allegations of police impropriety... and his subsequent campaigning against miscarriages of justice. The Court observes that neither of these reasons would appear to fall within the grounds... However, in light of the applicant's allegations that any interception is taking place without lawful basis in order to intimidate*

him... the Court considers that it cannot be excluded that secret surveillance measures were applied to him or that he was... potentially at risk of being subjected to such measures."

So he was allowed to proceed. And I'll ask the court then to go to page 51 please. Judge, there's an important passage at 166, page 51, in relation to oversight and the review of oversight under the Act and under the system. And I'll just read that long passage, because I think it is interesting in the context of the UK system of legislation just to see the level of, I suppose, detail the court goes into and also what it thinks is important in terms of oversight. So they note that: 15:15 15:15

"*As regards supervision of the RIPA regime, the Court observes that apart from the periodic review of interception warrants and materials by intercepting agencies and, where appropriate, the Secretary of State, the Interception of Communications Commissioner established under RIPA is tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. He has described his role as one of protecting members of the public from unlawful intrusion into their private lives, of assisting the intercepting agencies in their work, of ensuring that proper safeguards are in place to protect the public and of*

advising the Government and approving the safeguard documents... The Court notes that the Commissioner is independent of the executive and the legislature and is a person who holds or has held high judicial office... He reports annually to the Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes) which is laid before Parliament... In undertaking his review of surveillance practices, he has access to all relevant documents, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires".

MS. JUSTICE COSTELLO: "Closed material", I presume, that would be classified?

MS. HYLAND: I beg your pardon, Judge? 15:16

MS. JUSTICE COSTELLO: "Closed material", I presume, is classified?

MS. HYLAND: Yes, exactly. That's right. Different terminology, but the same principle.

"*The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. The Court further notes that, in practice, the Commissioner reviews, provides advice on and approves the section 15 arrangements... The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his*

biannual review of a random selection of specific cases in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself."

And so many of the aspects of the activity there of the Interception of Communications Commissioner echoes what the court has already heard in the US context. For example, if you look at the end: His biannual review of a random selection of specific cases; I think the 15:17
precise same thing was done, is done in the US context.

Then, Judge, going on to paragraph 167, the court refers to the desirability of supervisory controls to a judge, you've seen that already in **Klass**. But the 15:18
court then goes on to say:

"... *the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems*" - and the court refers to the G10 - "*any person who suspects that his communications have been or are being intercepted may apply to the IPT... The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high*

judicial office or be experienced lawyers... In undertaking its examination of complaints by individuals, the IPT has access to closed material" - the same point there, Judge - "*and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant... In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid... The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom.*"

Judge, there is, I think, a parallel to be drawn between that and the Ombudsman, or the Ombudsperson in the Privacy Shield context. Because the Ombudsperson again is independent, independent of the Intelligence Community, it is the Under Secretary, it is entitled when receiving a complaint to go to other bodies, including, I think, PCLOB and the inspectors, who have access to classified information, who must give it assistance and there is no requirement for the complainant to the Ombudsman to prove or to establish that they have been the subject of interception or surveillance. 15:19 15:19

So it's a very similar type approach. Rather than putting a notification requirement in place, which the court has seen in **Klass** may be some many years after the event when it is eventually safe, considered safe to notify people - so there is inherent limitations, if you like, on the notification itself given the subject matter; on the other hand, there is, if you like, a closed procedure which the applicant or the complainant doesn't have access into the workings of, but on the other hand doesn't require to show that they have been the subject of the surveillance and, by making a complaint, sets in train a process which allows an investigation done which safeguards the secrecy of the information, but nonetheless, I suppose, permits a control or a view of what has taken place. 15:20

So there are different ways to approach this issue, but it's interesting to see that the court in this case were satisfied with the method of control by the IPT. 15:21

And if one goes on, you'll see at paragraph 168 the court observes the reports of the Commissioner scrutinise any errors which have occurred in the operation of the legislation. And I drew your attention to the fact that that, in the US context, also takes place. 15:21

"*In his 2007 report, the Commissioner commented that none of the breaches or errors identified were*

deliberate and that, where interception had, as a consequence of human or technical error, unlawfully taken place, any intercept material was destroyed as soon as the error was discovered... There is therefore no evidence that any deliberate abuse of interception powers is taking place."

And you'll see there then that the court goes on to say:

"... *domestic law on interception... together with the clarifications brought by the publication of the Code indicate... the procedures... The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors... Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures... are justified under 8(2).*"

And there was no violation. Then just turning to 58, just to close off the article -- oh, sorry, before I deal with Article 13, can I just identify something of interest in the context of Article 6? Now, Article 6 is

not something that this court is concerned with, it's the right to a fair trial and I don't believe it's been part of this case at all. But when the court was looking at *that* alleged breach in this context, I think there is something of interest. 15:22

At page 58 you will see there - and it's a little bit like the suppression remedy in Article 1806 that the court heard so much about - asking the court to take it up please at paragraph 187, which is just at the bottom 15:22 of page 57.

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: You'll see the court says:

"... *the Court recalls that the entitlement to disclosure of relevant evidence is not an absolute right. The interests of national security or the need to keep secret methods of investigation of crime must be weighed against the general right to adversarial proceedings... The Court notes that the prohibition on disclosure set out in Rule 6(2) admits of exceptions, set out in Rules 6(3) and (4). Accordingly, the prohibition is not an absolute one. The Court further observes that documents submitted to the IPT in respect of a specific complaint, as well as details of any witnesses who have provided evidence, are likely to be highly sensitive, particularly when viewed in light of the Government's 'neither confirm nor deny' policy. The Court agrees with the Government that, in the*

circumstances, it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place. It is also relevant that where the IPT finds in the applicant's favour, it can exercise its discretion to disclose such documents and information under Rule 6(4)."

And it *is* interesting there that the special advocates were held *not* to be possible to appoint. In fact, as you've seen in the US context, now in the US there *is* special advocates being appointed before the FISC. 15:23

Then just finishing off, Judge, the last page, page 60, you'll see there that there's a reference to Article 6 and there's -- I beg your pardon, Article 13. And there's no separate identification of breach of Article 13. 15:24

Then the last two cases, Judge, cases of **Zakharov** and **Zabo**. This was a Russian and a Hungarian case respectively. And if I could just ask the court to look at tab 45? This was a Russian lawyer who was challenging the -- I beg your pardon, he was not a Russian lawyer, I think he was in fact, he was a journalist in fact, I beg your pardon, he was being represented by an NGO. But if I can ask the court just to turn to page two, you'll see there was the 15:24

editor-in-chief of a publishing company and of an aviation magazine and he was chairperson of Glasnost Defence Foundation, an NGO monitoring the state of media freedom in the Russian regions which promotes the independence of the regional mass media.

Interestingly, Judge, his initial challenge was against mobile network operators, not the government as such. You'll see paragraph 10:

"... *he brought judicial proceeding against three mobile network operators, claiming that there had been an interference with his right to the privacy of his telephone communications. He claimed that pursuant to Order no. 70... the mobile network operators had installed equipment which permitted the... the FSB to intercept all telephone communications without prior judicial authorisation. The applicant argued that Order no. 70, which had never been published, unduly restricted his right to privacy.*"

And he sought an injunction. And I wonder can I ask the court please to go then to paragraph one hundred and -- no, sorry, that's not the one. Could I ask the court to look at page 24? And the paragraph number is paragraph 118. And you'll see there a description of the type of interception, two types of interception - total interception and statistical monitoring:

15:25

"*Total interception is the real-time interception of communications data and of the contents of all communications to or by the interception subject. Statistical monitoring is real-time monitoring of communications data only, with no interception of the content of communications. Communications data include the telephone number called, the start and end times... supplementary services used, location of the interception subject and his or her connection status.*"

And the court will be very familiar with that, the difference between content-based interception and, if you like, meta-data, which is something the court has seen again already in the US context.

15:26

Then if I could ask the court to move on please to paragraph 147. And I'm just showing the court there that there's a reference by the court to the **Digital Rights** decision. Then I don't think I need to open that, the court is familiar with that, but just to show 15:26 that the court is looking at **Digital Rights** there.

Then moving on to paragraph 167. And we're back then to the standing point. And the court has already looked at the dicta in **Klass** and in **Kennedy**. 15:27

Can I ask the court to look at paragraph 171? And you'll see there the court says:

"*In the Court's view the Kennedy approach is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the Court.*"

Then the court repeats its analysis in **Kennedy**. And then at the bottom of the page, paragraph 172:

"*The Kennedy approach therefore provides the Court with the requisite degree of flexibility to deal with a variety of situations which might arise in the context of secret surveillance, taking into account the particularities of the legal systems in the member States, namely the available remedies, as well as the different personal situations of applicants.*"

Then, Judge, if I could ask the court to go on to page 57? And you'll see at paragraph 231 the court identifies that: 15:27

"*In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: The nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping;*

the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed."

Then, Judge, turning on to page 62, a curiosity in this case. Because ultimately the court found that the Russian system was very deficient and was *not* in compliance with Article 8(2). But at paragraph 249 there *was* in fact a *judicial* authorisation system for warrants, which again I think shows the importance of not taking any particular aspect of the scheme out of context. Because you might've said, or you might've expected that where you had judicial authorisation, the court has already said in **Klass** it's desirable but not required and that, therefore, judicial authorisation would tick the box, as it were, because in Russia that *was* a requirement. But in fact the court went on to look at the practice in Russia and it became clear that in fact the judicial authorisation was *not* sufficient, because the judges were not sufficiently independent and did not have the information they needed to *make* the decision, so it was effectively a tick-box exercise. So that was as a result of the court looking in some considerable detail at the practice in Russia, as well as the actual legislative requirements. 15:28 15:29 15:29 15:29

Judge, can I then ask the court to move on please to

page 256 -- I beg your pardon, paragraph 256? Paragraph 256 identifies some of the concerns that the court has. You'll see there that the court noted a concern that:

"*Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial... Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point.*"

I think I can also just tell the court that at paragraph 255 the court was concerned there was no obligation to destroy irrelevant data and, at paragraph 252, there was no indication as to when measures were to be discontinued. And these were causes for concern.

15:30

Paragraph 265; the courts had concerns because there was no limitations on the authorisation measures. If I could ask the court just to look at paragraph 265, halfway down the paragraph:

15:30

"... *the OSAA does not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation... courts sometimes grant... authorisations which do not mention a specific person*

or telephone number to be tapped, but authorise interception of all... communications in the area where a criminal offence has been committed. [They] *do not mention the duration... such authorisations, which are not clearly prohibited... grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long.*"

Then, Judge, at paragraph 275 the court repeated its point about non-judicial bodies being acceptable, but as long as they were sufficiently independent and had sufficient powers and competence. 15:31

The court then went on at paragraph 279 to express concern about Russian prosecutors who supervised interceptions. But you'll see there at 279 the court noted that: 15:31

"... *in Russia prosecutors are appointed and dismissed by the Prosecutor General after consultation... This fact may raise doubts as to their independence from the executive.*"

Then paragraph 284; the court noted that it was for the government to show the practical effectiveness of supervision arrangements. And again this goes to practice, as opposed to law, or as opposed to legislation. Paragraph 284: 15:32

"... *it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples... However, the Russian Government did not submit any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach of law. It follows that the Government did not demonstrate that prosecutors' supervision of secret surveillance measures is effective in practice. The Court also takes note in this connection of the documents submitted... illustrating prosecutors' inability to obtain access to classified materials relating to interceptions...* [This] *raises doubts as to the effectiveness of supervision by prosecutors in practice.*"

And just thinking about that supervision and contrasting it, I suppose, with the **Bates** opinion that the court saw in the FISC context whereby the court had to consider the authorisation applications and the court itself in 2011 on two occasions refused certain applications for authorisations and sent them back and saying they would not authorise the particular authorisations in question. 15:33

15:33

So none of this is -- as I say, it's impossible to make absolute comparisons, but I think one can clearly see here that there is undoubtedly, in the court's view, a manifest deficit in the whole of the Russian regime and

in particular the control, what we're looking at here, the supervision arrangements and the prosecutors' ability to access classified material, that's obviously a very important point.

15:33

Then, Judge, you'll see in relation to notification, paragraph 287, there is a point about **Klass** and I think there's a quote from **Klass** that the court has already seen in relation to the difficulties of notification and how it may be many, many years before one can actually be notified. 15:33

Then at paragraph 288 the court indicates that in certain circumstances though the absence of a requirement to notify may cause a breach of 8(2). And one sees in all of these cases there are no per se rules, the court always looks at the totality of the circumstances. So at paragraph 288 there's quotations from the various cases that the court has already seen and about two-thirds of the way down the paragraph there's a reference to a case the court hasn't seen -- I'm sorry, about halfway down the paragraph, reference to a case the court hasn't seen, **Association For European Integration on Human Rights** and **Popescu**: 15:34 15:34

"... *the Court found that the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek*

redress for unlawful interferences with his or her Article 8 rights and rendered the remedies... [illusory and theoretical]... *The national law thus eschewed an important safeguard against the improper use of special means of surveillance... By contrast, in the case of Kennedy*" - and that's a case the court *has* looked at - "*the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications.*"

The court then, at paragraph 289:

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

The court then went on to note that there *was* an

entitlement to seek information, but noted that in order to lodge such a request, you had to be in possession of the facts of the search measures. So again that was conditional on the person's ability to prove his or her communications were intercepted. 15:36

At paragraph 291 the court says:

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

Then there is a reference at paragraph 292 to a hierarchical appeal to a direct supervisor did not meet the requisite standards of independence. And at paragraph 293, the Russian government put forward some other judicial procedures, the court went through them. But ultimately the court decided that at paragraph 300: 15:36 15:36

"... *the Court finds that Russian law does not provide for effective remedies to a person who suspects that he or she has been subjected to secret surveillance. By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschews an important safeguard against the improper use of secret surveillance measures.*"

In those circumstances, in *all* of the circumstances, all of the various different points that the court has already looked at, some of which I've identified to you, the court found that there was a violation of Article 8. They didn't, the court didn't go on to identify a separate violation of Article 13, having regard to its findings on remedies at 286 to 300 that I've identified to the court. 15:37

Can I just ask then the court finally to look at **Zabo**? And that's at tab 46. **Zabo**, I suppose, is of particular interest because it refers to the Venice Commission. And I think the court has heard once about the Venice Commission report on surveillance by Prof. Swire - it's a 2007 report. And the Venice Commission is a body of the Council of Europe and it, I think, has been set up to promote democracy, particularly -- I think it was originally set up to promote democracy in former communist countries and it carries out research and studies and makes recommendations. And it has, as I say, done a 2007 report. And there are important extracts from that report in the case of **Zabo** which I'm going to just ask the court to look at. 15:37 15:38 15:38

But just to deal with the facts in **Zabo**. There were two Hungarians. They were a member of an NGO which voiced criticism of the government - and again I think

it's striking how much the cases and the people who are taking these cases mirror what the court has already seen in the US context, the ACLU, Amnesty, Privacy, all of these different bodies, the NGOs seeking to identify challenges to surveillance measures. And one sees it on both sides of the Atlantic. 15:38

If I could ask the court then to look first then at the summary on the Venice Commission, and that may be found at paragraph 21 of the judgment, which is in fact to be found at page 15. Judge, you'll see there at paragraph 21 "*The Report on the Democratic oversight of the Security Services adopted by the Venice Commission*" and it contains the following passages. And there's a reference at paragraphs 81 and 82 to national security policy. 15:38 15:39

Then at paragraph 130, "*Internal and Governmental Controls as part of overall accountability systems.*" and this is very important, in my submission, how the Venice Commission characterise the primary guarantee against abuse of power, not litigation, not remedies by individuals, but rather, at paragraph 130: 15:39

"*Internal control of security services is the primary guarantee against abuses of power, when the staff working in the agencies are committed to the democratic values of the State and to respecting human rights. External controls are essentially to buttress the*

internal controls and periodically ensure these are working properly."

Then moving on, Judge, to Parliamentary accountability:

"*There are several reasons why parliamentarians should be involved in the oversight of security agencies. Firstly, the ultimate authority... of security agencies is derived from legislative approval of their powers, operations and expenditure. Secondly, there is a risk that the agencies may serve narrow political or sectional interests, rather than the State as a whole... if democratic scrutiny does not extend to them.*"

Then paragraph 153:

"... *the most frequent arrangement is for parliament to establish a single oversight body for all the major security and intelligence agencies, rather than having multiple oversight bodies.*"

Then the next heading, "Judicial Review and Authorisation":

"*195. Judicial control over internal security services can take different forms. First, there is prior authorisation... and/or post hoc review, of special investigative measures, such as telephone tapping,*

bugging and video surveillance. This is the normal practice in European States."

Then "Accountability to Expert Bodies"; they can serve either as a supplement or replacement for parliamentary bodies or judicial accountability and the Venice Commission then weighs up the pros and cons of having this type of expert body. 15:40

Then under the heading "Complaints Mechanisms": 15:41

"... *it is necessary for individuals who claim to have been adversely affected by the exceptional powers of security and intelligence agencies, such as surveillance or security clearance, to have some avenue for redress. Quite apart from strengthening accountability, complaints may also help to lead to improved performance by the agencies through highlighting administrative failings. The requirements of human rights treaties, and especially the European Convention... with its protections of fair trial, respect for private life and the requirement of an effective remedy must obviously also be borne in mind.*"

Then, Judge, paragraph 242: 15:41

"*Plainly, though, legitimate targets of a security or intelligence agency should not be able to use a complaints system to find out about the agency's work.*

A complaints system should balance, on the one hand, independence, robustness and fairness, and, on the other hand, sensitivity to security needs. Designing such a system is difficult but not impossible."

So again -- well, I'll go on to finish and then I'll comment on that. Paragraph 243:

"*Individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts. As already mentioned, for a variety of reasons, the capacity of the ordinary courts to serve as an adequate remedy in security fields is limited. The case law of the European Court of Human Rights ... makes it very clear that a remedy must not simply be on paper.*"

Judge, in our submission, that is terribly important. It's an inescapable fact that the capacity of the ordinary courts to serve as an adequate remedy in this field is limited. And that cannot be ignored. And we say that overwhelmingly obvious fact was ignored by the DPC, and that rendered her draft decision hugely problematic, because she didn't engage with the subject matter. 15:42

Paragraph 244:

"*An alternative is to allow an investigation and report into a complaint against an agency by an independent official, such as an ombudsman...*

245. In these ombudsman-type systems, the emphasis is on an independent official investigating on behalf of the complainant. These independent offices usually exist to deal with an administrative failure by public bodies, rather than a legal error. Their investigations may give less emphasis to the complainant's own participation in the process and to transparency than would be the case with legal proceedings. Typically an investigation of this type will conclude not with a judgment and formal remedies, but with a report, and (if the complaint is upheld) a recommendation for putting matters right and future action...

246. A less common variation is for a State to use a parliamentary or expert oversight body to deal with complaints and grievances of individuals... There may be a benefit for a parliamentary oversight body in handling complaints brought against security and intelligence agencies since this will give an insight into potential failures of policy, legality and efficiency. On the other hand, if the oversight body is too closely identified with the agencies it oversees

or operates within the ring of secrecy, the complainant may feel that the complaints process is insufficiently independent. In cases where a single body handles complaints and oversight it is best if there are quite distinct legal procedures for these different roles."

Then just turning on to the conclusion of **Zabo**, because I'm conscious of time, Judge, and if I could ask the court to look please at paragraph 86. And you'll see there, Judge, that there is a question of remedies and notification - again we come back to the same point. At paragraph 86, you'll see at the bottom of paragraph 86 there's a reference to **Weber** and **Zakharov** and then there's a point taken that in Hungarian law: 15:44

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

So in that case the *absence* of notification, *along* with the absence of formal remedies in case of abuse indicated that the legislation fell short. 15:44

Paragraph 88:

"... *the Court notes that is for the Government to illustrate the practical effectiveness of the*

supervision arrangements with appropriate examples... However, the Government were not able to do so in the instant case.

89. In total sum, the Court is not convinced that the Hungarian legislation on 'section 7/E(3) surveillance' provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures."

And I've just brought the court to the end, but there is other flaws in the legislation that have been identified. And, Judge, ultimately the court held that there *was* a breach of 8(2).

15:45

Now, Judge, in the time that we have left, I wonder can I ask the court to start looking at the FRA report? And I know the court has heard a great deal about it and I think there may be time to let the court actually look at it. And it may be found, Judge, in book - sorry, I just want to make sure I have the right book, because... 15:45

MS. JUSTICE COSTELLO: Well, the tab will help.

MS. HYLAND: The tab will help, exactly. It's exhibited to the affidavit of Jeffrey Robertson. 15:46

MR. GALLAGHER: 61.

MS. HYLAND: Tab 61, yes. Judge, I'm sorry, there's another -- it can be found, certainly in my book, Judge, at tab 11. So this is the early books of the

affidavits and it's Jeffrey Robertson.

MS. JUSTICE COSTELLO: Well, if this is the "Surveillance By Intelligence Services: Fundamental Safeguards and Remedies in the EU", I have that. Thanks. 15:46

MS. HYLAND: Exactly. That's right, exactly, Judge. Just before I open it, can I just identify for the court please who the FRA are and the legal basis pursuant to which they were set up? And I'm just going to hand in to the court the regulation whereby they were set up in 2007 (Same Handed). And I don't need to detain the court on this, but I think it's just to show the court, as I already mentioned, that they are an official body of the European Union. 15:46 15:47

You'll see that it was a Council Regulation that set them up on 15th February 2007. And just turning to page four of that document, you'll see that the objective is set out at Article 2. And the objective is to provide the relevant institutions, bodies, offices and agencies of the Community and its Member States, when implementing Community law, with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights. 15:47 15:47

So that is what they are charged with doing. And the

council determines a multi-annual framework for the FRA in five-year increments. And this increment is 2013 to 2017. And the respect for private life and protection of personal data was selected as one of the thematic areas, which I suppose is fortunate for us in this particular context. 15:48

There's a number of different activities they're tasked with; they're tasked with collecting, analysing and disseminating reliable and comparable information and data, they're tasked with formulating and publishing conclusions on particular topics and also with raising public awareness of fundamental rights. 15:48

If I could just ask the court then to look at the introduction to this report and just to see the context in which the report was done. And as I said, they had been specifically asked to do so by the European Parliament following the Snowden disclosures. And just looking at the foreword, you'll see that it's the first part of the FRA's response to the European Parliament request. It was the subject of -- you'll see in the third paragraph: 15:48 15:48

"*The European Parliament responded with a resolution which... calls on the* [FRA] *to research thoroughly fundamental rights protection in the context of surveillance, in particular in terms of available remedies.*"

And this report is the first part. It aims to support the adoption and meaningful implementation of oversight mechanisms in the EU and its Member States. And again those words "oversight mechanisms", immediately we see them jumping out. 15:49

"*It does so by analysing the legal frameworks on surveillance in place in EU Member States, focusing on so-called 'mass surveillance', which carries a particularly high potential for abuse. The report does not assess the implementation of the respective laws; instead, it maps the relevant legal frameworks in the Member States. It also details oversight mechanisms... outlines the work of entities... and presents the various remedies available to individuals.*"

The next page, Judge, is the country codes. It just shows that each of the 28 Member States has been the subject of the investigation. And then the introduction - I think I've already identified to you the context in which the request was made. 15:49

Then turning over the page -- Judge, the page numbers, by the way, are at the bottom of the page, variously the left-hand side and the right-hand side. Rather unfortunately, they're in a kind of a coloured band which makes it a bit hard to see then, but I hope the court can see them. 15:50

Then, Judge, if I could ask the court to turn on please to page nine. And you'll see there that there's a reference to the European Court of Human Rights on the right-hand side, on the right hand column. And there's a reference to what you've already looked at, Article 8 and Article 13. 15:50

Then turning over the page, at page ten there's a reference to European Union law and there's a reference on the left-hand column to the Data Protection Directive, the E-Privacy Directive and the Framework Decision, all of which I think the court's attention has been drawn. And you'll see there that, at the bottom of that column: 15:50 15:51

"*According to Article 52 (1) of the Charter, any limitation to this right must be necessary and proportionate, genuinely meet objectives of general interest recognised by the Union, be provided by law, and respect the essence of such rights.*"

Then on the right-hand column they deal with the national security exemption. And you'll see there it's stated: 15:51

"*Applicability of these instruments*" - and they're the instruments that have just been mentioned - "*in the field of security is, however, subject to the specific*

legal and policy framework in the area and particularly to the national security exemption. Article 4(2) of the TEU provides that 'national security remains the sole responsibility of each EU Member State'. This exemption is reiterated both in Article 3(2) of the Data Protection Directive and in Article 1(4) of Framework Decision... which excludes 'essential national security interests and specific intelligence activities in the field of national security' from the rules applicable to 'regular' law enforcement action."

Judge, just in respect of that Framework Decision, in 2018, on the same date, I think, as the GDPR is coming into effect, that will become the Law Enforcement Directive. Because as the court knows, criminal law -- 15:52
that deals with criminal law and surveillance in the criminal law context. It was in the form of a Framework Decision because it was outside the four walls of the EU. Its now, criminal law has now been brought in and that's why it's now possible to make 15:52
that a Law Enforcement Directive, as opposed to being a Framework Decision, which it previously was. And that goes to the point that Mr. Gallagher made yesterday whereby criminal law has now moved from being outside the tent, as it were, to within the tent. And that's 15:52
not the case with national security.

"*The limits of the national security exemption are subject to debate, including in relation to the*

activities of intelligence services. Although international guidelines exist, there is no uniform understanding of 'national security' across the EU. The concept is not further defined in EU legislation or in CJEU case law, although the CJEU has stated that exceptions to fundamental rights must be interpreted narrowly and justified...

The lack of clarity on the precise scope of the national security exemption goes hand in hand with the varied and seldom clearly drawn line between the areas of law enforcement and national security in individual Member States. This is particularly true with counter-terrorism."

Then the court goes on -- the FRA goes on in the last paragraph:

"*It falls outside the scope of this report to analyse in great detail the extent of EU competence in this field. However, the current situation is relevant not only to surveillance and the rights of privacy and personal data protection, but also to efforts at the EU level in the area of internal security, in accordance with Article 4(2)(j) of the TFEU, which defines the area of freedom, security and justice as an area of shared competences between the EU and the Member States.*"

Then, Judge, at the bottom of the column on the next page:

"*This unclear delineation of 'national security' also has repercussions for the applicability of EU law, which depends both on the interpretation of the national security exemption's scope and on the specific characteristics of the various surveillance programmes carried out by intelligence services. Although the existence of such programmes remains largely unknown, even in light of the Snowden revelations, some contain elements that can justify the full applicability of EU law. For instance, when EU companies transfer data to intelligence services, including those of third countries, they are considered under the Data Protection Directive as data controllers who collect and process data for their own commercial purposes. Any subsequent data processing activities, such as the transfer of personal data to intelligence services for the purpose of the protection of national security, will therefore fall within the scope of EU law. Any limitations of the rights to privacy and personal data protection should be examined according to Article 13 of the Data Protection Directive and Article 15 of the e-Privacy Directive, as well as Article 52(1) of the Charter.*"

Judge, then:

"*The essence of the right to privacy and protection of personal data shall at any rate be respected. The 'national security' exception thus cannot be seen as entirely excluding the applicability of EU law. As the UK Independent Reviewer of Terrorism Legislation recently put it*" - Judge, that's David Anderson, whose report I'll be coming to briefly tomorrow - "'*National security remains the sole responsibility of each Member State: But subject to that, any UK legislation governing interception or communications data is likely to have to comply with the EU Charter because it would constitute a derogation from the EU directives in the field*'."

Then, Judge, in relation to methodology - I think this is particularly important - you'll see it was done through desk research in all 28 EU Member States based on a questionnaire submitted to the network. 15:55

"*Additional information was gathered through desk research and exchanges with key partners, including a number of FRA's national liaison officers in the Member States and individual experts.*"

Then there's an identification of the individual experts. Can I ask the court then to turn to page 15 please? And we'll see there that there's some descriptions of surveillance measures. And one of the particularly helpful things about this report is that 15:55

there are diagrams, and I think that is perhaps a useful way to understand some of the concepts.

But can I just ask you, before looking at the diagram, just at the bottom of page 15, a very important point that I think possibly has not been stressed sufficiently: 15:55

"*For intelligence services, one of the key challenges of collection is the quantity of data available. As Lowenthal puts it, '[A]s of 2013, there are some 7 billion telephones worldwide [...] generating some 12.4 billion calls every day. Newer communications channels add to the total. In the United States alone, 2.2 trillion text messages were sent in 2012, as well as 400 million tweets...' This requires important budgetary investments that not all countries can afford. Cousseran and Hayez identify the following EU countries as having services with important capacities that can afford SIGINT collection: The UK (5,500 staff working at GCHQ), France (2,100 staff working at the Directorate General of External Security... and 700 staff working at the Directorate of Military Intelligence... Germany (1,000 staff working at the BND) and Sweden... Brown et al. Add the Netherlands, Italy and Spain to the list of Member States performing SIGINT. The US National Research Council's analysis shows that SIGINT requires discriminants (or selectors) to make it possible to filter the data before its*

storage, and further analysis by the intelligence services... Figure 1 illustrates this process."

And there's a helpful diagram, I think, Judge, which identifies there that there's the signal extract, filter, discriminant, store, query, analyse and disseminate. So it's, if you like, an iterative process, it's not simply one set of search terms, it is continually being reduced downwards to make it manageable. 15:57

Then, Judge, can I ask you to go please to page 20? And page 20 differentiates between what the court is now well familiar with, targeted surveillance and signals intelligence. Different terms are used, I suppose, in different reports by different agencies in different jurisdictions, but the format that's used here is, targeted surveillance is identified here as the targeting of a particular individual, I think that is what they are intending to mean by that. If the court just looks there at the second paragraph headed "Targeted Surveillance": 15:57

"*Targeted surveillance as regulated in the Member States' laws refers to concrete targets upon suspicion that an act falling within the remit of the intelligence services' tasks could be committed before a surveillance measure can be initiated. In several Member States, such targets may either be a group of*

people (defined through their relation to an organisation or a legal person) or an individual."

Then turning to 1.3.1.2, "Signals Intelligence":

"*FRA's analysis of the legal frameworks that regulate surveillance methods used by intelligence services shows that five Member States (France, Germany, the Netherlands, Sweden and the United Kingdom) detail the conditions that permit the use of both targeted surveillance and signals intelligence. This report focuses on these five Member States due to the existence of <u>detailed</u> legislation on SIGINT. This does not mean that this list is in any way exhaustive. FRA's selection is based on the fact that this type of collection is prescribed, in detail, in the law.*

Three examples illustrate where the accessible law of a Member State provides insufficient details to allow for a legal analysis of the exact procedure in place on how signals intelligence is collected."

And there's then an identification of Italy, some of the SIGINT activities in Germany and in France, the French bill. So it's clear that the analysis is being done where the FRA can do it, where there is sufficiently clear legislative provisions in relation to the collection of signals intelligence. But they are clearly identifying that that is not necessarily

15:59

the case in all of the Member States and that there may be situations where they -- sorry, they're saying there *are* situations where they simply are not in a position to carry out that analysis. And that is, of course, hugely important. That goes to the very first of the conditions you looked at under the Convention - in accordance with law. In other words, it's something identifiable in law so a person can actually identify its existence and know of its provisions. And the FRA is identifying there that that's not the case in certain Member States. 15:59 16:00

Judge, I'm conscious that it's just coming up to four o'clock and...

MS. JUSTICE COSTELLO: Yes. Well, perhaps we'll take it up tomorrow then. 16:00

MS. HYLAND: Very good. Thank you.

THE HEARING WAS THEN ADJOURNED UNTIL THURSDAY, 9TH MARCH AT 11:00 16:00

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z