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 THURSDAY, 9th MARCH 2017 - DAY 18

18

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 THURSDAY, 9TH MARCH 2017

MS. JUSTICE COSTELLO: Good morning.

REGISTRAR: At hearing, Data Protection Commissioner -v- Facebook. 11:05

SUBMISSION BY MS. HYLAND:

MS. HYLAND: Good morning, Judge. Judge, I think yesterday I was just, I had just finished at the FRA Report, so if I could ask the court please to take it up again, and the court will recall that it's to be found in Tab 11 of book, well -- 11:05

MS. JUSTICE COSTELLO: Oh, I'm using Tab 61.

MS. HYLAND: You're using it at a different place, I see, Judge, yes. It's the same document in any case that we were at yesterday. And, Judge, I think I had been on page 21.

MS. JUSTICE COSTELLO: Yes. 11:06

MS. HYLAND: And I think in fact, Mr. Gallagher had just reminded me that there was a passage that was important just in relation to the German activities, and I wonder could I just open that. So looking at page 21 on the left-hand column, this is in respect of the SIGINT activities. 11:06

And you may remember where we had left it off was the extent to which Member States provide for legislation

in respect of the signals intelligence as opposed to, if you like, the old fashioned targeted surveillance. The point that had been identified was that some Member States do not in their legislation have specific provisions dealing with signals intelligence or only have it in part. 11:06

There had been an identification of *five* Member States where there were legal frameworks in place regulating signals intelligence and Germany was identified as one of them. But in fact when one looks in a bit more detail one sees that Germany, there is some, I think, detail about the way in which it is regulated and I'm just going to look at that. 11:06

11:07

The paragraph on the left-hand side: "*Similarly, in Germany, some of the SIGINT activities that the Federal Intelligence Service may undertake is not regulated in detail by law, unlike other SIGINT activities in Germany. The Federal Intelligence Act states that the BND 'shall collect and analyse information required for obtaining foreign intelligence, which is of importance for the foreign and security policy of the Federal Republic of Germany' and that it 'may collect, process and use the required information, including personal data'. This definition of the BND's competences provides the legal basis for the German intelligence service to perform SIGINT activities abroad between two foreign countries or within one single foreign country,*

provided that the intercepted signals have no connection - besides the actual data processing - with Germany. This SIGINT activity is referred to as 'open sky' and according to various commentators takes place outside any legal framework. So far however, no judicial decision, either in Germany or by the ECHR has confirmed this assessment. This surveillance method does not fall within the scope of the Act on Restricting the Privacy of Correspondence, Posts and Telecommunication (G10 Act)." 11:07

And you will remember, Judge, from yesterday G10 is still there.

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: "*Which was adopted in application of Article 10(2) of the Basic Law to lay down the specific conditions to restricting privacy of communications. Consequently, this surveillance method is outside the G10 Commission's remit (the expert body in charge of overseeing the intelligence services). The Parliamentary Control Panel is the sole body that oversees this surveillance method. The absence of tight control has triggered calls for reform, and the matter is being discussed before the NSA Committee of Inquiry.*" And I think that's a different NSA. 11:08

And, Judge, then can I ask the court please to go on to page 24. And at page 24, Judge, you'll see that there is a summary then of the various different legal

systems that have been considered. And on the left-hand side column, the second full paragraph down:

"*In sum, despite legislative efforts to regulate the work of intelligence services, the Council of Europe Commissioner for Human Rights recently concluded that 'in many countries, there are few clear, published laws regulating the work of these agencies'. The lack of clarity and hence necessary quality of the legal rules governing the work of intelligence services raises fundamental rights issues. It has furthermore triggered lawsuits in a number of Member States. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, stated that bulk access to communications and content data without prior suspicion 'amounts to a systematic interference with the right to respect for privacy of communications, and requires a corresponding compelling jurisdiction'.*

11:09

Though it is too early to assess the full impact of the Snowden revelations on legal reforms, post-Snowden inquiries in some Member States indeed led to the conclusion that their current national legal frameworks need to be reformed. The annual report of the French Parliamentary Delegation on intelligence, the parliamentary oversight body, linked its assessment of the revelations to the need for overarching intelligence reform in France. In the United Kingdom,

11:09

the post-Snowden inquiry by the Intelligence Security Committee also resulted in the conclusion that the British legal framework is deserving of reform. This was supported by a report issued by the independent Reviewer of Terrorism Legislation." 11:09

And he criticises there the regulation of Investigatory Powers Act.

Judge, can I just make a comment. Yesterday I talked about the requirement in accordance with law under the Convention and I said that in most of the cases that we were looking at yesterday that was not an issue because there was legislation in being and it was whether it was necessary in a democratic society test that the court was looking at. But in fact what's being talked about here is the provision *necessary in accordance with law*, where there aren't actually any legal frameworks governing the access at all, then that very first condition will not be met. 11:10 11:10

And then, Judge, the heading *"Surveillance following a legitimate aim"* and there's a reference there to the Convention case law, and the court has looked at some of them. 11:10

Then, Judge, just one discrete point on page 25, you will remember there was some discussion between yourself and Mr. Gallagher as to *state security* and

national security and the relationship between those two terms, and you will see that this report does identify a view on that. And the second column, the second last paragraph, starting with the words *"in some EU secondary legislation"*, this is the next page, 25. 11:11

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: "'*National security' is explained as state security, for instance in Article 15(1) of the e-Privacy Directive. Moreover, the CJEU in* ***ZZ*** *implicitly held that the notion of state security as used in EU secondary legislation is equivalent to the notion of 'national security' as used in the national law."* 11:11

Then, Judge, can I ask the court to go on please to page 29. 29 is a new chapter dealing with the oversight of intelligence services. And oversight, I have already addressed the court on this, and you'll see there that the chapter, the very first paragraph, the chapter outlines how oversight mechanisms are established in the EU Member States. It looks at the accountability mechanisms imposed by law on the intelligence services. 11:11

Then on the following column you'll see there: 11:11

"*The general consensus taking from the Venice Commission report and academic studies, is that oversight should be a combination of: Executive*

control; parliamentary oversight; judicial review; and expert bodies.

Judicial review, which mainly occurs as a result of a lawsuit, is covered under Chapter 3 of this report. 11:12
Judicial involvement in oversight of intelligence services occurs via warranting and monitoring of surveillance measures. However, since these bodies are not exclusively judicial, the broader category of approval and review of surveillance measures has been 11:12
used in this report. The role of the ombudspersons in the oversight of intelligence services is covered in Chapter 3, since it is mainly a complaints-handling body."

11:12

Then, next line: "*By giving diverse powers to an array of bodies that should complement each other, the maximum level of oversight is guaranteed. Their oversight, however, is only effective if they are independent and granted sufficient powers and* 11:12
resources, both human and financial, to fulfil their mandate."

And then there's a reference to the UN.

11:12

And then, Judge, something that Prof. Swire said in the American context is echoed here at the bottom of that left-hand column. You'll see the wording:

"*To achieve the maximum level of protection, in addition to the four layers of legally-based oversight mentioned above, the media and civil society organisations also play an important role.*"

11:13

And that's something that was identified by Prof. Swire in the US context. And the report observes that: "*NGOs have launched lawsuits in various EU Member States, promoted reforms, developed international principles and act as watchdogs.*" 11:13

And then, Judge, you'll see that there's, on the second column, the third paragraph down: "*Control of the services, however, cannot be limited to external authorities. Intelligence services have a clear* 11:13 *responsibility to act within the law, and the law itself can state such a responsibility. Though not strictly 'oversight', since that implies a certain measure of independence, internal control can be achieved by establishing a clear set of internal* 11:13 *administrative policies that guide staff.*"

And then, Judge, turning over the page, you will see a diagram which identifies what we have just been talking about here in relation to control and the various 11:13 bodies that play a part in the control of intelligence services.

And then, Judge, can I ask the court please to go to

page 42, although that chapter is important time is short and I want to move on in particular to Chapter 3.

But, first, Judge, can I ask the court to look at page 42 because it does identify in a table form -- 11:14

MS. JUSTICE COSTELLO: Hmm.

MS. HYLAND: -- the relevant expert bodies in the various EU Member States. And you'll see there that in the Irish context, about half way down, the relevant oversight or expert body is the Complaints Referee and 11:14 designated judge of the High Court, and I'll come to that when I'm looking briefly at the Irish situation.

And in the UK, Judge, at the bottom of the page, you'll see there is three bodies identified: The Intelligence 11:14 Services Commissioner, the Interception of Communications Commissioner and the Investigatory Powers Tribunal. I suppose it is also relevant, Judge, that there are some countries, some Member States, that it appears to be not applicable, but certainly they 11:14 don't have relevant expert bodies and that does appear to be a gap having regard to what has already been said about the necessity for same.

Can I ask the court then to go on please to page 47 and 11:15 this is important I think in the context of data protection authorities, because obviously this is of relevance, the extent to which data protection authorities have a role in this field. And perhaps

I should ask the court just to look back one page to 48 - sorry 46 - where the subject is taken up under the heading *"data protection authorities"*. And you will see that it is stated that:

11:15

"*Data protection authorities also constitute expert bodies in the context of oversight. They play a fundamental right in safeguarding the right to the protection of personal data.*"

11:15

And there is a reference there to the EU primary and secondary law and then in particular the Data Protection Directive.

And then --

11:15

MS. JUSTICE COSTELLO: Sorry, this is in the context, it's not just national securities surveillance?

MS. HYLAND: Exactly. Exactly, Judge. Because in fact, if one goes on, you will see they are just talking generally at this point and then we start honing in on the national security sphere. Because on the next page, left-hand column, second last paragraph:

11:15

"*FRA findings show that, compared to other fields of data processing activities and other data controllers of the public and private sector, DPAs in most Member States have no competences over national intelligence services, or their powers are limited. As highlighted earlier, both the Data Protection Directive and the*

11:16

e-Privacy Directive are subject to the national security exemption. Regulation of the competence of DPAs in respect of intelligence may, however, be provided in national law."

And then they identify: "*Seven Member States where the DPAs have the same powers over national intelligence services as they do over any other data controller. This does not necessarily mean that national legislators have endowed the DPAs with the full range of powers listed above. It means that the legislators have not distinguished between intelligence services and other categories."*

Then: "*In 12 Member States they have no powers over intelligence services. They are either expressly excluded by the general data protection law or by specific laws."* 11:16

And there is some examples there. And then in Luxembourg there is a reference made. Then moving on to the second last paragraph: 11:16

"*In nine Member States - including Ireland - DPAs have limited powers over intelligence services. While these DPAs have the power to issue non-binding recommendations on general matters related to national intelligence services' surveillance, limitations vary considerably by Member State."* 11:17

Then, Judge, there is further detail given in respect of particular countries.

Then if I could ask the court to go on to page 51. Sorry, I should just draw the court's attention to another helpful chart on page 49 which summarises the information that you have just been given there and identifies the various roles of DPAs. 11:17

And then, going on to page 51, one sees there expert bodies as alternatives to judicial supervision, and I am just looking at the box there. 11:17

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: It's a quote from a case called **Telegraaf Media Nederland** and the Court of Human Rights there held: 11:17

"*The Court has indicated when reviewing - sorry, I said, yes it is the Court of Human Rights decision - the Court has indicated when reviewing legislation governing secret surveillance in the light of Article 8, that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.*" 11:17 11:18

And the court is familiar with the **Klass** quote there and I think there is nothing - and then there's a

reference to **Kennedy** and I think both of those quotes the court in fact already saw yesterday.

And then if I could ask the court to look please at page 57. Sorry, there is one other helpful chart again on the next page, page 52, and this is the point about target, *"prior approval of targeted surveillance measures"*, and you will remember that that was a question in the US context that the court was looking at. 11:18

But I think it is important to remember here, Judge, that the phrase *"targeted surveillance measures"*, you'll remember this morning when I started there is a distinction between drawn being *targeted surveillance measures* and *signals intelligence measures*, so I think this is, if you like, the old fashioned, if I may call it, warrant-type situation, and I think that's what that's being referred to there. 11:18

Can I ask the court then please to go on to page 57, and the court sets out its key findings in this area and I won't go through those. I think I have dealt with them by and large, but it's a useful summary for the court to see the findings. 11:19

Then moving on to the chapter that's possibly the most relevant at page 59, that on *"Remedies"*. You'll see there that the court identifies the necessity for a

remedy to *"be effective in practice and in law"* and then on the first column on the second last paragraph:

"*As presented by FRA reports on access to remedies for violations of data protection and on access to justice, a number of remedial avenues are available to victims of privacy and data protection violations.*" 11:19

But again, Judge, that is in the general sphere. Because on the next paragraph it states: 11:19

"*When an individual wishes to complain about interference with his or her right to privacy and data protection by intelligence services, the remedial landscape appears even more complex. The different remedial avenues are often fragmented and compartmentalised, and the powers of remedial bodies curtailed when safeguarding national security is involved. In fact, data collected for this research shows that only a very limited number of cases challenging surveillance practices have been adjudicated at the national level since the Snowden revelations.*" 11:19 11:20

And there's a number of important points about that. 11:20 First of all, the word *"fragmentation"*, because you have seen that as part of the DPA's criticism. This was a report that was out by the time the DPA made her decision. This is a 2015 report, she made her decision

on May 2016. She does not appear to have reverted to the existence of this report, but it does seem very important in our submission that in the European context also this fragmentation is identified.

11:20

Now you will remember yesterday from **Silva** and from **Leander** that in fact the court says that in certain circumstances a grouping or a mix of different remedies will be acceptable under the Court of Human Rights jurisprudence, but nonetheless it does appear to be identified here as a criticism of the European system by the FRA.

11:21

Then, Judge, just moving on to the last paragraph on that page:

11:21

"*Various actors have highlighted loopholes in the remedial landscape. In the UK, for example, the Information Commissioner pointed out in written submissions to the Intelligence and Security Committee of Parliament that 'state surveillance of individuals' communications, be this content or metadata, engages significant privacy and data protection concerns. The Data Protection Act provides only limited reassurance as a wide ranging exemption from its provisions can be relied on where safeguarding national security is engaged. The current legal and regulatory régime is fragmented.*"

Again we see that word: "*And needs review to ensure that it is fit for purpose in providing appropriate and effective oversight and redress mechanisms given the communications technologies and networks in use today and likely to be in use in the foreseeable future.*" 11:21

That's a long quote from the Information Commissioner but cited with approval by the FRA.

You'll see then that there's an identification by way of diagram of the various avenues for persons, the Ombudsman - I beg your pardon, Ombudsperson institutions, the courts, ordinary and specialised, the oversight bodies other than DPAs with remedial powers and the DPAs. And that's, I think, an important 11:21 11:22 identification there of remedial avenues at the national level because again the DPC treated the remedial avenue as only being litigation by an individual person, and that is a narrow approach particularly in this context because of all of the 11:22 limitations on that type of redress that we have already identified.

And, Judge, you'll see there that, when one looks at the ECHR case law in respect of Article 13, the 11:22 remedies provision of the Convention, that you already have looked at yesterday, you'll see there there's a case that I didn't open, **Wiberg -v- Sweden** where they --

MS. JUSTICE COSTELLO: Which page are you on now?
MS. HYLAND: Sorry, Judge, I'm on page 60, the same page that that diagram is on, and there's a box there with an extract from the Convention case law.
MS. JUSTICE COSTELLO: Oh, ***Segerstedt-Wiberg***. 11:23
MS. HYLAND: Yes, exactly, I am sorry, you are right. I took the easy way out there. You will see:

"The 'authority' referred to in Article 13 [of the ECHR] 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 remedy is effective. Furthermore, where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must become available to the individual."

11:23

And then turning over the page, Judge, you'll see there a precondition obligation to inform and the right to access. And at 3.1 FRA deals with this point:

"The obligation to inform and the right to access one's own data can generally be perceived as a strong safeguard for ensuring the effectiveness of a remedial action, and, ultimately, legal scrutiny by judicial or non-judicial bodies. From the point of view of the 11:23

right to data protection, these safeguards also ensure transparency of data processing and the exercise of other rights of the individual, i.e. the rectification and/or deletion of data being processed unlawfully. In the context of surveillance, even with necessary restrictions, the obligation to inform and the right to access also enhance transparency and accountability of the intelligence services and help to develop citizens' trust in government actions. Legal and judicial or non-judicial bodies from the point of view of the right 11:23
of data protection these safeguards also ensure transparency of exercise of other rights of the individual, i.e. the rectification and/or deletion of data being processed unlawfully in the context of surveillance even with necessary restrictions, the 11:24
obligation to in fact the right to access also enhance transparency and accountable of the intelligence services and help citizens trust in government actions. To safeguard national security, obligations under Article 13 may be restricted to the extent necessary 11:24
and properly justified."

And then there's a discussion of the Court of Justice case law. Then there's also a reference to **Klass** as well, and the court has already seen that, and if 11:24
I could ask the court to turn over then.

Then, Judge, just looking at the situation in the Member States, the first column on the left-hand side:

"*The legal frameworks of all Member States allow restrictions on the obligation to information and the right to access on the basis of a threat to national security and/or the intelligence services objectives.*

Differences are, however, observed as to the conditions and levels of restrictions. Some Member States do not provide for the obligation to inform and the right of access. Others provide for restrictions on the grounds of existing threat to national security, yet these restrictions are not identical. Finally, some Member States balance the restrictions by giving oversight bodies the mandate to a) check whether the invoked national security threat justification is reasonable in fact and/or b) to exercise the right to access indirectly, i.e. on individuals' behalf." 11:24 11:24 11:25

And I suppose, Judge, one must just bear in mind here that the FRA have already said that they have only looked at five Member States in the context of *signals* intelligence. So what's being looked at here is in the context of *targeted* intelligence, and I think that is important to remember so as not to assume that what's being discussed here is in the context of signals intelligence because we know that in only five cases they were in fact able to consider the relevant laws in being. 11:25 11:25

And then: "*The obligation to information and the right*

to access are not provided for in eight Member States - and they identify those Member States including Ireland - This is attributable either to national data protection laws, which do not apply, or to derogations enshrined in specific laws." 11:25

And that also includes the United Kingdom.

Then half about half way down: "*In some Member States, States, the obligation to inform and/or the right to access are restricted because of rules applicable to classified documents and official secrets. In Latvia, the specific law on the intelligence services stipulates that information gained by the intelligence services is of restricted access or classified as an official secret."* 11:26

And then the last paragraph: "*In the other 20 Member States, the obligation to inform and right to access are provided for in the law, albeit with restrictions. The conditions vary regarding when the individual must be informed or may exercise the right to access, or other qualifying aspects."* 11:26

And then there's an identification of the various laws. 11:26
And then just at the very bottom line:

"*In five Member States, specific laws exempt the intelligence services' activities from the remit of*

general data protection legislation.

Independent of whether this is done on the basis of a general data protection law or in accordance with specific legislation, individuals' right to access and the services' obligation to inform tend to be restricted on the ground that the information would threaten the objectives of the intelligence services or national security. This restriction applies for the entire period during which such a threat exists. An assessment of the threat should therefore be performed over time to ensure that the restriction is justified."

Judge, this is important, particularly important this section, because you will remember that it was asserted by Mr. Murray that the **Tele2** case in particular, I think at paragraph 120, has a right to notification. And we have already said, Mr. Gallagher has already said that this is in the context of criminal enforcement in any case. It's easy to see, in my submission, why that must be right. Because it could not be the case that the Court of Justice unilaterally would have imposed an obligation on all intelligence services to notify without any caveat or possibility for that notification right to be restricted where the national security demands that to be the case. 11:27 11:27 11:27

And in fact when one looks at the wording of paragraph 120 there is a reference to *"in accordance with the*

national laws". So even in the criminal sphere there's a --

MS. JUSTICE COSTELLO: Paragraph 120 of what?

MS. HYLAND: I beg your pardon, of **Tele2**, of the decision of the Court of Justice in **Tele2**, which of course came after the data protection's decision in any way. But it is just important to reflect on the fact that, as we have already said, there is no EU obligation to notify. There *is* no obligation under the Convention of Human Rights to notify. There are some cases where the Convention, where the Court of Human Rights have said that a Member State lack of notification coupled with the régime as a whole is a breach of Article 8. 11:28 11:28

But the notion that there's a *standalone* EU law right to notify without exception in the national security side is just simply not borne out by anything that has been opened to this court and it is in my submission important because it seems to be a core aspect of what the *DPC* believed to be the EU law and we say that's quite mistaken. 11:28

Can I ask the court then please to go to page 65, just some two pages on. Now we move into the specific signals intelligence area. You'll see there that, on the second column on the last paragraph: 11:28

"*Only two of the five Member States authorised to*

conduct signals intelligence distinguish between the obligation to inform an individual in case of targeted surveillance versus their obligation to do so when an individual is affected as a result of signals intelligence. These provisions focus on the obligation 11:29
to inform an individual regarding data collection that is conducted automatically and according to predefined filters. In this phase, the laws provide for the lifting of the obligation to inform. In particular, the obligation to inform does not apply if a) the 11:29
search terms are not directly related to the individual (Sweden) or b) the data are immediately deleted after they have been captured through use of the selectors (Germany)."

11:29

I think what that flags to the court in my submission is that the question of notification in the context of signals intelligence is a delicate and difficult one which is very different to that where there is the traditional warrant authorising tapping of a person's 11:30
phone. And in that situation it is of course considerably easier to provide notification. But where one is looking at signals intelligence, with all the complexities that this court has already been exposed to, the situation is, I think, one that could only be 11:30
dealt with in detailed legislation and hasn't been dealt with at the EU level in detailed legislation. There is some national legislation, not very many Member States as we can see, but nonetheless it is not

something that is susceptible, if you like, to a one-size-fits-all answer, if I may describe it in that way.

Now just turning over the page to 66 *"Judicial Authorities"*: 11:30

"Courts provide an avenue for individuals to complain about interference with their privacy and to seek a remedy, including in the area of surveillance. However, several obstacles stand in place for an individual complaining about signals intelligence: The courts' lack of specialisation; general procedural obstacles, such as costs, delays or complexity; and a lack of concrete evidence and a high burden of proof for establishing the veracity of evidence, or possible invocation of state secrecy privilege, including 'neither confirm nor deny' stances. These major obstacles can, in some cases, be mitigated in systems with specialised tribunals/courts, where judges possess the knowledge necessary to decide on often technical matters and are also allowed to access secret material. Other elements that can facilitate an individual's access to remedies include more relaxed standing proof rules, class actions and effective protection of 11:31 *whistle-blowers. The Parliamentary Assembly of the Council of Europe has stated that whistleblowing is 'the most effective tool for enforcing the limits placed on surveillance'. The Committee of Ministers of*

the Council of Europe adopted a Recommendation on the protection of whistleblowers."

And then there's a reference to whistleblowers.

11:31

But that paragraph, Judge, the importance of it in this case in our submission cannot be overemphasised. Because it shows that all of the obstacles that were identified in the US context are also present in the European context in the different Member States and that is vital, we say.

11:31

"Lack of specialisation and procedural obstacles" and then there's an identification of the **Schrems** case.

11:32

Then turning over the page, Judge, to page 67 and going to the top of the page:

"*Furthermore, for individuals to obtain adequate redress for a suffered harm, they must usually bring sufficient evidence of unlawful surveillance in the context of targeted or signals intelligence, individuals often do not have the fully-fledged right to be notified that they have been the subject of surveillance measures and/or to have access to such data. There is often no information provided in practice. In the United Kingdom, for instance, there is a well-established policy of 'neither confirm nor deny' responses to questions about sensitive matters of*

11:32

national security. Individuals have therefore little opportunity to submit concrete evidence, which often makes the courts (but in some cases also non-judicial bodies) inaccessible avenues in practice. The Council of Europe Commissioner for Human Rights stated that 'such modifications to proceedings can make it difficult or impossible to have a fair trial'. The Irish High Court acknowledged the inability to provide evidence of such situations."

11:32

Then there's a reference to the German case that Mr. Gallagher had already identified to you, about the 37 million communications, 12 being considered relevant and the Federal Administrative Court holding the complaint was:

11:33

"*Inadmissible as complaints against strategic surveillance of telecommunications under the relevant domestic law were only admissible if it was evident 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 data collected through the search terms are immediately deleted."*

11:33

11:33

And the court then goes on or, sorry, the FRA goes on to say:

"*In this context and in light of existing ECtHR*

jurisprudence on victim status, the possibility to challenge the constitutionality of the mere existence of legislation permitting secret measures, without having to allege that such measures were in fact applied to an individual, is an important safeguard." 11:33

And then there's a reference to **Weber and Saravia** that the court has already seen. And then:

"*The applicants in what became known as the **Weber and Saravia** case complained about the expansion of the Federal Intelligence Service's powers of strategic telecommunications surveillance. The German Constitutional Court ruled that the legal provisions on the competences of the BND regarding surveillance for the purposes of pre-empting money laundering, the use of obtained data, the transfer of data to other authorities and on the limited obligation to notify affected persons, were not compatible with the German Basic Law. The court also demanded stronger oversight by the G10 Commission. Because of this judgment, the law was substantially revised in June 2001. The court applied similar rules to the burden of proof as the European Court of Human Rights."* 11:33

11:34

And in fact, Judge, I think that was the ruling of the constitutional court prior to it going to the Court of Human Rights because in the **Weber** case you see them referring back to the constitutional challenge.

And then, bottom of the page: "*In addition to these specific procedural obstacles and the fact that individuals often simply do not know that they are a target or encompassed by surveillance, going to court often exposes individuals to lengthy, time-consuming,* 11:34 *complicated and costly procedures. That is why individuals may prefer to access justice via non-judicial avenues or through intermediaries, such as relevant civil society organisations. The latter may play a vital role in taking such complaints to court when class actions are allowed, as well as in bringing cases of a more general nature requesting access to specific information on the activities and investigative methods of intelligence authorities to contribute to greater transparency and accountability in this area. However, civil society organisations often lack adequate resources, and few are able to offer comprehensive services to victims of data protection violations."* 11:35

And then, Judge, to the next column, just looking at the Irish case:

"In Ireland, a complaint can be made to the Complaints Referee, a judge of the Circuit Court nominated to hold this specialised position. The referee may investigate whether there has been a contravention of the relevant provisions of the Act on interception of communications. If a complaint is upheld, the

Complaints Referee will quash the interception, report the matter to the Taoiseach (prime minister) and recommend a compensatory payment. To date, this has not occurred. In parallel, a civil action for damages for breach of privacy protected by the constitution can also be taken in the High Court."

And it is noticeable - I beg your pardon *notable* - in the Irish context that there is no right to notification here, and the DPC obviously must have been aware of that being in this jurisdiction. There is a different remedial approach which is to make a complaint to the Complaints Referee and I will deal with that. 11:35

Can I ask the court then please to go to page 70 and then there is a consideration of *"non-judicial remedies, independence, mandate and powers"*. Actually, Judge, could I just ask you to look at the UK, just on the previous page, page 69, on the left-hand column there is just a brief summary of the UK approach. 11:36

"*It has been the long-standing policy of the United Kingdom government to give a 'neither confirm nor deny' (NCND) response to questions about matters sensitive to national security. The IPT - that's the Investigatory Powers Tribunal - recognised the legitimate purpose and value of such a response in several cases. It held that 'the NCND policy is needed*

to help to preserve secrecy', and that it does not interfere with the right to privacy in cases where there is no relevant information held on the complainant. In 2010 for example, 30% of the 164 complaints received by the IPT were directed against security and intelligence services", and then there is some detail about that.

Judge, then there's an identification of the various types on page, the following page, page 70, the various non-judicial remedies and the types of non-judicial bodies. At 3.3.2, the issue of independence of those bodies, and then if I could ask the court to turn to page 72 and you'll see there at 3.3.3 *"powers and specialisation of non-judicial remedial bodies"* and the FRA notes that: 11:36 11:37 11:37

"*Any non-judicial body tasked must have the power to conduct a thorough review of the case which includes having access to all relevant materials and having the power to grant a binding remedy. Although this section focuses on the powers of non-judicial remedial bodies, the question of specialisation of such bodies is also briefly touched on."* 11:37

And then there is a reference in the box to a case, the case that we have already looked at, or sorry the case the court already identified **Segerstedt-Wiberg**, and that is in respect of the parliamentary Ombudsman and

its role in Sweden. In that particular case it was not considered to be effective for the very good reason, Judge, that, about half way down:

"*They both lack the power to render a legally binding decision. In addition, they exercise general supervision and do not have specific responsibility for enquiries into secret surveillance or into the entry and storage of information on the security register.*" 11:38

So it seems that they have general powers but not one specific to the surveillance area.

Then, Judge, just coming to the end of that report, at page 75 one sees the key findings, and again I don't think I need to set them out because I have gone through them. 11:38

So, Judge, that, I think, is an important report. It shows the very grave issues on the European side as well as on the US side and shows that there can be no complacency or assumption that on the European side there is unhindered access to courts for the purposes of vindicating privacy rights in the area of surveillance. 11:38

Some of that arises because of the particular issues with surveillance. It's, if you like, the structural issue and the FRA Report recognises that oversight is

the correct response in that situation, that there must be a holistic approach.

Judge, can I move now please to the United Kingdom and I'm going to just deal very briefly with the David Anderson report known as the report of the bulk powers review. This is an August 2016 report. David Anderson is the independent or was, he is now changed, there is a new person, independent reviewer of terrorism. He had done the report called a *"Question of Trust"* in 2015 which was referred to in the FRA Report, but this is a different report. 11:39

And, I suppose, why am I asking the court to look at it? Well, for a number of reasons. First of all, I think it's helpful in describing the kinds of surveillance that take place in the United Kingdom, much of which you will see echoes of from the US system. It directly compares the US surveillance, some of the various different avenues, with the UK, and I think that's a useful. It makes reference to the PCLOB, it makes reference to the Snowden disclosure. It shows that the same types of activities are going on in the United Kingdom as are going on in the US and one cannot see the US as any kind of outlier in this respect. And I'm going to move quite briefly through it, Judge. 11:39 11:40

MS. JUSTICE COSTELLO: Where is this report and who has exhibited it.

MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: And what status does it have in these proceedings?
MS. HYLAND: So it has been exhibited by Mr. Clarke and Mr. Robertson. Sorry, both of them refer to it, neither of them actually exhibited it, but both of them refer to it, said that they had read it and said that they took on board its conclusions. 11:40
MS. JUSTICE COSTELLO: But I still haven't read a word of Mr. Robertson's affidavit. 11:40
MS. HYLAND: Yes. Well, I can do that straight way.
MS. JUSTICE COSTELLO: Well, there was an issue as to what was to be allowed --
MR. GALLAGHER: It's resorted or resolved, sorry.
MS. HYLAND: Yes, that's now been -- and the reason I'm doing it last is -- 11:40
MS. JUSTICE COSTELLO: Does that mean I can read it or I can't read it?
MS. HYLAND: You can, Judge. You can only read parts -- you can read parts of it basically. We have identified -- 11:40
MS. JUSTICE COSTELLO: How do I know which parts?
MS. HYLAND: I'm going to hand that up, sorry, Judge. The reason I was doing it at the end, I will hand it up straight away to you now. 11:40
MR. GALLAGHER: It's a party trick.
MS. HYLAND: Yes. I hope it doesn't disappoint, Judge, after the --
MS. JUSTICE COSTELLO: In which cup is the pea.

MS. HYLAND: The anxious waiting. Judge, it quotes a lot from the FRA Report and the bulk powers review and that's why I was intending to go to them first.

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: But the court obviously -- 11:41

MS. JUSTICE COSTELLO: No, no, that's fine. I just want to know where I'm going.

MS. HYLAND: Yes, exactly. So, Judge, I can identify that, perhaps if I could then, subject to the court, I could just open the parts of the bulks powers review 11:41 first and then go back.

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: Because it means I won't be, if you like, repeating that again. So, Judge, if I could just ask you then please to look at page 1 of the bulk powers 11:41 report.

MS. JUSTICE COSTELLO: Which? Is this exhibited in this document?

MS. HYLAND: I am so sorry, I beg your pardon, no. What I'm going to do, Judge, is, I'm going to give it 11:41 to you in a paper form, the bulk powers report. It is on the tablet in some of the additional materials, but I think it may be as easy just to give it to the court in a bulk, well in a bulk version. It certainly is quite bulky. I'm only going to move through it quite 11:41 briefly because of its size, but there is very valuable and important material contained in there. I can also give, the tablet is at, that particular report is on the tablet at present.

Can I just ask the court then to look please at page 1 of it, the executive summary, and you will see what the report is doing. He is evaluating the operational case for four of the powers in the Investigatory Powers Bill currently before the Parliament at that time. It has now been passed into law and those four powers were bulk interception, bulk acquisition, bulk equipment interference and bulk personal data sets, and I'm only going to look at the first two. 11:42

You'll see the third bullet point: 11:42

"*The security-cleared review team comprised technical, investigatory and legal experts who consulted widely.*"

You'll see that in the fifth bullet point the report concludes there was a proven operational case for three of the bulk powers and a distinct though not proven operational case for bulk equipment interference. 11:42

And you'll see then at the, I think it's the seventh bullet point: 11:43

"*The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower.*"

And the next bullet point: *"The Review was not asked to reach conclusions as to the proportionality of desirability of the bulk powers."*

And then if I could just ask the court please to go to page 4, paragraph 1.9, you'll see there this term *"mass surveillance"* that has been -- 11:43

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: -- before the courts. You will see there it is stated: 11:43

"Whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called 'mass Surveillance'. Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (whether held by the Government or by communications service providers [CSPs]) is not given on an indiscriminate or unjustified basis. Such limitations and safeguards certainly exist in the Bill."

Then turning over to paragraph 1.17 there is a reference there to the Snowden revelations and you will see about a third of the way down he says: 11:44

"The material taken by him through access to US National Security Agency [NSA] systems, and the

articles subsequently published in outlets including the Guardian and the New York Times, have been the basis for suggestions that in the UK as elsewhere, broad and obscure powers were being exercised in a manner that few had understood. Litigation, fuelled by those allegations, has persuaded the IPT - the Investigative Powers Tribunal - to indicate that some powers have lacked the necessary accessibility and foreseeability to comply with international human rights standards." 11:44

Then if I could ask the court to go to page 10 please, and I think this is very important. The *"bulk acquisition capability"*, and later in the report we see that described. You will see that it is stated there 11:44 the top of the page, paragraph (d), top of page 11:

"*The bulk acquisition capability which MI5 and GCHQ had under section 94 TA 1984 was not publicly avowed until November 2015."* 11:45

And what that means, Judge, and we will see a case called **Privacy International** about that. In litigation brought by **Privacy International**, and in the context of the Bill in respect of the new UK legislation, it was 11:45 admitted by the UK intelligence services that in fact they had been carrying out bulk acquisition since 2001 but it had never been a matter of public record or known at all, and, as one will see from here, it was a

very sensitive collection programme.

MS. JUSTICE COSTELLO: So even though he makes the distinction about mass surveillance and there is an acceptance of bulk acquisition.

MS. HYLAND: Yes. 11:45

MS. JUSTICE COSTELLO: Are we talking about 'a rose is a rose by any other name', or are we talking about a distinction?

MS. HYLAND: No, I think what he is saying is that, even when it was not avowed, when it was not known, 11:45 when there was no legislation about it, it was still not *mass surveillance* in the way that he referred to earlier on with no limitations or no controls or no winnowing down. But I think his point here is that it was not in any way known about, it was not in any way 11:46 subject to legal controls. So there are two, if you like, different points. One, I suppose, is operational and the other is perhaps legal.

Then just turning to page 16 you will see that there's 11:46 a reference at 1.44 onwards to *oversight bodies* and the reviewer had access to oversight bodies with access to classified information. And at paragraph 1.47 there is a reference to the PCLOB and the assistance that a member of the PCLOB had given to the Independent 11:46 Reviewer in this context.

Then, moving on to page 20, you will see he identifies the various, four types of powers, bulk powers, that he

is looking at and he has a chart there at page 20. And the bulk power in question, there is four, interception, acquisition, EI, which is equipment interference, and BPD which is bulk personal data sets and he categorises them depending on various approaches.

Then, just to turn on to page 21, the definition of *"bulk interception"*. And at 2.7:

"*Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.*"

So in some respects similar to 702. 11:47

Then at page 23 paragraph 2.13 *"how bulk interception works"* and there is some very clear, in my submission, Judge, very clear explanations in this report:

11:47

"*Interception is the process of collecting communications in the course of transit, such that the content becomes available to someone other than the sender or recipient. The fruits of interception (the*

main focus of which must be overseas-related: Can include both the content of such communications and information about them. Bulk interception typically involves the collecting of communications as they transit bearers (communication links)." 11:48

And in that respect it may be more similar to 12333 there, he appears to be talking about direct access on the bearers: "*Bulk interception involves three stages which may be called collection, filtering and selection for examination*" and he goes through those at 2.15 onwards. 11:48

At 2.18 he identifies the method of selection, he says: "*The application of these queries - and he's been talking about the various selectors - may still lead too many items for analysts to examine, so GCHQ must then carry out a triage process to determine which will be of most use. This triage process means that the vast majority of all the items collected are never looked at by analysts. Even where communications are known to relate to specific targets, GCHQ does not have the resources to examine them all. Analysts use their experience and judgment to decide which of the results returned by their queries are most likely to be of intelligence value and will examine only these."* 11:48 11:49

Then he talks about, at 2.19, the *"strong selector process"* and the *"complex query"* process. Then, moving

on to paragraph 29, he identifies some case law of the Court of Justice. At 2.28, he says:

"*More fundamentally, it has been suggested on the basis of CJEU case law that any bulk collection of the content of communications is per se unlawful.*" 11:49

And at footnote 78 he refers to the **Schrems** case. And, interestingly, he says, by way of comment on that:

11:49

"*The bulk interception régime does allow for the collection of content in bulk, though the Government may be expected to argue, if necessary, that access to that content is not granted on a generalised basis, and that the distinction suggested by the CJEU is hardly a binary one, given that content is held for only a few seconds under the procedure outlined at 2.19(a) above.*" 11:49

Then, Judge, turning on to page 31, you'll see there's a description there of how bulk acquisition works. 11:50 And, Judge, this is a different, we have now moved from bulk interception to bulk *acquisition* and this, I think, can be analogised to Section 215 in the US context.

11:50

This is the point, this is the collection, Judge, that was not identified and accepted until 2015 that I just mentioned a moment ago. And you will see at paragraph 2.35:

"*Secret directions under section 94 have since at least 2001 the GCHQ and from 2005 (MI5) enabled the SIAs to acquire.*"

They are the different intelligence bodies. 11:50

MS. JUSTICE COSTELLO: SIAs are?

MS. HYLAND: They are the - sorry. Yes, they are signals intelligence agencies, it's a generic term for a number of different agencies:

11:50

"*Enabled the SIAs to acquire communications data in bulk, including in particular records of domestic communications, for the purposes there set out.*"

And there's a description of that. 11:50

And at paragraph 2.41, he says: "*It can be said however that: (a) that the existing power and the power in Part 6 Chapter 2 of the Bill both enable the SIAs to obtain large amounts of communications data, most of it relating to individuals who are unlikely to be of any intelligence interest; but (b) content cannot be obtained under either power, and it is not currently envisaged that the bulk acquisition power in the Bill will be used to obtain internet connection records.*" 11:51

Then, Judge, turning on, please, to page 40, in fact this is in relation to EI, and I think I'm going to move on past that. But if I could ask the court to

look at page 57 there's an interesting comparison of Section 215 powers and the bulk acquisition powers.

At page 57 you will see at paragraph 3.47: "*Section 215 telephone records programme.*" Then there's a reference to the PCLOB's first report, which the court knows about: 11:51

"*Was on the telephone records programme conducted under an order issued by FISC under Section 215 of the USA PATRIOT Act.*" 11:52

And there is a summary there of that particular programme and the history of that programme. And then under the heading "*comparison with UK bulk powers*", 3.50: 11:52

"*On the basis of the summary description quoted above, the Section 215 programme has obvious similarities with the bulk acquisition power described above:* 11:52

(a) each programme allows for the storage of telephone communications data (or metadata) in a single database;
(b) the 'call detail records' described by the PCLOB fall within the definition of the 'traffic data'." 11:52

But then, interestingly, he goes on and he says:

"*It would be wrong to assume the two programmes are*

identical or even close equivalent." 3.51.

And what he concludes is that in fact the *UK* programme was much broader and much wider and allowed for much greater collection that the section 215. At 3.51(a) he says: 11:52

"*Nature of communications: The s215 power is limited to the collection of 'telephone records' relating to 'calls'. The UK bulk acquisition power relates to 'communications data', a category which is capable of including data relating also to e-mails, texts and voice over internet protocol telephony."*

"Types of providers", that's (b). In both cases essentially what he is saying is that it's not clear, both in the US and in the UK, whether or not records were obtained from *mobile* providers as well as landline providers. 11:53

11:53

"*(c) Categories of records. The records collected under the Section 215 power, again according to PCLOB, typically included 'the date and time of a call, its Duration, and the participating telephone numbers'. They did not include cell site location information. The UK category of 'traffic data', to which each of the current s94 directions relates, is potentially broader: In particular, it extends to location data and other related material. Under the Bill, the power will*

continue to extend to 'any communications data', with no statutory exclusion even for ICRs."

MS. JUSTICE COSTELLO: I am sorry, you will have to help me, ICRs?

MS. HYLAND: I think they are internet communicate - there is a, Judge, I will move the annex which had the key in it so I will come back to you in one moment. 11:53

MS. JUSTICE COSTELLO: I told I'm lost with these abbreviations.

MS. HYLAND: It's not a case for someone who doesn't like acronyms, Judge. Then *"permitted uses"*: *"The only purpose for which 'NSA analysts were permitted to search the s215 calling records housed in the agency's database' was 'to conduct queries designed to build contact chains leading outward from a target to other telephone numbers', on the basis of 'a reasonable, articulable suspicion (RAS) that the number is associated with terrorism'. But as demonstrated by the IO."* 11:54

Sorry, that's a UK supervisory body: *"And by the fact that no reasonable articulable suspicion is required under current UK law or under the Bill. UK analysts have a considerably wider range of uses for their records."* 11:54

So again a difference between the two programmes. And then *"scale of use"*, very interesting.

Yes, Judge, sorry, ICR is internet connection records.

MS. JUSTICE COSTELLO: Okay.

MS. HYLAND: Then just finally, Judge, on *"scale of use"*:

11:55

"The scale of use of the two programmes is very different. In 2012, the NSA (which is a foreign-focused organisation) queried only 'around 300 seed numbers'. In 2015 MI5 made 20,042 applications to access communications data obtained pursuant to s94 directions, relating to 122,579 items of communications data, and GCHQ identified 141,251 communications addresses or identifiers of interest from such communications data, which directly contributed to an intelligence report. That is despite the fact that data under s215 was retained for five years, as against 12 months under the UK power."

So, Judge, I think that's probably all I can do in the time available. But it is absolutely clear that one cannot, when one looks at this report, I suppose have any feeling that the US system is set apart or different. Judge, there is many other points in that report that one could look at, but for the moment that's, I think, all I can do.

11:55

11:56

Judge, can I just ask the court now, please, to go on to the affidavit of Mr. Robertson. Much of what he says relates back to the FRA and to that report we have

just looked at so I hope I'll be able to go through that relatively quickly. I think the court should have a copy of it with --

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: -- highlighted in yellow. Yes, very good. 11:56
So what we have done, Judge, is the parts that we have identified are of evidential value are identified in yellow and the rest is commentary by --

MR. MURRAY: Well, sorry, the parts that are in yellow are the parts that I have agreed to admit into 11:56
evidence. The rest are not admitted into evidence, that's my firm understanding.

MS. HYLAND: Yes, and I am explaining why they are there.

MS. JUSTICE COSTELLO: I read the yellow bits. 11:56

MS. HYLAND: Yes, but I am simply explaining why the court is being presented in this way with the report.

The introduction, Judge: "*I am the founder and co-head of Doughty Street Chambers, a large human rights practice in London comprising 35 QCs and 101 barristers. I hold BA and LLB (hons) degrees from Sydney University, a BCL degree from Oxford (which I attended as a Rhodes Scholar) and honorary doctorates from the Universities of Sydney, Brunel (UK) and the National University of Political and Constitutional Studies (Bucharest). I am a visiting professor in human rights law at the New College of Humanities and Queen Mary College (University of London) and a senior*

fellow at Regents University. I was admitted to the English Bar in 1974 and was made a Queen's Counsel in 1988, and have been a Master of the Middle Temple since 1997. I served as a Recorder (part-time judge) in London for 17 years (1993-2010), and as a United Nations appeal judge in the·Special Court for Sierra Leone (2002-07) acting as the Court's first President. I was appointed by the Secretary General as a 'distinguished jurist' member of the UN's Internal Justice Commission (2008-12), responsible, among other things, for interviewing and nominating UN judges, and in 2011 I received the New York Bar Association award for Distinction in International Law and Affairs. My book 'Crimes against Humanity - the Struggle for Global Justice' has been published in five editions in the UK and the US. As an advocate I have appeared in some 200 reported cases in international, media and constitutional law in superior courts in England, in the Privy Council, in the European Court of Human Rights, the European Court of Justice and in other national and international courts. I am author of the International Bar Association's thematic paper on the Independence of the Judiciary.

2. Specifically in relation to national security interception, this is an area to which I have given special study and has been a significant aspect of my practice since 1977, when I defended Duncan Campbell in the ABC official secrets case in which he was accused

of exposing for the first time the interception role of GCHQ. Thereafter I represented and/or advised a number of 'whistleblowers' and publishers which wished to report their revelations about matters of public interest relating to national security, and have written and lectured on the problems of balancing the right of individual privacy with the operations of intelligence services. I authored the 6th and 7th edition of what was then the main textbook on civil liberties 'Freedom - the Individual of the Law' with 11:58
chapters on these subjects, and my current textbook 'Media Law' (written with Mr Justice Andrew Nicol) also deals with the UK and European position. I advised Messrs Heinemann, the publishers of 'Spycatcher', a book about MI5 by a former employee, which the UK government sought to ban on national security grounds, and I represented the MI5 agent David Shayler in the House of Lords case, dealing with his prosecution for exposing 'national security' surveillance of public figures (this is the most authoritative determination of issues under the UK's Official Secrets Act). I have acted for many years as an advisor to international newspapers (the Wall Street Journal, New York Times, Barrons and others) and national media outlets in respect of public interest reporting that could impinge on national security, and advised the editor of 'The Guardian' in relation to publication of material from Edward Snowden. I have acted for Julian Assange and for Wikileaks. I am a member of the Advisory Panel of

the Australian Privacy Foundation.

3. I do not believe that I have any conflict of interest in providing what I trust is an objective expert opinion. I have, as a Queen's Counsel, been instructed to give an opinion to Facebook as to the consequences of the Schrems decision, but I have no other or continuing connection with that or any other of the organisations which may be affected by this case. In any event I am bound by my duty to the Court to assist it as best I can in respect of matters within my field of expertise and this duty overrides any conceivable obligation I may owe to the party instructing me or paying my fees. I should mention that I am a pro bono trustee of the Bureau of Investigative Journalism, which in 2014 brought a complaint, as yet unheard, to the ECtHR alleging that data interception violated journalists' rights under Article 10 to protect their sources, but I have no involvement in the case and it will not produce any financial benefit to the Bureau. I have cross-examined officials and agents of the UK intelligence services, and appeared with former directors of GCHQ (for example, at Chatham House) but I have not been 'positively vetted' or otherwise inculcated with the ethos of the secret world of signals intelligence - my knowledge of it partly comes from defending 'whistleblowers' and journalists prosecuted for exposing it. In this course I have had my telephone

tapped - easily ascertainable in Britain in the 1970's by declining to pay the telephone bill and observing that it was not cut off (the state's appetite for information being greater than its appetite for money)." 12:00

I think the stenographer just wishes to change there.

"*I expect, more recently, that certain of my telephone calls and e-mails may have been picked up in PRISM or Tempura programmes which work on 'key word' (i.e. 'selector') interception*" -- 12:00

MS. JUSTICE COSTELLO: The Tempura programme? Am I missing something? Is that a new word?

MS. HYLAND: I think it's a UK programme. I think it's -- well, I saw reference to it in David Anderson's report. But I'll see if I can find the references to where -- 12:01

MS. JUSTICE COSTELLO: But it doesn't appear it be a US one anyway.

MS. HYLAND: It doesn't appear to be a US one, no. 12:01

"*The key word being the mention of my client, Julian Assange. At other times I have had the benefit of secret surveillance against potential threats to myself, such as when I was with my client Salman Rushdie, who was the subject of a terrorist 'fatwa' and when I was counsel to an inquiry involving the Medellin cartel and when I was President of the UN Court in*

Sierra Leone. I have no opposition to national security surveillance: I believe that it is necessary and sometimes effective in countering terrorism. I have expressed a general criticism of the composition of its oversight bodies because they lack persons with expertise in privacy and human rights - those I have termed 'patriotic sceptics', a class that would include Mr Schrems."

Then turning over the page, paragraph five: 12:02

"*I was invited to provide this opinion by way of instruction from Gibson Dunn and Crutcher LLP on August 24th, 2016, which I append (without the enclosures) as Appendix 1 to this affidavit. As will be appreciated from the issues I was asked to address... these included a description and analysis of protections and remedies available in the 28 EU Member States in respect of national security protection. This is a vast undertaking, and I am relieved to report that it has already been undertaken by the European Agency for Fundamental Rights, as part of its project for the mapping of Member States' legal frameworks in respect of privacy... personal data... and rights to remedies*" - Articles 7, 8 and 47 - "*Its report in November 2015, 'Surveillance by Intelligence Services: Fundamental rights, safeguards and remedies in the EU' is the most comprehensive and authoritative account of this subject, inspired by the Snowden revelations and*

written with the shadow of terrorist attacks in Europe well in mind. I have considered it carefully and adopt it as providing a sound factual basis for my opinion in respect of the disarray and disparity in law and practice in the European States. It is appended as Appendix 2, and I have additionally drawn upon the FRA country studies which backgrounded it, and on its Case-Law Database which compiles case law from the CJEU and ECHR and some national jurisdictions in respect of privacy, data protection and remedies. The FRA project is ongoing: I consider that its work so far serves to endorse my opinion· about the unreality of the assumptions concerning EU law made in Schrems.

6. I have indicated, in Appendix 3 and in the course of this opinion, the published material upon which I have relied for information which is not directly known through my work and experience. In relation to contemporary US law and practice I have been supplied with an article, 'US Surveillance Law, Safe Harbour, and Reforms since 2013' by Peter Swire, and with Professor Swire's draft report in these proceedings. I have also found helpful and authoritative two reports by David Anderson, a UK Queen's Counsel whom I know and consider to be an important, quasi-official exponent of issues relating to the law and practice of national security surveillance by the UK (especially by GCHQ) in respect to the combating of terrorism, notably his June 2015 Report "A Question of Trust', and his August

2016 'Report of the Bulk Powers Review'."

And that's what we've just looked at, Judge.

"*I consider the facts emerging therefrom to be reliable. The former report sets out the powers and duties of European States in respect to surveillance systems which encroach on personal privacy, and the latter makes what is in my view (and, more importantly, the view of the UK Government) an unanswerable case both as to the legality of bulk (or 'generalised') surveillance with appropriate oversight and as to its utility in identifying and investigating terrorist threats before they result in mass murder*."

Judge, can I skip on then please to the next section. And that section may be found in -- sorry, Judge, I actually had a marked-up version and I'll find that in one second. If I could ask you again, Judge, please to go to page 27. 12:04

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: "*European rights and remedies against SIGINT.*

The human rights provisions which apply to 47 Council of Europe States, which include the 28 EU states, are those in the European Convention which in the case of national security operations permits a wide 'margin of

appreciation' (see later). Article 8 requires respect for privacy, and Article 13 guarantees an effective remedy. But the Council of Europe Commissioner for Human Rights has said that 'In many Council of Europe member states, bulk untargeted surveillance by security services is either not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures'."

That's a quote from the report that Mr. Gallagher opened to you yesterday -- or, sorry, the day before, I think, Judge.

"*According to this report only five states have laws applicable to Signals Intelligence intercepts, and in general 'national legal frameworks lack clear definitions indicating the categories of persons and scope of activities that may be subject to intelligence collection'.*

40. As for oversight:
'There is no Council of Europe member state whose system of oversight comports with all the internationally or regionally recognised principles and good practices' ... 'Diversity in politics and legal systems has translated into a great variety of bodies that oversee intelligence services. EU member states have vastly different oversight systems. As for

remedies against surveillance abuses, 'The remedial landscape appears ever more complex: The powers of remedial bodies are curtailed when safeguarding national security is involved'.

41. The Snowden revelations galvanised the European Parliament to call for a fundamental rights analysis of the powers of intelligence services, and various EU bodies concerned with digital data embarked on enquiries about the law and practices relating to national security intercepts within the twenty eight member states. Just as the enquiries began to report the absences of safeguards and remedies, with recommendations for reform especially in respect of bulk digital interception, Europe was hit with a series of terrorist atrocities, beginning with the attack on the offices of Charlie Hebdo magazine in January 2015 and various Paris locations in November 2015 and continuing the following year with horrific attacks in Brussels and Nice. States of emergency were declared and governments (especially in France and the UK) became more concerned with enhancing the powers of the security services, which in the case of digital interception were already very wide. The most comprehensive analysis is the [FRA report].

"*42. This FRA Report highlights 'the great diversity among member states regarding how intelligence services are organised and perform their essential tasks'.*"

And I've already read that aspect of the amount of staff they have and the statutory basis for targeted surveillance in 26 of the 28, but only five having any legislation in respect of signals intelligence. 12:07

"*The Council of Europe Commissioner for Human Rights has recently concluded that 'in many countries, there are few clear, published laws regulating the work of these agencies'.*

In relation to oversight, the FRA report examines:

(a) Executive Control."

12:07

Then, Judge, there is a summary of the various -- and I think I'll read this, because he has identified what he considers to be important.

"*This means, inevitably, an exercise of political power through the President/Prime Minister or ministers responsible for national security. It is not independent of government - it is government. The Report reveals a considerable measure of political direction and control. In France, the President chairs the National Intelligence Council, which includes the Prime Minister and other relevant ministers, and the Prime Minister is responsible for the Inspectorate which oversees the intelligence services. Bulgaria,*

Croatia, Italy and Portugal have similar arrangements, whilst in Greece the intelligence services are under the direct authority of a government minister. In the UK, ministers rather than judges authorise surveillance warrants, and the Prime Minister exerts powerful influence by appointing the two Commissioners responsible for oversight and by nominating members of Parliament's Intelligence and Security Committee. In Germany, the Federal Chancellery supervises the work of the intelligence service (the BND). In short, the report demonstrates how control is exercised by the executive in most states through its powers to task the services, to appoint and dismiss its leading officials, to appoint members of oversight bodies, to issue instructions and to approve surveillance measures. Executive control is, in my judgement, a very unsatisfactory safeguard - indeed, it is not a safeguard at all against politicisation and malicious abuse of data for political reasons to undermine or damage data subjects. Nor is it a safeguard against intelligence service error or overreach: Ministers in my experience almost always issue the surveillance warrants that their officials request because they are elected politicians and afraid of embarrassment if they do not and it later emerges that, had they done so, information might have been gleaned that would have helped to avoid a terrorist atrocity. They do not have the time or the judicial mindset to study each case, and tend to act as 'rubber stamps'. Human rights

require safeguards against *the involvement of politicians in the secret surveillance process.*

(b) Parliamentary Oversight

44. Most EU States, with the exception of Malta, Finland and Portugal, have parliamentary committees that concern themselves with the intelligence services. However, as the Council of Europe Commissioner puts it, 'The nature of these bodies means that most are not in a position to undertake regular, detailed oversight of operational activities including the collection, exchange and use of personal data.' Most are concerned with budgetary allocation and receive reports from security chiefs, some in secret and some in public. Only four committees in EU Parliaments can receive and investigate complaints and involve themselves in authorisation measures - in Romania, Hungary, Luxembourg and Germany. All the others must operate on trust - and in my experience security services cannot be trusted where they are concerned to cover up embarrassing failures or to over-promote success in an effort to obtain a higher budgetary allocation. The FRA report notes a confusion in the composition of parliamentary committees: Some cannot obtain access to classified information, and some have members 'vetted' by the intelligence services before they can obtain access. Security clearance of MP's is required in Estonia, Hungary, Latvia, Lithuania and Poland, but in

other countries it is regarded as violative of the separation of powers. Whether MP's are vetted or not, these Parliamentary committees do not represent a 'safeguard' of any great weight, as they cannot investigate and the majority of MP's will in any event be drawn from the governing party. Their lack of curiosity about the development of bulk interception or the omnipresence of GCHQ/NSA surveillance power prior to the Snowden revelations speaks for itself. The FRA report notes that 'Remarkably, the majority of Parliamentary Committees do not have access to classified information received from foreign secret services ... Therefore in practice there is for the most part no oversight of intelligence sharing.'

(c) Expert Oversight

45. Only 15 of the 28 member states have established expert committees for intelligence service oversight. These could provide independent oversight, if properly resourced, although most are appointed by Government and most members are 'vetted' by the intelligence services. There are questions over their independence from government or the intelligence services or both - and some states do not supply them with the resources necessary to be effective. Only Ireland, the report notes, 'has established the position of a specialised judge, who is in charge of adjudicating matters of communications interception'. Judges are favourite

appointees to expert bodies (intelligence commissions and the like) in all member states, although 'Judges are legal, not technology specialists ... and do not necessarily have the expertise required to oversee intelligence services'. The report endorses the recommendation of the Council of Europe Commissioner for Human Rights, that oversight bodies 'should, to the greatest extent possible, be composed of individuals with diverse backgrounds' including experts who can 'provide them with a better understanding of surveillance systems and their human rights implications.' However, in a lengthy review of oversight bodies, I note that none of them seem to have places reserved for experts on human rights or civil liberties and may require 'vetting or membership of the intelligence establishment'.

46. A study of Data Protection authorities in Europe reveals that in 12 member states they have no power over intelligence services at all, since this work is expressly excluded from their remit by the general data protection law. In a further 9 member states, they only have a limited power to make non-binding recommendations. The 2014 recommendations of their representative body, the Article 29 Data Protection Working Party (WP 29), that effective and independent supervision of intelligence services is necessary and should be carried out by Data Protection authorities, has not been heeded. Among the FRA Report's

conclusions are that 'EU Member States have vastly different oversight systems' and 'In *some member states, the authorisation of surveillance measures does not involve any institutions that are independent of the intelligence services and the executive.' Importantly, it comments:*

'Access to information and documents by oversight bodies is essential. While information gathered by intelligence services is sensitive, and safeguards must guarantee that it will be dealt with accordingly, oversight bodies cannot carry out their tasks without first having access to all relevant information. The opposite, however, seems to be the norm'."

Then, Judge, if I could just ask the court please to go on then to page 49...

MS. JUSTICE COSTELLO: You want me to leave 33 and following?

MS. HYLAND: Oh, I'm so sorry, yes, I've actually missed -- sorry, I beg your pardon, Judge. So then the heading "Remedies in Europe". And then turning over to 33: 12:12

"*The FRA report on 'Remedies' in Europe demonstrates that they are subject to even more severe limitations and problems than remedies in the US.*

49. I refer to pages 59-76 in the FRA Report I have

appended as Appendix 2. It finds that, in seeking a remedy against the intelligence services, 'the different remedial avenues are often fragmented and compartmentalised, and the powers of remedial bodies curtailed when national security is involved'. Only a few cases challenging surveillance practices have been brought at the national level... Moreover, 'strict procedural rules on evidence and legal standing' deter recourse to the courts.

50. The first and obvious reason for the lack of remedy is that targets or victims of national security surveillance are not notified of the fact that their communications have been intercepted. The FRA reports that 8 member states do not provide any right to information or access."

Then there's a reference to the Czech Republic.

"*In the other 20 countries, rights to be informed come with conditions that exempt provision of information, e.g. in respect of 'necessary measures in the interest of national security'... In 5 of these states, data protection laws specifically exempt intelligence services from compliance. In only 6 member states does there appear to be a generalised right to be informed after surveillance has ended, although in (for example) Germany this is subject to the threat having disappeared - a question that arises in respect of*

'sleepers' and ISIS indoctrinees who may be 'resuscitated' in the future (the G10 Commission can decide that information can be withheld, even after 5 years, if release would endanger the national interest), while in Cyprus and Greece the intelligence services may request the Data Protection Authority to bar release on the grounds of national security. In some member states, the oversight body neither confirms nor denies SIGINT data processing when requested by a potential target. Only 2 member states have specific provisions on the obligation to inform SIGINT targets, and in one case the obligation does not apply to bulk collection and in the other it does not apply if the data has been immediately deleted."

I think this is Germany and Sweden, Judge, from the report we looked at.

"*51. In rare cases where targets obtain information that they have been targeted, further difficulties arise, over and beyond the general procedural obstacles - costs, delay and complexity. There is a high burden of proof, invocation of 'state secrecy' privilege and rules related to standing. Courts lack expertise in dealing with intelligence matters and tend to defer to the intelligence services.*"

Then there's a quote from the report which the court has already looked at, I think that's page 67 of the

report. Then going on to paragraph 52:

"*Given the problems with taking cases to the courts, some states offer specialised judges and quasi judicial tribunals. In Ireland the Complaints Referee has the power to quash interception, report to the Prime Minister and recommend a compensatory payment, although there had been none by the date of the Report. In the UK, the Investigatory Powers Tribunal (IPT) has exclusive jurisdiction to hear claims about SIGINT and the conduct of intelligence agencies, but it usually sits in secret and its powers are strictly limited to deciding whether legislation has been complied with and whether the agencies have acted 'reasonably'. It has upheld the UK policy of 'neither confirm nor deny' which prevents complainants from learning whether they have anything to complain about, and it has upheld the sharing of intelligence from PRISM on the grounds that there were 'sufficient safeguards in place'. In a landmark decision published in October 2016, the IPT ruled that bulk personal data collected by GCHQ and other intelligence agencies in years prior to the avowal of the practice in March 2015 was collected unlawfully, in contravention of ECHR principles as to the accessibility of law and the need for oversight. However, this was a pyrrhic victory for Privacy International: The Tribunal pointed out that individuals who could not prove that they had reason to believe that their data had been examined would have no*

right to personal action.

53. The FRA considers certain non-judicial remedies available in some EU counties, but it concludes that Data Protection Authorities, powers over intelligence services are weak, and that ombudsmen, although theoretically useful as a means of circumventing legal rules about standing, can only offer non-binding recommendations in cases of maladministration. It questions whether any such non-judicial bodies have true independence from government and the intelligence services, and notes that only 5 have the power to make binding decisions.

54. The FRA report is the most comprehensive and authoritative account of the laws and practices in relation to signals intelligence of the 28 member states of the EU. It confirms my opinion that national remedies for abuse of data gathered by way of digital interception by intelligence agencies are ineffective and inadequate. I have found no case, whether before or after the Snowden revelations, where an individual has been compensated by a court for being improperly targeted by SIGINT or for having their data misused to their detriment."

Then a heading "The Question of Aliens":

"*55. There has been no study, at least to my knowledge,*

about digital surveillance of foreigners ('aliens') in Europe, although a number of state laws do single them out for special treatment. Thus Article 5(2) of Germany's Artikel 10 Gesetz G10 restricts the German intelligence services in monitoring German citizens, but this restriction does not apply to citizens of other EU countries or foreigners - including, of course, Americans. There is a new bill which passed its first reading in the Bundestag in July 2016 which permits the German Foreign Intelligence Agency (the BND) to place foreigners under surveillance without a court order in the interests of national security, with certain safeguards applicable only to EU citizens (i.e. not to Americans). It allows the BND to share the information with foreign intelligence agencies - so that Americans in Germany could have their personal data intercepted without court order and passed on to the CIA. In the UK, sections 8(4) and 16(3) of the Regulation of Investigatory Powers Act offers greater protection to communications sent and received within the UK than are afforded to 'external communications' that are either sent from within the UK or received from outside, and hence more likely to involve a foreign communicant. In Poland, a Surveillance law introduced in Parliament in January 2016 gives police the power to intercept the comm1mications of foreigners without a court order in circumstances where such an order would be required for monitoring citizens.

56. These discriminatory initiatives have been justified by terrorism concerns over the refugee influx, and it remains to be seen how courts will react."

Then, Judge, turning on to the next page, heading "Bulk Data Collection". And you'll see there:

"*In my opinion bulk collection is acceptable, in a national security context if (but only if) it is subject to safeguards that ensure it remains strictly necessary and proportionate to the protection of national security.*"

Then going on to 58: 12:18

"*I do think that the legitimacy of bulk collection in the above context has now been put beyond doubt by the 'Report of the Bulk Powers Review' presented to the UK Parliament in August 2016 by an expert panel chaired by David Anderson QC. This followed concern over the admission by the UK Government in 2015 that GCHQ had long had a bulk acquisition capacity, used not only in respect of UK residents but residents throughout Europe (so much, incidentally, for European remedies: GCHQ had been bulk-collecting Euro data without let or hindrance for many years). The Review noted the internal safeguards in terms of retention and destruction procedures, and the external safeguards - a Government*

minister must sign the interception warrant (not a satisfactory safeguard in my view), and noted (at p.29) that until 4th November 2015 'the existence of the capability was an extremely tightly-controlled secret.' It endorsed the 'firm and reasoned conclusions" of the US Privacy and Civil Liberties Board on the utility of bulk collection, which under the 702 programme 'makes a substantial contribution to the Government's efforts to learn about the membership, goals and activities of international terrorist organisations, and to prevent acts of terrorism from coming to fruition.' So far as ECHR law was concerned, it relied on Weber to endorse the conclusion in Mr. Anderson's previous report, 'A Question of Trust' that '... bulk data collection and analysis in the absence of suspicion is not itself a disproportionate interference with the right to respect private life'...

59. The 2016 review closely considered GCHQ's anti-terrorist operations, including 19 case studies where bulk intercept information was used to apprehend terrorists or abort their plans. It found that over half of GCHQ's intelligence reporting on counterterrorism was based on data from counterterrorism warrants (in the year 2015, GCHQ identified from bulk surveillance no less that 141,251 particular communications or addresses of 'interest' to its intelligences operations. The report concludes that 'bulk acquisition has been demonstration to be

crucial (to) counterterrorism, counter-espionage and counter (nuclear) proliferation ... bulk acquisition has contributed significantly to the disruption of terrorist operations and, through that disruption, to the saving of lives'.

60....I have my own doubts (shared by Mr Anderson) as to whether a warrant granted by a Government minister is an appropriate safeguard for GCHQ bulk collection operations: Ministers are not independent of the Government, they are the Government, and in my experience they act as 'rubber stamps', hardly ever refusing to endorse warrants put before them by their secret services, this is because they are politicians, and overly afraid of political consequences if they were to turn down a request to monitor someone who later committed a terrorist crime. But there can be no doubt that bulk collection serves a legitimate aim and (with strong and appropriate safeguards) is necessary, in the sense of responding to a pressing social need, to protect democracy."

Then, Judge, I think the next point that I'd ask the court to look at is at page 49, which is headed up "'Below the Waterline' Arrangements". And it's paragraph 77: 12:21

"*I should mention one important development in juristic thinking about how 'adequacy' and 'sufficiency' tests*

are to be applied to the operations of secret surveillance organisations. It derives from recent case-law of the UK's Investigatory Powers Tribunal, when it has been asked by NGO's to consider the legality of PRISM and of other operations conducted by GCHQ. It has overridden the claimant's objections and determined to take into account, in determining the adequacy of safeguards, what it terms 'below the waterline' arrangements, namely the internal rules, codes and supervisory directions and oversight provisions that bind the administrators of secret surveillance, even though they may not be made public. The phrase, taken from naval warfare where ships are torpedoed - 'holed below the waterline' - is not entirely apt, but it does signify the administrative and disciplinary rules and codes, often unknown to the public, which are designed to ensure compliance with Article 8 within a large spying organisation. Evidence about these administrative rules and safeguards, which are not law but which have practical importance in day-to-day surveillance operations by GCHQ, have been deemed relevant and admissible in deciding whether safeguards against misconduct by security service officers are 'adequate'."

Then, Judge, I can take the court, please, to the conclusion section, which is at page 63.

"*104. In summary, looking at the present position in*

relation to national security data collection in the US and comparing it with the European equivalent, I have no doubt that Europeans have more real protection for their data in the US than they do at home. For example, Europeans have very little protection against national security surveillance from the ECHR, given its 'fairly wide' margin of appreciation doctrine. European law does not necessarily require court approval for it, and European Governments have no clear prohibition against spying on foreigners. Europeans have been spied upon for many years by GCHQ, and have had data of interest transferred by that organisation to the NSA and to DSD in Australia, and to New Zealand and Canada in relation to which they have had no knowledge and no remedy. In some respects, US standards are not 'essentially equivalent' but effectively superior. I endorse Timothy Edgar's comment in Foreign Affairs:

'The US has an impressive array of privacy safeguards, and it has even imposed new ones that protect citizens of every country. Despite their weaknesses, these safeguards are still the strongest in the world ... the US government should urge other countries to follow its lead'.

106. In this respect, Europeans cannot ignore the importance of the US intelligence agencies to their own security. International terrorism is a blight in

Europe, as the Paris, Nice and Brussels atrocities demonstrate, and information from the NSA, which is usually volunteered to its European counterparts, may save lives. Article 8(2) expressly permits derogation when this is necessary in the interests of national security and public safety. The PCLOB report anxiously interrogated the value of PRISM: It concluded:

'The programme has proven valuable in the government's effort to combat terrorism - monitoring terrorist networks under 702 has enabled the government to learn how they operate and to understand their priorities, strategies and tactics... (and) to identify previously unknown individuals who are involved in international terrorism and it has played a key role in discovering and disrupting specific terrorist plots aimed at the US and other countries'.

107. So I am satisfied - and I think the plaintiff should be satisfied - that US law and practice post PPD-28 is 'adequate' - sufficient, at least, to prevent any reversion to the secret world exposed by Snowden in which personal metadata was "hoovered up" without court or any other lawful authorisation and without any prospect for, redress. I am reinforced in this view by the history and tradition of a country with constitutional protection for privacy long before European countries; with elected representatives

prepared to investigate through congressional committees the conduct of the intelligence services (which are in any event obligated by statute to keep them 'fully and currently informed' of all intelligence activities); with a media that is more than willing to expose secret agencies, and powerful NGOs, like the ACLU, which take legal action when privacy rights are infringed on grounds of national security. At the present moment I consider that US privacy protections in respect of data sought for national security purposes are, in reality, more effective than any such protections in the EU."

Then at paragraph 109:

"*The US has a long history of balancing Fourth Amendment rights against the needs of law enforcement and national security: Its procedures are much more transparent and its oversight more formidable than that which obtains in European states. Citizens in the US are better protected in this area of national security interception than citizens in Europe.*

110. However, the question is whether the personal data of European citizens is 'adequately' protected in the US. On close study of the regulatory foreground at intelligence agencies it is evident that PPD-28 foreshadowed an end to disparate treatment and that all foreign data is now being protected to a considerable

extent by administrative rules and arrangements, both above and below the waterline - which implement that directive without actually bestowing enforceable legal rights on foreign data subjects."

Turning over the page, Judge, to paragraph 112:

"*I have been engaged, as advocate, advisor and author, in matters relating to signals intelligence over the past 45 years. In the 1970's, when the Cold War was still in progress, the subject was impressed with utter secrecy: Communism, which threatened the West, was the main target, and the criminal law was used to suppress journalistic enquiries about the UK/USA agreement and about GCHQ and its bases in Cyprus and Hong Kong and Australia and the NSA base in Turkey. There was a mystique about SIGINT, derived in part from the role of code breaking in allied success in World War Two. As the Cold War receded, SIGINT emerged from the shadows and although GCHQ was not recognised by legislation in the UK until 1989, it had begun to work against IRA terrorism and now, of course, it is in the front line of defence against Islamic extremism, with a role to play in identifying cyber attacks and nuclear proliferation.*

113. Evidence has emerged of abuse during the Cold War era, both in the CIA/NSA overreach established by the Church and Pike Committees and in cases in the UK and

Europe where individuals had been damaged or their job opportunities destroyed by leaks from the intelligence services as to their supposed 'subversive' tendencies. Protection against abuses of this kind came with the development through Article 8 of the 'privacy pillars': Clear definition of allowable targets, warrant authorisation, and rules about third party access and data retention and destruction. In respect of 'ordinary' criminal surveillance, there were requirements for notification and, in consequence, for legal remedies. This was not possible, however, in national security cases where surveillance was often longstanding of suspected communist cells and 'sleepers', and I am unaware of any SIGINT organisation in Europe voluntarily notifying interception targets and then being successfully sued. The rare cases brought against government agencies by targeted organisations (such as the Campaign for Nuclear Disarmament) were a result of information from whistleblowers, not from laws requiring notification.

114. The scourge in Europe in recent years of Islamic extremist terrorism has provided a strong justification for new forms of SIGINT surveillance, including measures of bulk collection, provided they can be demonstrated to work. That demonstration must necessarily be secret, to person or bodies of sufficient distinction that their publically-announced satisfaction carries credibility. Since the Snowden

revelations, the PCLOB in the US and the Anderson Reports in the UK have provided that credibility in relation to the utility for counter terrorism of operations which incidentally invade the privacy of numerous innocent persons. The consequence, in order to keep faith with privacy rights, has been for the Courts to insist on more stringent oversight, including oversight by persons independent of the security agencies.

115. In my opinion, this is being reflected in the US, where overseers within the surveillance organisations include lawyers experienced in privacy whilst external overseers include persons of distinction who have experience in technical matters and in civil liberties advocacy that qualify them to take the necessary sceptical approach the behaviour of SIGINT agencies. This development has not taken place in Europe, as the FRA Report demonstrates: Judges are generally used to provide the 'independence' necessary for oversight, although they tend to be deferential to the state, lack technical experience and are not usually assisted by privacy advocates as amici. In my opinion, in order to fulfil their purpose, oversight bodies must include persons whom I would describe as 'patriotic sceptics' - citizens whose loyalty to democracy is not in doubt" --

Sorry, Judge, this mass reading is taking it out of me.

"... *whose experience and qualifications in civil liberties will give confidence that they will look critically and intelligently at SIGINT conduct and claims. The introduction of such persons in oversight positions is resisted on the basis that they are not 'vetted' or otherwise inculcated into the secret world of SIGINT, but this is the very reason why patriotic sceptics should be counted amongst its overseers.*"

So, Judge, you have that report now, after some delay. 12:29
And I wonder could I just then deal with two other topics, or three other topics before I finish, Judge? And they are, very briefly, the position in Irish law, a number of points about SCCs and the position in respect of standing in the EU context. And I'll just 12:29
try and deal with them all briefly, Judge.

Can I just ask the court to look please at the Irish position? And what I'm going to just do, Judge, is hand in three pieces of legislation. There is *some* 12:30
legislation in the books, but they're not the updated versions, so we have taken the liberty, Judge, of effectively updating the legislation with any amendments so the court has the most up to date version. I should say that it's not an official 12:30
consolidation, because that isn't available, it's a consolidation that's been prepared by my solicitors in relation to the Interception of Postal Packets and Telecommunications Messages Regulation Act 1993 (Same

Handed). So that *is* in your book, Judge, that section, but the section that's in your book is not the completely updated one. And then, Judge, I'm also going to ask the court to look at Communications (Retention of Data) Act as well. 12:30

Judge, just very briefly, before I open the legislation though, I'll just summarise what the position is in Ireland. First of all, what if Mr. Schrems made a complaint in Ireland about how his data was being 12:31 treated by the security services? Well, the DPC, it's very unlikely, in our submission, that the DPC would be able to provide any redress, because Section 1(4) of the 1988 Data Protection Act, as amended, states that the Act does *not* apply to personal data that, in the 12:31 opinion of the Minister or the Minister for Defence, are or at any time were kept for the purpose of safeguarding the security of the State. So we say the DPC would not have a role because of Section 1, subsection 4. 12:31

Judge, in relation to prior judicial authorisation, we say that there's no requirement for same under either of the two Acts that I've identified to the court. In the 1993 Act the Minister gives an authorisation and in 12:31 fact in the Communications (Retention of Data) Act, that isn't even required - that's in relation to a direction to telecommunications operators and there's no need even for a Ministerial decision in that

respect. There are no notification requirements.

There *is* a facility to complain to a complaints referee, who can look into the matter, and in certain respects that is similar to the Ombudsperson provision that we have under the Privacy Shield. 12:32

In relation to standing, we're not aware of any cases where a challenge has been brought in respect of signals intelligence and where a court has adjudicated or dealt with this issue at all. 12:32

In relation to the state secrets issue, the court will be aware of case law such as **Ambiorix** and **Murphy -v- Dublin Corporation** where the courts are entitled to refuse the production of a document. In **Murphy** the court held that where the vital interests of the State, such as the security of the State, may be adversely affected by disclosure or production of a document, greater harm may be caused by ordering rather than refusing disclosure or production of the document. So that's an approach that is known in Irish law just as it is in the US. 12:32 12:33

In relation to standing, Judge, in the case of **White -v- Dublin City Council** - and I know much of these the court will be well familiar with, Irish rules on standing, so I'm only just identifying a number of cases we think are relevant - Fennelly J. held that a 12:33

challenge, it's well established that a challenge to the constitutionality of a statute will not normally be addressed unless the person mounting the challenge shows he is affected by the provision. In **Cahill -v- Sutton**, Henchy J. observed that a person must able to assert that his interests have been *adversely* affected or stand in real or *imminent* danger of being *adversely* affected by the operation of the statute. 12:33

There's no targeting or minimisation statutory provisions as far as we can ascertain, unlike, for example, in the US. In respect of what's known as meta-data - in other words, data that's not content-based data - particularly in relation to telephone calls, the who, why, where, when - in other words, information *about* the call, as opposed to the content of the call - that's governed by the 2011 Act. And as I've mentioned, it's not even necessary to have a Ministerial warrant to obtain, to direct a service provider to supply data. 12:33 12:34 12:34

I should say, Judge, the 2011 Act is based -- it was adopted to give effect to the Data Retention Directive. That is the Directive that was quashed in **Digital Rights Ireland** - so I should draw the court's attention to that - but it remains law in Ireland at present. It *is* being challenged, I understand, I don't know any more about it than that, but that is still extant law in Ireland. 12:34

Judge, in relation to oversight and ex post facto review, there are powers given to a judge of the High Court. And essentially the judge is designated under the two Acts I've talked about, the 1993 Act and the 2011 Act. And that judge is charged with keeping the operation of the Acts under review and of providing reports. And I'm just going to ask the court to hand -- if I may hand up the reports that have been provided by the judge. I think the judge is Judge McDermott at present. And there have been reports, we have been able to access reports for the years 2014, 2015 and 2016. But the court will see that the reports are very summary in form, don't disclose any substantive information, if I may say that. 12:35

And I suppose when one contrasts them with, for example, the kind of reports we saw in the US context -- I think the court was handed up a report, a semiannual assessment of compliance with 702 in the US context and it was a six-monthly report from, I think, June to November 2015 and I think there were some considerable number of pages, with a considerable amount of detail in the report. And I'm going to contrast the report not by any way of criticism of the High Court judge in question, but by way of, I suppose, identification of the fact that the resources have not been put in place by the government to carry out the kind of detailed assessment of compliance that one sees 12:36

in the US context. Those reports are just being handed up there and I'll just take the court through them (Same Handed).

You'll see, Judge, that the report that I think the court is being given is the 2015 report under Section 8(2) of the Interception of Postal Packets and Telecommunications Messages and the Communications (Retention of Data) Act 2011. And it's in similar form to other years. You'll see there: 12:36 12:37

"*As the designated judge under the above mentioned Acts, I arranged to visit the relevant authorities to examine files and records concerning the operation of the powers vested in them under the above Acts.* 12:37

1. On 23rd October 2011 I attended at the office of the Department of Justice and Equality and met with officials, who made available to me documents and records relating to the operation of the Acts as requested. I examined the files and records furnished and spoke to the officials responsible for the operation of the Acts and liaised on with other Irish authorities in respect of same. All documents requested by me were furnished and all questions posed by me in relation to the files and records produced were answered to my satisfaction. 12:37 12:37

2. On 30th October 2015 I attended at the Office of

the Revenue Commissioners and the Headquarters of the Defence Forces in McKee Barracks. In each of these locations, such documents and records relating to the operation of the above Acts as were requested by me were made available and examined. I spoke to the officers and personnel responsible for the operation of the above Acts. I had a number of questions in relation to the files produced, which were answered to my satisfaction. 12:37

12:38

3. On 30th October 2015 I attended at the headquarters of An Garda Síochána at the depot at the Phoenix Park, where I met with officers and personnel responsible for the operation of the above Acts. I examined computer records and hard copy files relating to the operation of the above Acts which were made available for my inspection and all documents and records which I requested were furnished and examined. All questions posed by me in relation to the operation of the Acts and the documents and records produced were answered to my satisfaction. 12:38 12:38

4. On 3rd November 2015 I attended the Office of An Garda Síochána Ombudsman Commission and I met with members of the Commission and personnel responsible for the operation of the above Acts. All documents relevant to the operation of the acts which I requested were furnished and questions posed by me were answered to my satisfaction. 12:38

5. I am satisfied, having examined the records and documents produced to me and from the information conveyed to me at these meetings that the relevant state authorities are in compliance with the provisions of the above Acts as of the date of this report."

Judge, that's for the year 2015. And in relation -- I think you've also been handed up a report from O'Neill J. of 2013, a single-page document; I don't know if the court has that? 12:38

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: Yes. And you'll see that it's in a similar form. And then another report from McDermott J. in 2014 and again in a similar form. 12:39

And I suppose if one contrasts again bodies such as PCLOB - and obviously it is in a different context and Ireland's a very different size - but it's just, I suppose, to identify the level at which oversight is being carried out in the US and perhaps not in the same respect in an Irish context. And this is something that one would expect the DPC to be aware of, because it is part of -- obviously she's operating in this country and these reports are publicly available. 12:39

Judge, just in relation then to the Irish Acts, I'm not going to go through them in any great detail, but if I could just ask the court to look please at the

complaints referee and the kind of responses that that complaints referee may have to a complaint. And one can see that, if you like, it's a closed system, if I may describe it in that way. Can I ask the court to look at the 2011 Act? It's in very similar terms in fact to the 1993 Act in terms of how one complains and what one does. And it's at Section 10, Judge, of that Act. And you'll see it's headed up "Complaints Procedure". 12:40

MS. JUSTICE COSTELLO: Yes. 12:40

MS. HYLAND: *"10. (1) A contravention of section 6 in relation to a disclosure request shall not of itself render that disclosure request invalid or constitute a cause of action at the suit of a person affected by the disclosure request, but any such contravention shall be subject to investigation in accordance with the subsequent provisions of this section and nothing in this subsection shall affect a cause of action for the infringement of a constitutional right.*

(2) A person who believes that data that relate to the person and that are in the possession of a service provider have been accessed following a disclosure request may apply to the Referee for an investigation into the matter.

(3) If an application is made under this section (other than one appearing to the Referee to be frivolous or vexatious), the Referee shall investigate –

(a) whether a disclosure request was made as alleged... and
(b) if so, whether any provision of section 6 has been contravened in relation to the disclosure request."

I think the reference to "frivolous and vexatious" is important, because it may well be that the referee may take the view that *if* somebody writes in and says 'I think I've been surveilled', but gives absolutely no basis for their reason for that, the referee may decide that it's a frivolous and vexatious complaint. Of course one cannot know, because there's no transparency about the decisions of the referee - as far as we can ascertain, there *are* no decisions of the referee that we've been able to find; and in fact there's no provision for them to be public, so that makes sense. So there is a complete lack of transparency in this respect. But the legal test in respect of "frivolous and vexatious", I think, is not *irrelevant* in this context. 12:41 12:41 12:41

Then going on:

"*(4) If, after investigating the matter, the Referee concludes that a provision of section 6 has been contravened, the Referee shall –*
(a) notify the applicant in writing of that conclusion, and
(b) make a report of the Referee's findings to the

Taoiseach.

(5) In addition, in the circumstances specified in subsection (4), the Referee may, if he or she thinks fit" - so it's an unfettered discretion on the part of the referee - "*by order do either or both of the following –*
(a) direct the Garda Síochána, the Permanent Defence Force or the Revenue Commissioners to destroy the relevant data and any copies of the data,
(b) make a recommendation for the payment to the applicant of such sum by way of compensation as may be specified in the order.

(6) The Minister shall implement any recommendation...

(7) If, after investigating the matter, the Referee concludes that section 6 has not been contravened, the Referee shall notify the applicant in writing to that effect.

(8) A decision of the Referee under this section is final."

12:42

And the referee *is* given the power to access official documents or records. But I suppose what's important here is that a person can make a complaint and the referee then either will simply indicate to the applicant that there has not been a breach and no more,

12:42

and no requirement for reasons - that's under subsection 7 - or will indicate that there *has* been a breach - and that's under subsection 4 - and then, as a matter of discretion, may make a recommendation in relation to a sum of compensation and may direct destroying of the relevant data. But there's no requirement that the complainant be told about the destroying of the relevant data. And indeed there's simply a recommendation for the payment to the applicant of a sum by way of compensation; it's not clear -- I beg your pardon, I'm sorry, the following provision provides that the Minister shall implement any recommendation. 12:43 12:43

But if one is a complainant one, I suppose, gets something very like what one gets as a result of Ombudsman's procedure; one either simply gets a statement saying simply 'No', or else one gets a statement saying 'Yes, this has been found', but with the additional feature here that there may be compensation provided. So I think similar in many ways. 12:43 12:43

Judge, can I just move on then please to deal with the SCCs? And I know the court has looked at the SCCs on a number of occasions, but I simply want to ask the court just to consider one discrete issue. 12:44

MS. JUSTICE COSTELLO: Where shall I find them again?

MS. HYLAND: So the SCCs are in book 13, I think.

MS. JUSTICE COSTELLO: Is that the US authorities --
MR. GALLAGHER: The EU authorities. The very first book.
MS. HYLAND: Yes, exactly. So book 13, Judge. You have a number of book 13s, but it should be in the first -- 12:44
MS. JUSTICE COSTELLO: Well, except my was called "1".
MS. HYLAND: Oh, I see. I'm sorry, Judge.
MS. JUSTICE COSTELLO: I don't have a 13. Somebody's superstitious. 12:44
MS. HYLAND: Oh, I see. I'm so sorry, I didn't realise that. So I can give you the tab number then. Divide 10, Judge.
MS. JUSTICE COSTELLO: Thank you very much.
MS. HYLAND: Of the European materials. And what I only wanted to ask the court to look at, Judge, was just to think a little bit about the actual remedy that's available through the SCCs. Because we know what the Data Protection Directive says in relation to SCCs and we know what the DPC says as well in relation to the SCCs in her decision. And I suppose it's no harm just to remind the court what exactly was said by the DPC - I don't think I need to open it. 12:44 12:45

But essentially, at paragraph 61 she said that the safeguards constituted by the SCCs did not answer the CJEU's objections in **Schrems**; she said they did no more than establish a right of contract to a remedy against an importer or an exporter; they weren't binding on the 12:45

US Government; and there was no provision to access a remedy in the event that the data may be the subject of interference by a US public authority.

And I suppose there's a number of points you could make to that. First of all, the way it's expressed sounds as if an objection is being made to the subject of interference by a US public authority per se; in other words, the very fact that a US public authority can access the data is a cause for concern. But that is not, of course, the basis of what she ultimately found. What she ultimately found was there wasn't sufficient *remedies* in US law. And in that context, in our submission, it was imperative that the first thing she ought to have done was not look to US law, but to look to the SCCs to see what precisely a person was entitled to obtain by way of a remedy under the SCC, i.e. the contractual remedy, which is the primary purpose of the SCCs. And she made an assumption that the remedy had to be in the US. But in fact there is no basis upon which she should have concluded that a US remedy is necessarily what a data subject requires. A contractual remedy in the EU may be sufficient depending on the nature of the breach. 12:45 12:46 12:46 12:46 12:47

So if I could just ask the court to look to the annex to the SCCs, because that's where one sees these particular clauses that go into every single contract. And Ms. Cunnane has exhibited the contract in question

- and I won't open it, because it's the same, in the same format effectively as this document. But you do have that before you and that's the contract between the exporter and the importer, Facebook Ireland and Facebook US. 12:47

But the core provisions, Judge, that the court should look at, in my respectful submission, is Clause 3, 4 and 5 of the annex to the SCC decision, and that identifies the obligations of the data exporter and the 12:47
data importer. And essentially it's a clever, if you like, device, because what it does is it wraps around the protections of the country where the data comes from and it allows those protections to travel to whatever country they go to. That's the best way of 12:48
looking at it, as a wraparound protection. And if there's a breach of those protections that travel with the data then there's a remedy against the exporter.

And what's important about this and what's easy, I 12:48
think, to miss initially is that the protections are those which come from the country of the data exporter. So let's talk about Ireland in the particular case; when data is being transferred, with it go the *Irish* rules in respect of data protection. And if *those* 12:48
rules are breached by the importer, there's a remedy. So it's not that when one moves the data to the US, immediately one leaves behind the protections of Irish law.

And one see that from the wording of Clause 4 and 5. And if I could ask the court just to look at Clause 4, "Obligations of the Data Exporter":

"*The data exporter agrees and warrants:*
(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law."

And when one goes to the body of the SCC decision, in the definitions section in Article 3, one sees the definition of "applicable data protection law". And what that means is: 12:49

"*The legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established.*"

So that's the crucial part there. What legislation is being discussed there? It's legislation which is applicable to a data controller in the Member State in 12:49 which the *exporter* is established. So what we're talking about here is *Irish*, in this particular case, *Irish* law, because the data exporter is established in Ireland. And whatever legislation in Ireland is

applicable to the privacy rights, that's the legislation that is protected, if you like, by the SCCs. And that's the legislation that's at issue whenever there's a breach. So one doesn't leave behind the Irish protections when the data is transferred. 12:50

If one looks, going back then to the SCC, to the annex and in particular Clause 4, you'll see there that under (b):

"*It has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses.*"

So you've already seen, Judge, the definition of data, the applicable data protection law definition. And so what does the exporter do? The exporter is telling, 12:51 instructing the importer to process that data in accordance with, in this case, Irish law. That's the obligation.

Then you see a corresponding obligation at Clause 5 of 12:51 the importer. The importer agrees: "*To process the personal data only on behalf of the data exporter and in compliance with its instructions... if it cannot provide such compliance*" it has to inform promptly the

data exporter of its inability and then the exporter can suspend or terminate the contract.

Then more widely, I suppose - that's promising to comply with the instructions - but then in 5(b), more widely, the data importer is asked to consider the legislative context in which it operates. And it indicates that it has no reason to believe the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and, if there's a change in the legislation which is likely to have a substantial adverse effect, it will notify the change to the data exporter. 12:51 12:52

So the subject has the protection of knowing that when its data is transferred to another third country, the Irish protections will go with it. And if they are not observed and if there's a breach, whether it's because the exporter doesn't give the right instruction or whether it's because the importer doesn't abide by the instruction or sees another party not abiding by it and does nothing about it, doesn't tell the exporter, in that situation action may be brought under Clause 6. And Clause 6 identifies liability and sets out what the liability is. 6(1): 12:52 12:52

"*The parties agree that any data subject, who has suffered damage as a result of any breach of the*

obligations... is entitled to receive compensation from the data exporter for the damage suffered."

And it's worth noting that it's in the same, the wording is the same wording as in the Data Protection Directive, where there is a right to damages under, I think, Article 22. 12:53

If one, I suppose, thinks of a couple of factual scenarios, one can see, in my submission, why the Data Protection Commissioner ought to have considered the types of situations she was worried about in relation to the US and considered how the SCCs would respond to those situations and what kind of a remedy would've been given to the data subject. And I suppose if one thinks of a number of different examples. First of all, one can think of a simple type example where let's say there is incorrect data and the data importer doesn't remediate the data, let's say there's a mistake about somebody's personal data - we saw that in many of the US cases, but let's say it happens, the data is exported to the US, the importer is told by the subject that the data being held is incorrect and the importer doesn't take any steps; that's, if you like, a plain private law scenario and in that case there will be a remedy against the data exporter. Why the exporter? Because I've already said it's the importer who is doing -- is failing to take action, failing to remediate. The reason is because the SCCs give the 12:53 12:53 12:53 12:54

right of action against the exporter. And that's because it's easier for a data subject to sue the exporter in the country in which they're based.

So there's a remedy you have; you don't have to go to the US to sue, you don't have to worry about US law, you're simply allowed to identify the fact that there has been a breach of *Irish* data legislation. It's happened in the US, the importer is the person who has breached it, the importer has *not* carried out the instructions that were given by the exporter and there's a cause of action and a right of action for the subject in Ireland against the exporter, because the exporter steps into the shoes of the importer. 12:54 12:54

What then of a situation which is, I suppose, involving in some way a public body? For example, let us say there is a request to the importer in the US for material, let's say the US Government requires personal data to be provided and let's say there is no lawful authority, let's say the Directive under FISA is not properly executed or there is no Directive or something of that sort and the data importer doesn't check; in that case, what is the position in relation to a remedy? Because that's obviously a core issue in this case. Well, first of all what one must look to is the *Irish* law. Because as we know, the relevant law is the applicable data protection law as identified in Article 3 of the Directive. What does the applicable 12:55 12:55

data protection law say? One looks to Ireland to see what would be the position if, let's say in an Irish context, data had been given by Facebook to the law enforcement, to the guards without any authorisation being produced by the guards. And in my submission, because of the national security exemption, there's nothing *in* the Data Protection Directive about that type of situation. Because as I've already identified, under Section 1(4) of the Data Protection Act, national security is exempted. 12:56

So in fact there would not be a response from the national legislation in that, the applicable data protection law in an Irish context. And in those circumstances, there would equally not be a response in the US context. But not because of the transfer; because of the fact that the wraparound Irish provisions that go with the data transfer simply don't contain provisions designed to deal with national security measures. 12:57

MS. JUSTICE COSTELLO: But the Irish situation would apply to Irish national security.

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: So An Garda Síochána, for example. 12:57

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: But let's say it's the NSA.

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: Quite clearly, the NSA isn't

part of --
MS. HYLAND: Absolutely.
MS. JUSTICE COSTELLO: -- the exemptions under Irish law.
MS. HYLAND: Yes. 12:57
MS. JUSTICE COSTELLO: So can you tease that one out for me?
MS. HYLAND: Well, I think one still has to find --
MS. JUSTICE COSTELLO: Because it is an exemption. And don't exemptions have to be construed narrowly? 12:57
MS. HYLAND: Yes, that's true, Judge. But if one thinks that what one --
MS. JUSTICE COSTELLO: From derogation, whatever.
MS. HYLAND: Yes, that's absolutely right, Judge. But if one thinks that what one is being promised by the 12:57
SCCs is for your *Irish* law rights to go with you to the US and to give you a cause of action back in Ireland for whatever happens in the US, it's difficult to conceive why, if there *is* no Irish law right for that particular type of wrongdoing, why there should be any 12:57
redress in that situation against an act of a US body where a similar act by an Irish security service would not give rise to any cause of action in the Irish context.
MS. JUSTICE COSTELLO: So what you're saying, just to 12:58
take it out of this particular factual situation, if the data was surveilled, for example, by North Korea, that you wouldn't be able to sue here in Ireland? You know what I mean?

MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: What I'm saying is our exception is obviously based on *our* rule.
MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: In relation to *our* national security. 12:58
MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: It doesn't even, as far as I can see, apply to the UK. For example, the UK were quite happily surveying half of Europe, if Mr. Anderson's report is to be believed, and that apparently was legitimate and lawful. 12:58
MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: So I don't get your -- I know this is an important point. 12:58
MS. HYLAND: Absolutely, yes.
MS. JUSTICE COSTELLO: And maybe you might want to address it to me after lunch. But it is this analogy point...
MS. HYLAND: Yes. 12:58
MS. JUSTICE COSTELLO: ... which I do need some help with.
MS. HYLAND: Yes, of course. Judge, can I just ask, just in relation to the North Korean example, is the example whereby there is surveillance being carried on *in Ireland*, if you like, by North Korea or elsewhere? 12:59
MS. JUSTICE COSTELLO: No. No, the data has been transferred and it's been accessed by your North Koreans' security. One might not take a sanguine view

of that.

MS. HYLAND: Yes, yes. Very good, Judge, I'll reflect on that after lunch. At the moment I think the relevant test in the SCCs is the applicable data protection law. So one has to look to that for protection -- 12:59

MS. JUSTICE COSTELLO: Yes, I know you're looking at the data protection law. But it's the next step. You're saying clearly in Ireland, if it was performed by An Garda Síochána, you wouldn't have a remedy. 12:59

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: It's your next step, that you're saying it therefore, it follows that because it's the analogous, the analogue, if you like, to An Garda Síochána, that therefore you still don't have a remedy? 12:59

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: That's the bit I need a bit of help with.

MS. HYLAND: Very good. We'll look at that over lunch. Thank you, Judge. It's just one o'clock I see. 12:59

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: Thank you.

(LUNCHEON ADJOURNMENT) 13:00

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

MS. JUSTICE COSTELLO: Good afternoon.

REGISTRAR: Hearing resumed. 14:04

MS. JUSTICE COSTELLO: Before we resume, I should say that I had a word with the President at lunch. He's going to see whether a judge might be able to take over my commitments on Tuesday, so if you might relay that to, well obviously Mr. Murray, but to Mr. Collins if he 14:04 is dealing with it.

MR. MURRAY: Certainly, Judge.

MS. JUSTICE COSTELLO: And the rest of you for your diaries. Now I'll try to have, I won't have that confirmed, I don't think, until tomorrow. 14:04

MR. GALLAGHER: Thank you.

MS. HYLAND: Thank you, Judge. Judge, just before lunch you asked me about a situation, for example, if the data had been identified by a Member State, for example such as North Korea. Can I answer the 14:04 question, if you like, in two parts. I identified, the court knows that we have always identified the national security exemption.

MS. JUSTICE COSTELLO: Hmm.

MS. HYLAND: But Mr. Gallagher yesterday clearly set 14:04 out the fact that that primary position that we adopt was not adopted in **Schrems** and by the Commission in the Privacy Shield.

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: And that when one adopts the **Schrems** and the Commission approach you do have regard and you must have regard to the fact that the processing is conducted in a national security context and that you have Charter rights in that context if the interference goes beyond what is strictly necessary. 14:05

So, taking the **Schrems** approach, there is a remedy for a person whose data has been taken, let's say in North Korea, by the security services with the acquiescence of the importer. Because in that situation the interference has gone beyond what is strictly necessary, it's not justified. You are now into, if you like, the terrain where EU law *does* apply, there's been a breach of your Charter rights, and, if the importer has not taken steps in that regard, then there is liability back in Ireland on the exporter. Because the data, I think the phrase that I identified to the court is *"the applicable data protection law"*. 14:05

MS. JUSTICE COSTELLO: And that's the Charter then applying **Schrems**. 14:06

MS. HYLAND: Exactly, it's the Charter, exactly. On that basis, Judge, that means that irrespective, if you like, where your data goes, the applicable data protection law travels, the Charter travels with it and the test then is whether or not it has gone beyond what is strictly necessary or not. 14:06

MS. JUSTICE COSTELLO: Mm hmm. And does that rubric apply whether it's lawful in the third country, and I'm

not taking about the US at the moment.
MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: Because you could obviously have and I took the example on a previous occasion of Nazi Germany. 14:06
MS. HYLAND: Yes.
MS. JUSTICE COSTELLO: What might have been in accordance with law, such a régime, would not be regarded as compliant with the Charter.
MS. HYLAND: Yes. And that's what is so powerful, if you like, about the SCCs because they take the concept of the applicable data protection law. 14:06

Now, can I just identify 1.2, Judge, and that's at Clause 5, there's a footnote to Clause 5 and that goes to the very point that you have just asked me about; what is, if you like, the relevant margin in the State to which the data is being transferred. 14:06
MS. JUSTICE COSTELLO: Mm hmm.
MS. HYLAND: Clause 5, as you know, is in relation to the data importer and the data importer of course is in the third country. 14:07

And you'll see there that, after the heading *"obligations of the data importer"*, 1, there's a footnote and that footnote says: 14:07

"*Mandatory requirements of the national legislation applicable to the data importer which do not go beyond*

what is necessary in a democratic society on the basis of one of the interests."

And I'll just skip on just so the sentence makes sense.

MS. JUSTICE COSTELLO: Mm hmm. 14:07

MS. HYLAND: "*Are not in contradiction with the standard contract clauses."*

So there what we see is the SCCs identifying that certain legislation in third countries will be 14:07 acceptable provided they are still within the bounds of Article 13(1) - and they are the various different necessary measures to safeguard national security, defence, and so on - but, once one falls out of that, then that legislation is not considered to be protected 14:08 by Article 13(1). So that gives, if you like, some guidance to the national importer in respect of the legislation which is and is not acceptable.

MS. JUSTICE COSTELLO: And the flip side of that is if they do go beyond what is necessary. 14:08

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: Then you are in trouble.

MS. HYLAND: Exactly. And in fact if you look and see 5(b) in fact puts an obligation on the importer to look around it, as it were, at the legislation because it 14:08 has to agree and warrant that:

"*It has no reason to believe the legislation applicable to it prevents it from fulfilling the instructions*

received."

And its obligations under the contract. And if there's a change that's going to have a substantial adverse effect it has to notify the change to the exporter and the exporter is entitled to suspend or terminate. 14:08

So there is inbuilt protections which is if the importer decides that I'm now in a régime that is making it impossible for me to comply with the instructions that I was given by the data exporter, I must tell the data exporter that and they can suspend or terminate. 14:08

So the SCCs are cleverly balanced to consider the kind of situations and the kind of countries into which transfers will be made and to consider whether they do or they don't comply with the privacy rights and the steps that need to be taken and the remedies that are available depending on the situation. 14:09 14:09

The SCCs are not blind to privacy issues.

MS. JUSTICE COSTELLO: Mm hmm.

MS. HYLAND: And I think that can be seen quite clearly actually by the definition of *"applicable data protection law"*. Because, if we go back to that definition, you will see that the definition is: "*Legislation protecting the fundamental rights and freedom of individuals and, in particular, their right* 14:09

to privacy."

So the SCC is absolutely focussed on the issues of privacy and fundamental rights, even though it's in a contractual context, that is to the forefront of the drafter's mind. 14:09

So they are the protections, if you like, that are available vis-à-vis the exporter/importer and the individual data subject only has to sue in the Member State from which the data came. But then there is another very important protection and safeguard, and the court has already seen that, and that is Article 4(1) of the SCC itself, just below the definition of *"applicable data protection law"*. 14:10 14:10

And that is the provision that allows the national supervisory authority to stop the transfer where they are of the opinion that, according to the test under Article 4(1)(a) the law imposes obligations "*beyond the restrictions necessary in a democratic society*", again picking up the language. 14:10

MS. JUSTICE COSTELLO: That's going back to the footnote?

MS. HYLAND: Exactly, exactly. It's a perfect, as it were it is perfectly squared off. You have both the data importer looking at the law to which it is subject in the third country and then you have the ultimate protection which is the supervisor who can take action 14:10

if it is established that the law to which the data importer is subject goes beyond the necessary requirements.

And, Judge, you'll be aware that the wording of that has changed, and I just have one point to make about that shortly. But I suppose the curiosity about all this from our point of view is that the Data Protection Commissioner better than anybody understands the obligations of 4(1)(a) and the entitlements of 4(1)(a), they are not just obligations, they are entitlements the office has, because they are incumbent upon the office here, as in every other Member State. And, given that that safeguard was there, it's difficult to understand why the DPC arrived at the conclusion at paragraph 61 that the SCCs were of no assistance given the concerns about US law. 14:11 14:11 14:11

Because one would have thought that the necessary corollary of the expression of the concerns was that action ought to have been considered by her in respect of 4(1)(a) and/or she should have realised that the data importer and the data exporter had obligations under the SCCs. So the complete failure to engage in any way with the substance of the mechanisms set up by the SCCs, we say, is a signal failure on the part of the DPC. 14:11 14:12

MS. JUSTICE COSTELLO: Just teasing that out, and I know that this doesn't apply to the US but it applies

sort of in theory to all third countries. You took me through a whistle-stop tour in relation to EU laws, and I think we can probably - EU Member State laws.

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: We can probably assume that there would be a similar patchwork in *non*-EU countries. 14:12

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: And some of them would not have any legislation governing interception of data.

MS. HYLAND: Yes. 14:12

MS. JUSTICE COSTELLO: But this is dealing with legislation.

MS. HYLAND: Yes.

MS. JUSTICE COSTELLO: So is there a gap in a situation, let us say country A another, totalitaria, has no laws, just allows its security agencies to access data. 14:12

MS. HYLAND: Yes. Well, I think one way you could perhaps address that is by looking at the wording of 4(1)(a), *"imposes upon him requirements to derogate"*. Now if you are being told that the data in your possession will be taken by the security services, let's say without any legal basis, but, for example, in **Zakharov** one of the things that was required was that a device had to be put on the bearers in order to permit interception, so that was a given. 14:13 14:13

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: And it was known. And let us say the importer is in a similar situation where it knows that

a device is being put, placed by the security services on its network or its bearers; in that situation, in my submission, that would be a requirement there. It's not a requirement imposed by law because there is no law, but it is undoubtedly a requirement which is interfering. And in that situation, Judge, it seems to me that Clause 5(b) would oblige it to contact the exporter and notify the exporter of the requirements that are being imposed on it. 14:14

Now it is certainly true that 5(b) does make reference to the legislation applicable to it from fulfilling the instruction received, but I think the core point here is the obligation to comply with the instructions. Because, if you look at 5(a), you must process the data *"in compliance with its instructions"* and, "*if it cannot provide such compliance for whatever reasons*", it has to tell the exporter of its inability to comply, and that would arise in a situation where it is not being mandated by legislation but by practice. 14:14

MS. JUSTICE COSTELLO: I should re-emphasise, that is not what the evidence has adduced here, but it was just trying to help construe the document.

MS. HYLAND: Of course, absolutely, and it does help, I think, to identify theoretical examples. 14:15

Judge, just the last point on the SCCs before I move off them is just a very net point but I think it's one worth making. Tab 14, I think you have been at Tab 10

of the SCC document.

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: Then Tab 14 is this *new* decision of December 2016. It's just a small amendment to the SCC and what it does is it changes the wording of 4(1). And the reason it changes it is because you will remember in **Schrems** the court was concerned that the Safe Harbour Decision had sought to tell the supervisory authorities when they could and couldn't prevent data flows. The court in **Schrems** took the view that that wasn't something the Commission could do in an Adequacy Decision. 14:15 14:15

MS. JUSTICE COSTELLO: Hmm.

MS. HYLAND: And it took the view that because of that ruling in **Schrems** that 4(1)(a), which we have just looked at, which is very prescriptive about when a data supervisor can and can't suspend, was overprescriptive. And you will see now that the wording that has been substituted is a much broader wording and it gives the DPCs around the Member States a much greater level, I suppose, of autonomy in terms of deciding when they should and should not suspend or ban data flows. And the reason it's important here is because it shows that the Commission following **Schrems** had no concerns about the SCC decision apart from this one discrete concern; In other words, they have made the powers of the Data Protection Commissioners a little wider and less constrained. But, apart from that, **Schrems** did not give rise to concerns about the legality of the SCCs. 14:15 14:16 14:16

Because what you have here is the DPC telling the court that it thinks that SCCs are unlawful because of the way they operate in the US context.

On the other hand, you have the Commission making an amendment to the SCC decision, a very minor amendment, and not in any way throwing into doubt any other aspect of the SCC decision. 14:17

MS. JUSTICE COSTELLO: And this is post Privacy Shield, isn't it? 14:17

MS. HYLAND: Exactly. It is just December, it just happened this December.

MS. JUSTICE COSTELLO: Yes.

MS. HYLAND: So I suppose it's, we say it's an endorsement of the legality of the SCCs by the Commission and a demonstration that there is no aspect of **Schrems**, apart from that discrete area that I have identified, that raises any concern about the SCCs and in our submission it undermines the concerns of the DPC in that regard. 14:17

And, Judge, can I just finish by going back to a point I made very briefly yesterday and that's just in relation to Article 47. Article 47 obviously is a very important part of the Charter and I think 14:17 Ms. Barrington has already spent some time identifying for you how it plays out in the Member States and in particular how remedies are a matter for the Member States subject to the twin principles of effectiveness

and equivalence. So it's for the Member States to identify remedies in the case of a breach of EU law provided that those remedies are equivalent to the ones applicable for national law breaches and are effective.

14:18

But I think it is probably worth looking in that context at one of the most recent decisions of the Court of Justice on Article 47 and in particular in a context that I mentioned to you yesterday which is the supreme irony of it being asserted that EU - I beg your pardon, that US standing rules are inadequate, so inadequate as to make the SCCs unlawful in a situation where one of the big, I suppose, issues in EU procedural law over many years has been the inability of individuals to take direct challenges to the Court of Justice, the General Court and/or the Court of Justice.

14:18

14:18

You heard Mr. O'Dwyer talking about constitutional challenges and you heard him saying that one of the difficulties with US law was apparently that it wasn't possible for EU citizens to bring, if I may call them, constitutional challenges, i.e. challenges to the *legality* of surveillance legislation as opposed to their application. We say that's wrong anyway because of the APA, that was ignored completely. But even if one puts that aside for a moment, what is striking is that in the EU context an individual citizen effectively cannot challenge the legality of an EU

14:19

14:19

measure directly before the Court of Justice or the General Court. It has to be done in a way that's being sought to be done here whereby it comes to a national court and there is an application for a preliminary ruling. In fact that is obvious because otherwise presumably Mr. Schrems would not be here, he would be simply bringing his case directly in Luxembourg. 14:19

And that is a very, very significant standing obstacle. There's been a great deal of lobbying about it over the years, a great deal of academic writing, a great deal of case law, a lot of people challenging it, so much so that in the Lisbon Treaty there was a small amendment made to respond to those concerns. But in fact, when one sees the substance of that amendment and sees this case **Inuit**, it was a very modest amendment indeed and it did not fundamentally change the conditions in relation to standing. 14:19 14:20

So we say that in any analysis by the court of the adequacy of the standing rules in the US context the court cannot ignore the standing rules in the EU context for a similar type of challenge, i.e. a challenge to the legality of an instrument of EU law in this case or US law, a legislative type instrument. 14:20

MS. JUSTICE COSTELLO: But, like, Mr. Schrems effectively was able to challenge the Safe Harbour Decision.

MS. HYLAND: Again through the Irish courts.

MS. JUSTICE COSTELLO: Through the Irish courts.

MS. HYLAND: Yes, that's right.

MS. JUSTICE COSTELLO: And he got there. It may have been a convoluted route, is that not a legal structural point rather than a standing point? 14:21

MS. HYLAND: Well, I think it isn't, Judge. Because you see the case law, there is a lot of cases where people do look directly for direct access and the court rejects their claims on the basis that they don't have standing. For example, in the challenges to the 14:21 Privacy Shield, there is two challenges going on, both of those, we think, is likely that there will be standing challenges to, Digital Rights are one of the people who are challenging it. It's very like on the basis of the case law that there will be a challenge on 14:21 the basis of their standing to directly challenge Privacy Shield, that is a direct action.

And so the fact as to whether or not the preliminary reference procedure is an adequate way of dealing with 14:21 the access to the Court of Justice, many commentators, including a number of Advocate Generals, have indicated that it is not because it's not a direct route effectively. And I wonder could I just ask the court in this respect just to look at a short extract from a 14:21 textbook and a then case of **Inuit** and then I will finish on that, Judge.

This is Paul Craig of Craig & de Búrca, the court will

probably be familiar with that book. And if I could just ask the court to look at page 305 *"Access to Judicial Review Standing"* and then, just turning over the page, *"locus standi - the background"*:

14:22

"*The complex case law on standing to contest the legality of EU norms is well known. A brief outline is given here to set the scene for the discussion of more recent jurisprudence.*

14:22

Article 230 provided for direct review of legality. Member States, the European Parliament, Council, and Commission were regarded as privileged applicants and therefore had standing to challenge the legality of any acts. The Court of Auditors and the ECB could bring actions to protect their prerogatives. Non-privileged applicants had to satisfy 234, which provided that."

14:22

And then there was, the test was whether it was of *"direct and individual concern to the former"*.

14:22

"*Direct challenge to the legality of EU norms by non-privileged applicants has proved extreme difficult. The Plaumann test has remained authoritative even since the early 1960s. Persons other than those to whom a decision was addressed could only claim to be individually concerned if that decision affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are*

differentiated from all other persons, and by virtue of these factors distinguished them individually just as in the case of the person addressed. The applicant in the instant case failed because it practised a commercial activity that could be carried on by any 14:23
person at any time. This made little sense pragmatically, since the existing range of firms is established by the ordinary principles of supply and demand: if there are two or three firms in the industry they can satisfy the current market demand. The number 14:23
is unlikely to alter significantly, if at all. The ECJ's reasoning also rendered it impossible for an applicant to succeed except in a very limited category of retrospective cases. The applicant failed because the activity of clementine-importing could be carried 14:23
out by anyone at any time. It was however always open to the Court to contend that others could enter the industry and hence to deny standing to existing firms.

The difficulty of directly challenging EU norms in the 14:23
form of regulations was equally marked. The Calpak test required the non-privileged applicant to show that the measure in question was not a real regulation, but that it was in reality a decision of individual concern to him. This was not easy, because of the abstract 14:23
terminology test. The ECJ held that a real regulation was the measure that applied to objectively determined situations and produced level effects with regard to categories of persons described in a general and

abstract manner. The nature of the measure as a regulation was not called into question by the mere fact that it was possible to determine the number or even the identity of those affected. The Court recognised that the purpose of allowing such challenge 14:24
was to prevent the Union institutions from immunising matters from attack by the form of their classification. If regulations were never open to challenge the institutions could classify matters in this way, secure that private individuals could never 14:24
contest them. Article 230(4) sought to prevent this by permitting a challenge when the regulation was in reality a decision, which was of direct and individual concern to the applicant. This required, as acknowledged in Calpak, the Court to look behind the 14:24
form of the measure in order to determine whether in substance there really was a regulation or not. The problem with the abstract terminology test was that, rather than looking behind form to substance, it came very close to looking behind form to form. This was 14:24
because it was always possible to draft norms in the manner specified by the abstract terminology test and thus to immunise them from attack. This was especially so since the court made it clear that knowledge of the number or identity of those affected would not prevent 14:25
the norm being regarded as a true regulation.

*The **Codorniu** case raised hopes that the standing rules for direct challenge were being liberalised, but the*

decision proved to have a limited impact. The ECJ affirmed the abstract terminology test as the criterion for whether a regulation was a real regulation, rather than a decision, but held that this did not prevent the regulation from being of individual concern to some applicants. The test for whether an applicant was individually concerned was laid down in ***Plaumann****. It was for the applicant to show the contested provision affected him by reason of certain attributes which were peculiar to him, or by reason of circumstances in which he was differentiated from all other persons. The hope raised by* ***Codorniu*** *was dashed by the realisation that in most instances the* ***Plaumann*** *test would be interpreted in the same manner as in* ***Plaumann*** *itself. The fact that the applicant operated a trade, which could be engaged in by any other person served to deny individual concern. The fact that the applicant was the only firm affected by the contested measure did not suffice to afford standing. Nor were the EU courts willing to apply the more liberal case law from areas such as state aids, dumping, and competition to challenges outside those areas. If the Union courts felt an applicant should be regarded as individually concerned by a true regulation it required complex legal reasoning to square this with existing orthodoxy."* 14:25 14:25 14:25 14:25 14:26

Then, Judge, this is your point here, is the reference procedure a suitable substitute:

"Indirect challenge to contest the legality of EU norms was an imperfect substitute for more liberal standing rules for direct challenge. The narrow rules for standing in cases of direct challenge were often justified judicially by the existence of indirect challenge via Article 234 since the individual could get to the ECJ via the national courts. Advocate General Jacobs in ***Extramet*** *pointed out however the limits of indirect challenge. He noted that Article 230 contained no suggestion that the availability of annulment depended on the absence of an alternative means of redress in the national courts. Such a result would, in any event, have been far from satisfactory since the existence of any domestic remedy would depend on national law."* 14:26

And that's important there, remedies do come from national law.

"Advocate General Jacobs held furthermore that the indirect method of challenge had serious disadvantages by comparison with the direct action under 230. National courts lacked expertise in the subject and did not have the benefit of participation of the Council and the Commission. The proceedings in national courts, combined with a reference, could involve substantial delays and extra costs. The national courts had no jurisdiction to declare EU regulations invalid and this made it likely that interim measures 14:26 14:27

would be necessary in some cases, even though the national courts might not be the appropriate forum for granting such measures. There are in additional procedural difficulties attendant upon indirect challenge. This was because a reference from a national court on the validity of regulation did not always give the court as full an opportunity to investigate the matter as would a direct action against the adopting institution. The ECJ's general strategy was, however, to ignore the applicants' difficulties in using indirect challenge. Thus in ***Asocarne*** *the applicants argued that widespread structural delays in the Spanish judicial system should be taken into account when assessing standing for direct actions. The ECJ's response subsequently cited in many cases was unequivocal. Such circumstances could not alter the system of remedies provided by the Treaties, and could not justify direct action where the standing conditions were not satisfied."* 14:27 14:27 14:27

Then there's a reference to intervention and how intervention was also difficult.

Judge, can I take that up then to look at how the court dealt with this plea. Because in this case of **Inuit**, which Ms. Barrington opened, we see a plea that this - sorry, Judge, this was handed in to you a few days ago but I can hand in --

MS. JUSTICE COSTELLO: I'm not sure where, I don't

think I have those back with me, or maybe I do. Have we any idea where it is in the folders? Have you any idea where it is in the index?

MS. HYLAND: I am so sorry, Judge, my solicitor will just hand in a copy. 14:28

MS. JUSTICE COSTELLO: Well, no, I have the copy here, but it's a question of where it is in the index.

MS. HYLAND: Oh, I am so sorry. It is where it is in the index, yes. It should be, I would have thought, probably in Book 3 maybe, I'm just guessing by when it 14:28 was handed in. It was handed in...

MR. GALLAGHER: Tab 35, we think, Judge.

MS. HYLAND: Tab 35.

MS. JUSTICE COSTELLO: Yes, 45.

MR. GALLAGHER: Of the book. (Short pause) 14:28

MS. JUSTICE COSTELLO: Sorry, it's a blank.

MS. HYLAND: I'll hand in a copy.

MR. GALLAGHER: We're just getting it.

MS. HYLAND: Sorry, Judge, we're just going to hand in a copy there to the court. 14:29

Judge, this is a case about seal products and it had a very interesting group of applicants with all sorts of exotic names. But if I could just ask the court to take it up please at page 18. Because what the 14:30 applicants were saying - in fact page 17 I think is where it starts - effectively they were saying that the restrictions on direct access and of --

MR. GALLAGHER: It is 45, Judge, I am terribly sorry to

interrupt.

MS. JUSTICE COSTELLO: No, I have it but mine is blank. I have Tab 45 but I have nothing in it.

MR. GALLAGHER: Oh, I am terribly sorry.

MS. JUSTICE COSTELLO: Best laid plans, yes. 14:30

MR. GALLAGHER: Sorry.

MS. JUSTICE COSTELLO: I don't know what happened there, but anyway.

MS. HYLAND: What they were saying, Judge, was that the direct action restriction was in *breach* of Article 47, 14:30 so they were invoking the Charter, their right to a remedy to say that they ought to be allowed to bring these kind of direct actions, not a million miles in fact from what is being complained about in the US context, and it is interesting to see the short shrift 14:30 the court gave to that argument.

At paragraph 89 you will see the argument: "*The appellants claim that the interpretation adopted by the General Court of the fourth paragraph of Article 263 TFEU - they are the standing requirements - is in breach of Article 47 of the Charter in that it enables natural and legal persons to bring actions for annulment of European Union legislative acts solely where those acts are of direct and individual concern to them, within the meaning of the fourth paragraph.*" 14:30

And the court at paragraphs 90, 91 and 92, the court sets out its standard jurisprudence on the way in which

the system works.

And then at paragraph 93: "*Accordingly, natural or legal persons who cannot by reason of the conditions of admissibility stated in the fourth paragraph of Article 263 TFEU, challenge directly European Union acts of general application do have protection against the application to them of those acts. Where responsibility for the implementation of those acts lies with the European Union institutions, those persons are entitled to bring a direct action before the Courts of the European Union against the implementing measures. Where that implementation is a matter for the Member States, such persons may plead the invalidity of the European Union act at issue before the national courts and tribunals and cause the latter to request a preliminary ruling.*

94. It must be emphasised that in proceedings before national courts, individual parties have the right to challenge before the courts the legality of any decision." 14:32

So this is before the *national* court.

MS. JUSTICE COSTELLO: Hmm. 14:32

MS. HYLAND: And then, Judge, you will see paragraph 96 there is a reference to the reference procedure:

"*97. Having regard to the protection conferred by*

Article 47 of the Charter, it must be observed that that article is not intended to change the system of judicial review laid down by the Treaties - and this is the Article 47 part - and particularly the rules relating to the admissibility of direct actions brought 14:32
before the Courts of the European Union, as is apparent also from the Explanation on Article 47 of the Charter, which must be taken into consideration for the interpretation of the Charter.

14:32

98. Accordingly, the conditions of admissibility laid down in the fourth paragraph of 263 must be interpreted in the light of the fundamental right to effective judicial protection, but such an interpretation cannot have the effect of setting aside the conditions 14:32
expressly laid down in that Treaty."

And at paragraph 100: *"It is for the Member States to establish a system of legal remedies and procedures which ensure respect for the fundamental right to* 14:32
effective judicial protection."

So again the remedies piece is put back in the Member State responsibility.

14:33

And then, looking at paragraph 102, we see the twin principles of effectiveness and equivalence that I mentioned already. And at paragraph 103:

"As regards the remedies which Member States must provide, while the FEU Treaty has made it possible in a number of instances for natural and legal persons to bring a direct action, where appropriate, before the Courts of the European Union, neither the FEU Treaty nor Article 19 TEU intended to create new remedies before the national courts to ensure the observance of European Union law other than those already laid down by national law.

104. The position would be otherwise only if the structure of the domestic legal system concerned were such that there was no remedy making it possible, even indirectly, to ensure respect for the rights which individuals derive from European Union law, or again if 14:33
the sole means of access to a court was available to parties who were compelled to act unlawfully."

We say that's a really important paragraph. Because if you compare that with the conclusions of the DPC in 14:34
respect of remedies in the US setting, she did not come to a conclusion that there was *no* remedy making it possible, even indirectly, to ensure respect for the rights. Indeed she identified that there *were* remedies and they had flaws and they were fragmented, but they 14:34
existed, and she didn't address at all the indirect remedies. And you know, Judge, from our submissions that we say there are many different indirect ways of obtaining recognition of rights under the Charter,

oversight, through the review by FISC, and in particular through the companies who are the subject of the directives.

So we say that that's the test in EU law. It's only in 14:34
those circumstances where the court indicated that it would depart from the existing legal architecture and yet that was not the test imposed by the DPC.

Then finally at paragraph 105: "*As regards the* 14:35
appellants' argument that the interpretation adopted by the General Court of the concept of 'regulatory act', provided for in the fourth paragraph, creates a gap in judicial protection, and is incompatible with Article 47 in that its effect is that any legislative 14:35
act is virtually immune the judicial review."

Now this is the argument of the appellants and that's how it is characterised:

14:35

"*It must be stated that the protection conferred by Article 47 of the Charter does not require that an individual should have an unconditional entitlement to bring an action for annulment of European Union legislative acts directly before the courts of the* 14:35
European Union."

And that's why I say they gave short shrift to the argument, despite the existence of Article 47, an

individual is not entitled to go directly to the courts of the European Union.

Judge, there is just two points as I finish. Mr. Gallagher reminds me correctly that of course in respect of constitutional type challenges, because of the Fourth Amendment individuals cannot bring, even with the help of the APA, and I said earlier on that they could and that was wrong. But of course the companies who are the subject of the directives can bring those challenges such as in **ACLU -v- Clapper**. 14:36 14:36

And then there was two other points. The first, Judge, in relation to the notification. There is uncontested evidence by Mr. DeLong and Prof. Swire in relation to the hostile actors and why notification presents problems, that hasn't been contested. Judge, if the court, contrary to all of the submissions we have made considers that a reference ought to be made, and we would obviously welcome an opportunity to be heard on the questions, and similarly in that context it would be very important to have a comprehensive record of the facts relevant to the issue, but we would hope that that won't arise and if it does arise that those issues would be for another day. May it please the court. 14:36 14:36

MS. JUSTICE COSTELLO: Thank you. Mr. McCullough?

SUBMISSION BY MR. McCULLOUGH:

MR. McCULLOUGH: We have prepared a speaking note, Judge, which I will ask Mr. Rudden to distribute. I hope it will be of assistance to the court in two ways: One in following the structure of what I am saying, Judge, but also it contains references in the footnotes to where the authorities are to be found and tries to quote from those authorities and from evidence where that will be helpful and that, I hope, will be of some assistance to the court and avoid it having to go back to the original sources. It may not be, Judge, but I hope it will. 14:37 14:37

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: There are two basic points that I want to make, Judge, and the first is one that was the subject matter of what I said when I was opening our case, Judge. We contend, Judge, there's no basis for a reference. The matters that form the subject matter of Mr. Schrems' complaint haven't been investigated. 14:37 14:38

Article 4 in particular forms a safety valve that the DPC ought to make use of under the circumstances that have arisen here. That's the first broad point, Judge. 14:38

The second is this: That we agree with the DPC that US law doesn't provide adequate protection for the rights of EU citizens and we add that that's true, not just of remedies, but also of substantive US law. The DPC has

concentrated on the former, but we say that her overall conclusion is equally true of the latter.

We say that all of that, Judge, should of course properly have led to the exercise of Article 4 powers under the SCC decisions itself, but that, if we are wrong about that, well then the SCC decisions are necessarily invalid. 14:39

If I can turn to the note, Judge, it deals first with the reformulated complaint, and the court will find that at Core Book 1 Tab 14. 14:39

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: And I hope not to go, not to have to go back over that, Judge, if the court can take what I say now in conjunction with what I said when I was opening the case. 14:39

MS. JUSTICE COSTELLO: No, no, I re-read yesterday.

MR. McCULLOUGH: Thank you, Judge. So there are three substantive issues that were raised in the reformulated complaint. 14:39

The first was the central issue which was a contention that Facebook's contract, described as the DTPA, simply doesn't comply with the relevant SCC decision, and I gave the court details of why that is so or why that was said by Mr. Schrems to be so. The court will recall that at the time that he made the complaint he had access only to a redacted version of the DTPA. The 14:39

court has subsequently had the opportunity to see an unredacted version. And his basic complaint was simply that the DTPA is not in compliance with the SCC decisions. It's a noteworthy feature of the complaint that it doesn't in fact impugn the validity of the SCC decisions themselves at all, it makes at its centre this basic starting point. 14:40

The second issue raised in the reformulated complaint was the additional means, beyond the SCC decision, by which Facebook transfers data to the US. The court is familiar with the fact that Article 26(1) in particular provides for a range of other possibilities. Article 26(2) deals with standard contractual clauses, Article 26(1) deals with other derogations. 14:40 14:41

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: And in particular there's consent, there's transfer for the performance of a contract. Mr. Schrems made it clear in his reformulated complaint that he was at an overall level complaining that his data was being transferred in breach of his rights under the Directive and the Charter. He made it clear that, as it happens, he knew that the SCC decisions were being relied upon, but it is perfectly clear from his complaint that he wasn't limiting his complaint to that, he was asking the DPC to investigate all of the means by which Facebook transfers data to the US. 14:41 14:41

And then the third point that was raised, Judge, was

this: That if the DTPA was in conformity with the SCC decision, the DPC ought nevertheless to exercise her powers under Article 4 of the SCC decision and suspend transfer of data by Facebook Ireland to Facebook Inc. And that was said, Judge, because, I'll come in a little more detail to Article 4, but that was said in the reformulated complaint to arise precisely because Article 4 is inserted in the SCC decisions for that purpose, to allow the DPC to exercise powers to suspend data transfer under circumstances where it comes clear to her that data in the US is not being treated in accordance with the rights of EU citizens. 14:42 14:42

So I just pause that and I'll come back to Article 4 in a moment. You see from the speaking note, Judge, the next issue we raise is the general one of when a reference can be made. And we refer there, Judge, to the TFEU itself and Article 267 and that provides, as the court can see in the footnote: 14:42

14:43

"*Where such a question is raised before any court or tribunal of a Member State, that court or tribunal may, if it considers that a decision on the question is necessary to enable it to give judgment, request the court to give a ruling thereon.*" 14:43

That's the fundamental rule, Judge, that a court will make a reference under circumstances where it is necessary to do so. So if the national court can

decide the question without reference to the issue of EU law that is said to arise in the case it will do so and it will only make a reference where it requires an answer to that question in order to enable it to answer the question. 14:43

Another part of that, Judge, which was mentioned yesterday by Mr. Gallagher, I think, that's the **Gasparini** case, which again is also mentioned in footnote 5, Judge, which provides that the court won't deal with hypothetical questions. Again it's part of the same picture. The court will only deal with questions where it is necessary for it to answer the question and, equally, it won't deal with moot questions. 14:43 14:44

MS. JUSTICE COSTELLO: But obviously there is the issue in this case that the only question I have been asked to do is make a reference.

MR. McCULLOUGH: Yes.

MS. JUSTICE COSTELLO: And you made the submission when you had your opening statement that they couldn't sort of narrowly craft the case that so you rule it out. 14:44

MR. McCULLOUGH: Exactly.

MS. JUSTICE COSTELLO: So that's the only thing that could be dealt with. So what I am concerned about, and you can help me with, is, if you are correct and you say 'they can't just whittle it down in this way, they have to then look at Mr. Schrems' complaint'. 14:44

MR. McCULLOUGH: Yes.

MS. JUSTICE COSTELLO: And I am looking at Mr. Schrems' complaint and what was required to deal with Mr. Schrems' complaint; the DPC, there's a huge emphasis on her independence and her independent role.

MR. McCULLOUGH: Yes. 14:44

MS. JUSTICE COSTELLO: Where's the borderline between me overstepping that role and her conducting, if she says 'this is the way I am conducting my investigation and this is what I need'.

MR. McCULLOUGH: Yes. 14:45

MS. JUSTICE COSTELLO: It may look to me as if I think you are barking up the wrong tree, for argument sake, but am I allowed to interfere with her independence by dealing with it?

MR. McCULLOUGH: Yes, I think the court must be. The court will of course have due respect for the independence of the DPC, but ultimately the issue here is or the issues here are the questions that arise in Mr. Schrems' reformulated complaint. Those are the issues that require to be investigated. As I submitted 14:45 to the court before, the DPC can't make a reference necessary simply by selecting a question, presenting to the court and saying 'hey presto it is now necessary to refer that question'. That's circular and self-probative, Judge. The question has to be this: 14:45 Is it necessary for the DPC to refer this question to the Court of Justice in order to decide the reformulated complaint. And the court must look at that and I don't think the court can avoid doing so

simply by reference to its respect for the role of the DPC. So the court, I think, must look at the complaint and must form its own view as to whether in fact the DPC is correct in suggesting that a reference is necessary in order to enable her to complete her task. 14:46

In some cases, Judge, that might be a difficult task, but in this case I respectfully suggest not. The three issues that I have said lie at the heart of the Mr. Schrems' complaint are actually just not addressed 14:46 in the Draft Decision. So there is in fact no analysis, just no analysis of the question of whether the DTPA is in conformity with the SCCs. There is *no* analysis of other means of transfer. The only reference to that in the draft determination is a 14:46 statement in the single paragraph in strand 1 where the DPC says that that is a means that Facebook uses, and there's no reference at all to Article 4 and no explanation of why Article 4 is isn't suitable.

14:46

So in a sense it's an easy enough task in my respectful submission for the court here. Those issues that clearly do lie at the heart of Mr. Schrems' complaint are simply not addressed.

14:47

It was also suggested, Judge, and we deal with this at paragraph 3 of the speaking note, that paragraph 65 of **Schrems 1** conferred a right on the DPC to bring this matter before the court and then created an obligation

on the court to refer if it shared the doubts of the DPC.

Paragraph 65, Judge, is set out in the footnote.

MS. JUSTICE COSTELLO: Mm hmm. 14:47

MR. McCULLOUGH: And you will see, Judge, it is set out in the context of paragraph 63. Paragraph 63 provides:

"*Having regard to the those considerations, where a person whose personal data has been or could be* 14:47
transferred to a third country, has been the subject of a Commission decision pursuant to Article 25(6) lodges with the DPC a claim concerning the protections of his rights and freedoms in contrast to the processing of that data and contests, in bringing the claim, as in 14:48
the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the DPC to examine the claim with all due diligence." 14:48

So it is Mr. Schrems' complaint, the complainant's complaint that is examined by the DPC. Then paragraph 65 provides in relevant part: 14:48

"*Where the DPC 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,*

the DPC must be able to engage in legal proceedings."

But what the DPC brings before the court, Judge, is not, if you like, something that is free standing and arises separately from the complaint, the DPC must consider whether the objections that are advanced by the person who makes the complaint are well founded. And Mr. Schrems' fundamental problem here, Judge, is that just hasn't been done. 14:48

Paragraph 65, Judge, doesn't go beyond the general rule of Article 267 of the TFEU, doesn't give right to a freestanding obligation to refer. It simply clarifies the circumstances in which, in this particular context, the context of the DPC, a claim is brought from her to the court to the CJEU, but it doesn't, as I say, change the basic ground rules of necessity. 14:49

Can I add this, Judge, to the three points that I made before, and I think I mentioned this in opening the case: That the making of a reference is also premature on a different ground, Judge, and that's on the basis that it is in draft form only and explicitly subject to further submissions. That statement, Judge, is to be found the various places of the Draft Decision, if the court could just turn to that for a moment. You'll find it, Judge, at Core Book 1 Tab 18. 14:49 14:49

Just to bring the court to some examples of the wording

of the DPC on which she makes it clear that this is a preliminary view only and doesn't in fact represent her final conclusion on the facts. If the court looks at page 2 paragraph 1(b):

14:50

"*While my investigation remains ongoing, I have formed the view, on a draft basis, and pending receipt of such further submissions as the complainant and/or FB-I may wish to submit, that a legal remedy compatible with Article 47 of the Charter is not available.*" 14:50

Down the bottom of that paragraph: "*Against that backdrop, I consider that the SCC Decisions (as defined below) are likely to offend against Article 47 of the Charter insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US notwithstanding the absence of any possibility for any such citizen to pursue legal remedies effective in the US.*"

14:51

And then: "*I emphasise again that this view has been reached on a provisional basis and this view, when articulated herein, is to be regarded as subject to receipt of such further submissions as the complainant and/or FB-I may wish to make.*" 14:51

And that language, Judge, is to be found throughout the draft determination, if the court turns forward to page 19.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: Paragraph 43, similar language. The DPC says that what appears to her to be the position on the current stage of her investigation and subject to such further submissions as may be made. 14:51

You'll find it again, Judge, on page 29 paragraph 60: "*For all the reasons outlined above, therefore, I have formed the view, subject to consideration of such submissions as may be submitted in due course by the* 14:51 *complainant and FB-I that, at least on the question of redress, the objections raised by the CJEU in its judgment in* ***Schrems*** *have not yet been answered.*"

So it is expressly, Judge, a determination that is 14:52 reached on the basis of an incomplete analysis of the factual background. And it is hard to see, Judge, how a reference can be said to be necessary by the DPC under circumstances where she herself says 'well I don't think actually know the full state of the facts 14:52 here'.

So just to look, Judge, then, we address this at paragraph 6 of the speaking note, on the three issues that we raised. I think the fact is, Judge, that that 14:52 issue simply hasn't been investigated. And we say, Judge, that a reference can't be said to be necessary unless and until it *has* been investigated.

Just to take the most obvious example, Judge, the most obvious possible outcome: The DPC investigates the basis of the complaint made by Mr. Schrems and determines that indeed, in accordance with what he says, the DTPA is not in accordance with the draft decisions, well then those data transfers are not permitted to continue. And there can be no basis under those circumstances for referring a question as to the validity of the decision under which they are transferred to the Court of Justice, it simply wouldn't arise as a necessary question. A far smaller more discrete more particular question would have been asked and answered which would relate to this particular company only. 14:53 14:53

And the same applies, Judge, in relation to the second ground: Unless and until the DPC investigates all of the basis upon which transfers take place, it follows that others may be relied upon. And it follows, therefore, Judge, in the same way that a reference is premature and, in my respectful submission, unnecessary unless and until that matter is investigated. 14:54

MS. JUSTICE COSTELLO: The question I was probably very incoherently putting to Mr. Gallagher yesterday --

MR. McCULLOUGH: Yes. 14:54

MS. JUSTICE COSTELLO: -- in the light of the Privacy Shield decision aren't they entitled to transfer data under Privacy Shield regardless of the SCC?

MR. McCULLOUGH: Well...

MS. JUSTICE COSTELLO: They may de facto say that they have been transferring it in accordance with their agreement which they say is pursuant to an SCC decision.

MR. McCULLOUGH: Yes. I'm not sure that he actually has said, Judge, that Facebook's intention would be to transfer all of their data. 14:54

MS. JUSTICE COSTELLO: No, he didn't say it was intention, I just sort of said, asked him, spinning forward, were they authorised to do so if the SCCs ultimately were to be struck down. 14:54

MR. McCULLOUGH: And skipping forward, Judge, the court will find this issue addressed at paragraph 53 onwards.

MS. JUSTICE COSTELLO: Well, okay. I'll let you deal with it in your own way. 14:54

MR. McCULLOUGH: No, but I'll address it now, Judge, because it arises now. The Privacy Shield, Judge, is a self-certifying process.

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: You can take advantage of Privacy Shield only if and to the extent to which you are willing to sign up to its principles. There is no evidence on what actually - there is no evidence on either of two points, Judge: Either what Facebook does in relation to Privacy Shield, does it actually take advantage of Privacy Shield at this stage and, if so, to what extent, still less is there any evidence on its intentions for the future. 14:55 14:55

So I don't think the court can simply assume that if the SCC decisions come before the Court of Justice, and the SCC decision is found to be invalid, that Facebook will say, will turn around and say 'well it doesn't matter in any event because we intend to use Privacy Shield', and the same applies to the exercise by the DPC of Article 4. I don't think the court can conclude that, if the DPC exercises her powers under Article 4 of the SCC decisions and prevented data flow to the US on the basis of those powers -- 14:55 14:56

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: -- that Facebook again would turn around and say 'well it doesn't matter because we intend to use Privacy Shield anyway'. The Privacy Shield issue remains in this case largely unexplored save in this one respect only, that Facebook relies upon Privacy Shield Adequacy Decision, and I'll come to that point, Judge. In my respectful submission that decision is not actually helpful or of any particular guidance to the court in this context. 14:56 14:56

So I don't think the court can make any conclusion as to what would happen.

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: If the court's concern is that this might be, if you like, something of a waste of time if a reference was to be made, or if the matter was to be sent back to the DPC, as we contend, with a direction for her to consider the points that are raised by 14:56

Mr. Schrems, I don't think the court can conclude any of that would be a waste of time.

It is certainly the case, Judge, that we know this from the draft determination: That Facebook transfers data to the US largely on the basis of the SCC decisions and that appears to be the position as we speak before the court at the moment. It was certainly the position as of the time of the DPC's investigation. 14:57

Just turning back, Judge, to, I suppose, the consequences of the DPC's failure to investigate the Article 4 point. The same applies there, Judge. If the court comes to the conclusion that the proper interpretation of the SCC decision itself is that the DPC should exercise her Article 4 powers if she is of the state of mind that she is, well then it must follow that a reference to the court as to the validity of the SCC decisions is unnecessary; in other words, if the same result can be achieved, an order whereby Mr. Schrems' data is not transferred to the US by the use of Article 4, it doesn't require the Court of Justice to consider whether the SCC decisions themselves are invalid. 14:57 14:57

So the whole Article 4 question, Judge, is one has to be determined, it's to be considered and determined by the DPC in advance of there being any question in my respectful submission of a reference being necessary. 14:58

Turning, Judge, to, this is the top of page 4, if I continue using the speaking note which I hope is helpful. We make the point, Judge, that the provisions of Article 4 reflect wider Union and Member State law of providing for rights of suspension. It might be helpful if I just remind the court of where you'll find that material.

It's in the Directive, Judge, which you'll find at the book of EU authorities Tab 4 (short pause) in Article 28 sub-Article 3. In dealing with the supervisory authority it is provided at sub-Article 3 that: 14:58

"*Each authority shall be in particular be endowed with.*" 14:59

Then turning to the second indent: "*Effective powers of intervention, such as*" and then skipping a few of those: "*Ordering the blocking, erasure or destruction of data or imposing a temporary or definitive ban on processing.*" 14:59

So that's, if you like, the broader origin of the powers. That's reflected, Judge, in the Irish Act which you'll find in the EU book of authorities, the second book, at Tab 17. This is a consolidated version of the Act, Judge, but if you look at page 48 you see section 11. 15:00

MS. JUSTICE COSTELLO: Yes.

MR. McCULLOUGH: And subsection 1. Section 11, subsection 1, Judge, at page 48 sets out the governing rule, the governing *national* rule for this case:

"*The transfer of personal data to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer.*"

It sets out matters to be considered. But if you turn in particular to subsection 7 on page 50, that provides: 15:01

"*The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from the State to a place outside the State unless such transfer is required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on the State.*"

And that's the national law reflection of Article 28. And in our respectful submission, Judge, when the DPC decided that the transfer breached Mr. Schrems' rights as an EU citizen, the proper response, as a matter of

EU law, was to invoke Article 4. Now, that, I think, follows from the structure of the draft decision itself, to which I'll turn in a moment. It's just, with respect, Judge, illogical to seek to invalidate a Commission decision on the grounds that it doesn't adequately protect the rights of EU citizens, under circumstances where it contains a clause specifically *entitling* the DPC to make an order which protects the very *same* rights that she says invalidate it. 15:02

15:03

I think I gave the court an example before, Judge, of a statute that provided for the protection, say, of the rights of confidentiality and it contained a section within it providing for a judge to grant an injunction to restrain a breach of the rights of confidentiality. 15:03
It would be an odd action, Judge, to seek to strike down that statute on some constitutional ground that it failed adequately to protect confidentiality when it contained within it a section giving the judge the power to make an order to enforce the very rights that 15:03
were said in that action to make it unconstitutional. It's an illogicality, Judge, as I respectfully submit, and indeed as others have submitted. Article 4 is inserted in the decision *precisely* for the purpose of enabling the DPC to exercise it in a case of this 15:04
nature.

Can I turn then, Judge, to the decision itself? And the court will find that at book one of the EU material,

tab ten.

MS. JUSTICE COSTELLO: Oh, that decision? I thought you meant the DPC's decision.

MR. McCULLOUGH: Oh, I'm sorry. My apologies, Judge, I mean the... 15:04

MS. JUSTICE COSTELLO: The SCC decision?

MR. McCULLOUGH: The SCC decision.

MS. JUSTICE COSTELLO: Book one, isn't it?

MR. McCULLOUGH: Yes, Judge.

MR. GALLAGHER: Divide ten, Judge. 15:04

MR. McCULLOUGH: Divide ten, Judge. Thank you.

MS. JUSTICE COSTELLO: Thank you.

MR. McCULLOUGH: I'll deal with Article 4 now, Judge, and while I have it open, I'll deal with the point that Ms. Hyland was discussing just before lunch with the court. 15:05

So this is the version of the SCC decision that was in place at the time that the complaint was made - and as the court's aware, it's subsequently been altered. And Article 4 provides that: 15:05

"*Without prejudice to their powers to take action to ensure compliance with national provisions... 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 of their personal data in cases where:*

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13... where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses."

And I'll come back to that, Judge, and I'll say why that was applicable in the circumstances. But it breaks down into two: First, it must be established that the data importer or sub-processor has requirements imposed upon him which derogate from the 15:06
applicable data protection law - that's EU data protection law - which go beyond the restrictions necessary in a democratic society as provided for in Article 13; and secondly, those requirements are likely to have a substantial adverse effect on the guarantees 15:06
provided by the data protection law and the clauses themselves.

(b) is:

"*A competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or*

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects."

And perhaps just keeping that open, Judge, for a moment, if I may turn to the DPC's draft decision and demonstrate why, in my respectful submission, Article 4(1)(a) was engaged. The court will find the relevant extracts from the draft determination set out at footnote 11 of the speaking note, Judge, and perhaps it's just as useful to look at it there, Judge. 15:06

MS. JUSTICE COSTELLO: Very good, yes. Save on the folders. 15:07

MR. McCULLOUGH: Yes. So particular reference is made to paragraph 43 and then paragraphs 60 to 62 of the draft determination. At paragraph 43 the DPC concluded that: "*It remains the case that, even now*" --

MS. JUSTICE COSTELLO: I'm sorry, what page on your speaking note are you? 15:07

MR. McCULLOUGH: Sorry, Judge, footnote 11.

MS. JUSTICE COSTELLO: Oh, yes. Thank you.

MR. McCULLOUGH: Which sets out relevant extracts from the draft determination. Paragraph 43 of the DPC's draft determination says: 15:07

"*It remains the case that, even now, a legal remedy compatible with Article 47 of the Charter is not*

available in the US to EU citizens whose data is transferred to the US where it may be at risk of being accessed and processed by US State agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter."

Then paragraphs 60 to 62, Judge, are perhaps the most importance ones, these are her conclusions. She says:

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

61. It is also my view that the safeguards purportedly... set out in the Annexes to the SCC Decisions do not address the CJEU's objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in Schrems. Nor could they... So far as the question of access to an effective remedy is concerned, it is my view that they cannot be said to ensure adequate safeguards for the protection of the privacy and fundamental rights and freedoms of EU citizens whose data is transferred to the US.

62. Accordingly, I consider that the SCC Decisions are

likely to offend against Article 47 of the Charter insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US in the absence in many cases of any possibility for any such citizen to pursue effective legal remedies in the US in the event of any contravention by a US public authority of their rights under Articles 7 and/or 8 of the Charter."

And just bearing those findings in mind, Judge, if you glance back at Article 4(1)(a). So the first question to be answered under 4(1)(a) is: Does the US law impose requirements which go beyond the restrictions necessary in a democratic society? And that's in fact *precisely* what the DPC finds when she says that the SCC decisions are likely to offend against Article 47 of the Charter. 15:09 15:09

MS. JUSTICE COSTELLO: Well, isn't that dealing with remedies rather than substantive law?

MR. McCULLOUGH: It is, Judge. Because that's what the DPC concentrated on. 15:09

MS. JUSTICE COSTELLO: Yes, exactly, she concentrated -- but I'm just wondering, looking at Article 4, is that dealing with substantive law or remedies or both?

MR. McCULLOUGH: Oh, both, Judge. I think, yeah, it's dealing with the provisions of EU law. 15:10

MS. JUSTICE COSTELLO: I'm just looking at it, just parsing it. "*It is established that the law to which the data importer or sub-processor is subject imposes on* him" - I presume that means the data importer or

sub-processor?
MR. McCULLOUGH: Yes, Judge. Or sub-processor.
MS. JUSTICE COSTELLO: "*Requirements to derogate.*" So that would be they would have to release data or make data available to one of the intelligence agencies in the US. 15:10
MR. McCULLOUGH: Yes.
MS. JUSTICE COSTELLO: Now, they're not concerned with remedies as such, the controllers.
MR. McCULLOUGH: No. But what the Directive governs, Judge, is the transfer of data. And it governs the circumstances under which data may be transferred. 15:10
MS. JUSTICE COSTELLO: Mm hmm.
MR. McCULLOUGH: So it's the transfer and then the release of data under circumstances in which there is not an adequate remedy for breaches of the rights of EU citizens. So -- 15:10
MS. JUSTICE COSTELLO: Yes, what I'm trying to focus on, I guess, is trying to work out (A) whether it's the *substantive* law, or whether it's breaches of the substantive law and whether it's a control on the US Government. I'm just trying to work it all into this, this Article 4. Because I understand obviously the objection - SCCs are only being relied on in circumstances where the domestic law of the third country, or "the problem". 15:11
MR. McCULLOUGH: Yes.
MS. JUSTICE COSTELLO: But what we're looking at here is "*It is established that the law*" - that's the 15:11

domestic law of the third country.
MR. McCULLOUGH: Yes
MS. JUSTICE COSTELLO: "*To which the data importer or sub-processor is subject imposes upon the data importer or sub-processor a requirement to derogate from the applicable data protection law*" - and that's either Irish law or Irish law and/or EU law, we'll... 15:11
MR. McCULLOUGH: Yes. Well --
MS. JUSTICE COSTELLO: Depending on various submissions. Some people have said Irish law, you've said EU law. 15:11
MR. McCULLOUGH: Well, it *is* Irish law, Judge. But Irish law must comply with EU law.
MS. JUSTICE COSTELLO: Yes, includes in the -- and with Charter and all that. 15:12
MR. McCULLOUGH: So I don't, if I may say parenthetically, I don't accept at all Facebook's submission that we can look at national law and say 'Well, as it happens, it doesn't meet EU standards'. The standards to which EU citizens are *entitled* are those for which the Directive and the Charter provides. 15:12
MS. JUSTICE COSTELLO: Establishes, yes. But it's derogating from the restrictions, which go beyond restrictions necessary in a democratic society. So is the first part of that dealing with, if you like, the taking, the processing, as opposed to the remedies? 15:12
MR. McCULLOUGH: Well, I don't think so, Judge. I think when we look at -- I suppose, Judge, looking at it on an overall basis, the purpose of the Directive,

or the relevant part of the Directive I should say, Article 25 and Article 26 -- perhaps if we just turn to them, Judge, it's useful to see it in context as well. And you'll find those, Judge, at --

MS. JUSTICE COSTELLO: I have them marked, thanks. 15:13

MR. McCULLOUGH: Thank you, Judge. So the purpose of, the overall purpose, Judge, under transfer of personal data to third countries. The Member States shall ensure - this is Article 25:

"*That the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.*"

So that's the point here of the relevant part of the Directive, is to ensure that there is, if you like, a 15:13 safe space, it has to stay within the EU. You can send it to a third country, but only *if* in that third country you have adequate levels of protection, which, in my submission, means the same level of protection as that to which you'd be entitled in the EU. And I'll 15:13 come to why I say that in due course.

Then if we go back, Judge, then to 4(1)(a). So the question is whether it's established that US law, in

this case, imposes upon the importer or sub-processor requirements to derogate from the applicable data protection law. So that's requirements to derogate from EU law, which, if you like, result in an inadequate level of protection. 15:14

MS. JUSTICE COSTELLO: But by definition they aren't going to be providing remedies in courts, they're obviously going to be providing -- well, I suppose they could be sued, if you're talking about under the clauses under this... 15:14

MR. McCULLOUGH: They could undoubtedly be sued, Judge. But the point, I think, here is that when data is transferred, it must be transferred only in circumstances in which there is the same level of protection for that data as obtains under EU law. 15:14

MS. JUSTICE COSTELLO: Hmm.

MR. McCULLOUGH: So what Article 4(1)(a) means; that if requirements are imposed by derogate from that, in other words which require the release of data --

MS. JUSTICE COSTELLO: No, I understand that, that they have to -- I understand your overall point, that it has to have the same sort of bubble of protection. 15:15

MR. McCULLOUGH: Yes.

MS. JUSTICE COSTELLO: I think somebody used that image before. But I'm asking you really is that referring to the overall substantive law, domestic law? 15:15

MR. McCULLOUGH: It's referring to both, I think, Judge. Just to bring it in the context of remedies, the transfer of data is permitted only if US law

ensures that it can't be released unless released under conditions that are effectively equivalent to EU law. And that includes both substance and remedies.

So a requirement to derogate, in the US context, is a requirement to release or a requirement to allow surveillance under circumstances where there is not an adequate remedy for those whose data is surveilled. And that's the requirement, Judge, and that's a requirement that goes beyond a restriction that is necessary in a democratic society. 15:15 15:16

The restriction is the restriction on the ordinary rights of data subjects. If you want to compare EU law to US law, there's no restriction similar to the standing difficulties that apply in the US. There *are* those restrictions in the US. And that means that the release is then subject to restrictions which go beyond those that would apply in EU law. So in my respectful submission, Judge, it must apply both to Articles 7 and 8, but also to Article 47, which is the remedies part of the Charter. 15:16 15:16

I was dealing, Judge, with the second part of Article 4(1)(a). 15:17

MS. JUSTICE COSTELLO: Yes.

MR. McCULLOUGH: So in my respectful submission, what the DPC found, Judge, amounts to a finding that the requirements of US law imposed upon -- sorry, that US

law imposed upon the data processors, the data importers and processors requirements to derogate from the applicable data protection law which go beyond the requirements necessary. And are those requirements likely to have a substantial adverse effect on the guarantees provided by the appropriate data law and the Standard Contractual Clauses? We'll just look at the findings of the DPC, Judge. 15:17

MS. JUSTICE COSTELLO: Mm hmm

MR. McCULLOUGH: In which she says that the SCC decisions are likely to offend against Article 47 of the Charter, or that the safeguards appropriately set out in the annex do not address CJEU's objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter. 15:17 15:18

It's evident, Judge, that she's formed the view, as required in the second part of 4(1)(a), that the effect of US law is to impose requirements which have a substantially adverse effect on the guarantees provided by the applicable data protection law, that's Irish and he U law. In other words, is there a breach of the rights of EU citizens here to a substantial degree involved? The answer to that must, on the DPC's own logic, be yes, because she says that there's a breach of Charter rights. 15:18 15:18

So in my respectful submission, Judge, that properly

brought 4(1)(a) into effect, in accordance with the findings made by the DPC. And that meant, Judge, that the proper response of the DPC, instead of bringing this application before the court, would have been to make an appropriate order pursuant to Article 4. 15:18

If a full investigation had been carried out, Judge, I should add that it may well be that 4(1)(c) and 4(1)(c) would also have come into play. So if the DPC had concluded following a full investigation that the 15:19 manner in which Facebook treated data wasn't in accordance with the Directive and the Charter, well, then it would've followed also that the data importer and sub-processor hadn't respected the Standard Contractual Clauses in the annex. 15:19

If I just turn, Judge, to those particular provisions now, if I may. If you look at the back, Judge, of the SCC decision which we were looking at before. I'll just deal with this point, but also the point that you 15:19 are discussing with Ms. Hyland. So you see, Judge, clause 1 contains a definition of applicable data protection law - it's the same definition as in the decision itself - clause 1(e). 15:20

Clause 3, subclause 1 provides for the data subject to enforce... I'm looking, Judge, at the 2010 decision.

MS. JUSTICE COSTELLO: Yes, I have that. That's the one behind tab ten, is it?

MR. McCULLOUGH: Yes.

MS. JUSTICE COSTELLO: Thank you.

MR. McCULLOUGH: So clause 3 provides:

"*The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.*"

Then it provides for the obligations of the data exporter. And I suppose (a), Judge, is perhaps the most important one: 15:21

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

Then various other obligations of the data excessively difficult follow. Clause 5 then provides for obligations of the data *importer*. 5(a): 15:21

"*The data importer agrees and warrants:*
(a) to process the personal data only on behalf of the

data exporter and in compliance with its instructions and the Clauses."

Clause 5(b):

"*That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware.*"

And the court will recall the discussion you had with Ms. Hyland about the extent to which you have a remedy in damages here and the extent to which that is satisfactory.

MS. JUSTICE COSTELLO: Well, I suppose Mr. Schrems has the authority -- could have sued both Facebook Ireland and Facebook Inc. on the basis of this clause, assuming he accepted that they had been transferred under an equivalent, a contract that complied with the SCCs. 15:22

MR. McCULLOUGH: Well, yes, Judge. I think it's not entirely clear, Judge -- 15:22

MS. JUSTICE COSTELLO: I mean, that's who it's designed to protect, isn't it? I'm not saying hes *obliged* to, but I'm just saying --

MR. McCULLOUGH: It is. No, it's designed to give you a damages remedy, Judge, as you can see from Clause 6:

"*The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.*"

Now, Ms. Hyland's original position, I think, Judge, was 'Well, it doesn't really. It looks as if it does. But in fact if material was taken by the US security services, you would then come back and ask whether you had a cause of action here'. And according to 15:23
Facebook's sort of *base* analysis, you don't. But I think after lunch, Judge, the position was the one that was set out by Mr. Gallagher yesterday in which Facebook says 'Well, that may be our base position, but we acknowledge that the cases demonstrate that one 15:23
doesn't get a free pass simply by playing the national security card; restrictions imposed that are said to be in the interests of national security must meet the standards of strict necessity'. And so it is said in those circumstances you might get a cause of action if 15:23
what occurred in the US was no worse than what could occur in Ireland.

I just make two points about that, Judge. First,

actually, it may not be a very good damages remedy *anyway*. And that is for one quite technical reason. Because if you look at Clause 3, the third party beneficiary clause,

MS. JUSTICE COSTELLO: Mm hmm. 15:24

MR. McCULLOUGH: You can enforce against the data excessively difficult this clause, clauses 4(b) to (i). You *can't* actually enforce clause 4(a), by way of a damages remedy in any event.

MS. JUSTICE COSTELLO: Yes, it's there. 15:24

MR. McCULLOUGH: And clause 4(a) is the one whereby the data exporter agrees and warrants that the processing itself, including the transfer, has been and will continue to be carried out in accordance with the relevant provisions of EU data protection law. 15:24

So that guarantee, although it's given, doesn't give rise when breached to a cause of action in damages. You *can* sue in respect of the other parts of Clause 4. But if you look at Clause 4(b), that, for instance, is 15:25 an agreement and warranty that the data exporter has instructed and throughout the duration the personal data processing server *will* instruct the data importer. So you can have a breach, you can have a cause of action in damages in the event of a breach of that. 15:25 But not, it appears, a cause of action in damages in respect of a breach of clause 4(a). But perhaps more importantly in any event, Judge --

MS. JUSTICE COSTELLO: And 4(a) would capture the

national surveillance, the security surveillance in the United States.

MR. McCULLOUGH: Hmm.

MS. JUSTICE COSTELLO: But possibly not (b), I don't know whether (b) would. 15:25

MR. McCULLOUGH: But not (b), Judge, no. The difference between them, Judge, is 4(a) says it'll happen anyway. 4(b) says 'I'll instruct it to happen'. So you can sue for a breach of somebody not giving the right instruction, you can't sue under 4(a), or you 15:26 can't sue for damages under 4(a) when it just happens that there is a breach of your data protection rights in the US, or whatever country it is to which your data is transferred.

15:26

So there is a gap in the damages remedy. And one can understand why there is, because that might be hard on the data exporter to allow a cause of action against him in damages for a matter over which he has little control. 15:26

But whatever about all that, Judge, more importantly, it's only a cause of action in damages. And this is a case, Judge, in which Mr. Schrems seeks, and is entitled to seek, an order preventing the material from 15:26 going to the US in the first place. That's what lies, I suppose, at the heart of Article 25 and Article 26; the data shouldn't *go* in the first place unless the relevant protections are in place. A cause of action

in damages is all very well - perhaps not *very* useful under the circumstances the court has heard very well described; it's going to be hard ever *actually* to ascertain that the US security services have *in fact* had access to this data. 15:27

But in any event, Judge, Article 25 and Article 26 provide the data shouldn't go in the first place unless US laws are effectively equivalent to EU laws and are in accordance with the Charter. And that's what 15:27 Article 4 provides for as well. They all hang together, Article 25/26 of the Directive, Article 4 of the decisions all hang together.

So with respect, Judge, the contention that a damages 15:27 remedy is enough I don't think *meets* the case that arises before the court here. Certainly Mr. Schrems' contention, Judge, is that the material shouldn't go in the first place.

MS. JUSTICE COSTELLO: Now, if you're saying a damages 15:28 remedy doesn't meet the case, just taking it at the highest level, Article 25 provides that you have an adequate decision in relation to the third country and that's fine, you can transfer data pursuant to Article 25. If you're going under 26, the article expressly 15:28 refers to SCCs.

MR. McCULLOUGH: Yes, Judge. Article 26(2).

MS. JUSTICE COSTELLO: Yes. And are you saying that in order to, at some very high level, to meet the

requirement of the Directive in relation to the protection of EU citizens' data, a damages remedy is insufficient?

MR. McCULLOUGH: Oh, yes, Judge.

MS. JUSTICE COSTELLO: How does that then play with the Directive saying that you can transfer, transmit data pursuant to an SCC? 15:29

MR. McCULLOUGH: Oh, but it doesn't, Judge. You start off with Article 25 -- you can transfer material pursuant to an SCC unless and until doing so leaves you in a position in which your rights are breached. The structure of the Directive starts off with Article 25, which provides that: 15:29

"*The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer* may take place *only if, without prejudice to compliance... the third country in question ensures an adequate level of protection.*"

So that's the starting point. It can't be transferred at all unless there's an adequate level of protection. And then there's Article 26, in which derogations are set out. Article 26(1) provides for derogations which really have to do with consent and waiver. Article 26(2): 15:30

"... *a Member State may authorise a transfer or a set*

of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights."

So I'll come to this in a moment, Judge, but the point of Article 26(2) is as follows; if you can set up a set of contractual clauses which ensure you the *same* protection as you would have got under Article 25 then you may transfer. But the decisions themselves and the structure of the Directive make it clear that in if *in fact* the Standard Contractual Clauses *don't* provide that for you, well, then the transfer can't take place. That's what Article 4 of the decision is all about. It says you may *have* an SCC in place, Article 4(1)(a) says you may even be *complying* with it, but the foreign law imposes requirements on you which involve, if you like, a derogation from EU standards and so it must stop.

15:30 15:31 15:31

MS. JUSTICE COSTELLO: So, like, the SCC are global in their application and then Article 4 is country specific, if a Data Protection Commissioner decides to suspend?

15:31

MR. McCULLOUGH: Oh, I think that's right, Judge, yes. Indeed I think it's perhaps even more specific, or *could* be more specific than that. It will apply to *any* transfer. So if, for instance, the DPC was able to

ascertain that particular requirements of, say in this case, US law applied only to one particular data importer, well, then the DPC could suspend the transfer of data to that particular data importer, or to a group of data importers if the particular requirements of US law applied to a group of them, or to the entire of a country if the requirements of the laws of that country applied to the entire. 15:32

And that's important, Judge, because I suggested earlier, and I think wrongly, that if the DPC was making an order under Article 4 she'd have to make it in relation to the US entirely. But I don't think that's correct in fact, Judge. When you look more closely at it, she could make an order under Article 4 that related to whatever exporter and importer or whatever group of exporters and importers were particularly affected by the relevant provisions of US law. And that, in turn, is important, because of course, we've heard a lot in this case about the risks to small and medium enterprise companies. But those companies, of course, don't seem to be subject to Section 702. So in fact the relevant order that could and should be made by the DPC under Article 4 would be a much more confined one than shutting down the flow of data to the US. 15:32 15:32 15:33

Can I just continue, Judge, to deal --

MS. JUSTICE COSTELLO: Oh, certainly. I'm sorry, I'm

interrupting you.

MR. McCULLOUGH: No, no. And it's helpful, I think, when you do, Judge, because it means I can answer the court's queries.

15:33

Making the point, Judge, at paragraph 11 of the speaking note that as the court's aware, there has been a new version of Article 4 put in place. The court will find that at book one, tab 14. And it replaces Article 4 in both of the decisions, Judge, but I 15:34 suppose we should look at, it's really the second one of them that's relevant, because it's the 2010 decision we've been talking about.

MS. JUSTICE COSTELLO: Yes.

MR. McCULLOUGH: So it's Article 2 of this 2016 15:34 amending decision. It doesn't amend only Article 4(1)(a), Judge, it replaces the entire of Article 4 as I read it. So now Article 4 simply reads as follows:

"*Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of* [the Directive] *leading to the suspension or definitive ban of data flows to third countries in order to protect individuals... the Member State concerned shall, without delay, inform the Commission which will forward the information to the other Member States.*"

MS. JUSTICE COSTELLO: And that's the applicable law that I have to consider when *I'm* considering the matter, even though the previous version was the

version that was in place when the...

MR. McCULLOUGH: Well, exactly.

MS. JUSTICE COSTELLO: ... DPC was writing her decision?

MR. McCULLOUGH: The DPC, in fairness, of course, could only have considered the version of Article 4 before her at the time. But if the matter -- but the court, in reality, has to consider this version of Article 4. Because if the DPC considers the matter anew, the DPC will and can exercise only this power, exactly. 15:35

That decision then removes the restrictions on Article 4 that were previously present. It did so because in **Schrems 1** the court had decided that the analogous article of the **Safe Harbour** decision contained an excessive level of restriction on the powers of the DPC to suspend data flows. Now, it was in fact in significantly more restrictive terms than Article 4 of the SCC decisions. But the court can see from the recitals to this implementing decision that it's that part of **Schrems**, of the **Schrems** decision. 15:36

MS. JUSTICE COSTELLO: So does that mean in considering the SCCs, I don't have to consider the nuances of 4(1)(a)?

MR. McCULLOUGH: I think ultimately probably not, Judge. Certainly if the court is considering what should now be done, the court should look at the present day... 15:36

MS. JUSTICE COSTELLO: Or more, if whether or not a

reference is necessary?
MR. McCULLOUGH: Well, exactly, Judge. I suppose that's really the way to look at it.
MS. JUSTICE COSTELLO: I look at it in the context of the current regime? 15:37
MR. McCULLOUGH: Yes. Yes, exactly, Judge. That, I think, is the best way to look at it: *Is* a reference necessary? And for that purpose, the court looks at the present state of the law.
15:37
I'll just briefly look, Judge, at why the DPC says in her submissions that we're wrong about this Article 4 point. And I will get the reference for those for the court. They're at core book 12, Judge.
MS. JUSTICE COSTELLO: Oh, I thought you meant her 15:37 submissions, not her decision?
MR. McCULLOUGH: No, her submissions, Judge, her submissions to this court.
MS. JUSTICE COSTELLO: Yes, I have those. I think they're tab three, is that right? 15:37
MR. McCULLOUGH: They should be at book 12, Judge, tab...
MS. JUSTICE COSTELLO: Seven is it? Or three?
MR. McCULLOUGH: Tab three, Judge, yes. And it's very briefly addressed, Judge, at paragraph 128 -- 127, I 15:38 should say, and the following paragraphs. I think it's fair to say three points are made, Judge.
MS. JUSTICE COSTELLO: Mm hmm.
MR. McCULLOUGH: At paragraph 128 it's submitted that

it's not open to Mr. Schrems to pursue the objections, in circumstances in which they don't arise from the draft decision and in which Mr. Schrems already canvassed his objections to the court and notwithstanding McGovern J. made directions for the proceedings to continue. 15:38

So I suppose the basic point, Judge, is that it's said that, well, I can't canvass these points because they simply don't arise from the draft decision. And with respect, Judge, that brings me back to a point I made earlier; that's an entirely circular point. 15:38
Mr. Schrems' complaint isn't limited by the parts of it that the DPC chose to examine or to refer to the court. The Article 4 issue is squarely raised by Mr. Schrems in his complaint. The court can see the parts of the complaint in which he *does* refer to it. And indeed, whether or not it was raised by Mr. Schrems - although it was - it *had* to be considered by the DPC. If the court just thinks of the job of the DPC, looking *at* the SCC decisions and considering whether to refer the question of their validity to the Court of Justice, *obviously* the DPC had to consider Article 4, or at least *should* have considered Article 4. 15:39 15:39

Then another point is made, Judge, at paragraph 131.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: "*The version of Article 4(1) then in place was not engaged, given that the Commissioners*

concerns did not relate to '<u>requirements</u>' imposed on data importers or sub-processors which had an adverse effect on the applicable data protection law or the SCCs."

And perhaps we've already addressed that, Judge.

MS. JUSTICE COSTELLO: Mm hmm.

MR. McCULLOUGH: In my submission, the requirements in question are the requirements of US law. And in fact the very point that is being made by the DPC in her draft decision is that the requirements of EU law are such as to lead to a breach of the data protection rights of EU citizens when their data is exported from the EU to the US. And so in my respectful submission, Judge, that part of Article 4(1) is met. 15:40

Then at article 131, subarticle 2 the DPC deals with a point to do with equal treatment and proportionality and she says it would be in breach of *those* principles to forbid transfers by Facebook Ireland to be suspended while other transfers were ongoing. And with respect, Judge, that, again I don't think could be right. I think the proper reading of Article 4 is that it entitles the DPC to make orders relating to one country, one entity, a group of entities. The DPC seems to *accept* that, because that's the premise of what she says, but she says that that would be wrong and a breach of the principles of equal treatment. 15:41

But in fact, Judge, when you consider the alternative that the DPC puts before the court, the proposal the DPC makes is that the court should refer to the Court of Justice the question of whether the *entire* of the SCC falls. Now, I know Mr. Murray has said that he is 15:42
asking the court to refer only the question of the legality of the SCC insofar as it relates to the US, but that, I think, is structurally hard to see. Can you have -- the structure of the SCC decisions under Article 26(2) *seems* to suggest a single worldwide 15:42
decision, as opposed to a set of decisions, one for each country. And while --

MS. JUSTICE COSTELLO: And so you couldn't get a decision of the Court of Justice saying the SCC decisions are valid save and insofar as they're used 15:42
for transfer of data to the US?

MR. McCULLOUGH: Yes. Or to say that they're okay for India, Pakistan and somewhere else but not okay for other countries. That doesn't seem to be the structure of Article 26(2). 15:43

So if you look at what the DPC -- that's a matter for the Court of Justice ultimately, Judge, of course. But that does seem to be the structure of it. And so it does seem wrong, Judge, that it should be advanced to 15:43
the court that it would be better to run the risk of striking down the SCCs in their *entirety* as against forbidding data flows on a more specific basis. Even *if* the SCC can be struck down by the Court of Justice

for one country only, that still creates a far wider effect than an Article 4 order restricted to those by whom the relevant parts of EU law are affected.

So, Judge, with respect, while it may be picking out one person to make an order under Article 4, that certainly seems better, and more in accordance in any event, with the SCC decisions themselves than to refer a question as to whether the entire edifice should come tumbling down. 15:43 15:44

MS. JUSTICE COSTELLO: So even though it could be almost a matter of happenstance as to whether somebody chose to sue - and I'm just taking them, for example, as, you know, Yahoo or Apple, or I don't know who else is transferring - does Twitter come as a -- I don't know, whatever it could be, as opposed to, in this case Facebook. So presumably, for example, Apple or Yahoo are subject to the same laws in the US as Facebook. But data flows to Facebook, on your argument, would be suspended, but the others would happily continue? 15:44 15:44

MR. McCULLOUGH: No, I can see how there might be a variety of different orders, Judge. I can see how one might suspend them for a single entity or for a group of entities. There are a limited number of entities that it appears from the documents the court has seen are subject to the existing 702 programmes. 15:45

MS. JUSTICE COSTELLO: But I'm just asking -- you see, Mr. Schrems has only complained about Facebook.

MR. McCULLOUGH: It *is* only about Facebook.

MS. JUSTICE COSTELLO: Would the Data Protection Commissioner be entitled to go outside the scope of the four walls of his complaint? Let's say you were right and she should exercise her powers under Article 4 of the SCCs; that would apply to a suspension of data -- 15:45

MR. McCULLOUGH: To Facebook only.

MS. JUSTICE COSTELLO: To Facebook only?

MR. McCULLOUGH: On the face of it, Judge, yes.

MS. JUSTICE COSTELLO: And how would that leave us? Is there any issue there, or is it just happenstance and 15:45 that's the way it falls?

MR. McCULLOUGH: I suppose it happens now, Judge. And perhaps not unknown in litigation that a circumstance that in fact affects many people, as it turns out affects one person only because that's the one person 15:45 that sued. I suppose once an order under Article 4 had been made against Facebook, it would, of necessity, be relatively easy, it would, of necessity, be relatively obvious that similar complaints would lead to similar results against other entities subject to the same 15:45 programmes.

But the major point I want to make, Judge, is that it is preferable and more in accordance with Article 4 and the SCC decisions in general that *focused* orders should 15:46 be made, as opposed to orders striking down the entire of the decision or invalidating the entire of the decision.

And it's pointed out to me, Judge, that the Article 28(3) power is, of course, wider than the Article 4 power. So it is, I suppose, in principle open to the DPC to make an order under Article 28(3) or to initiate her own investigation. 15:46

So just to conclude on Article 4, Judge. It was said to you in the last couple of days a few times by Mr. Gallagher, I think, that a striking feature of this case is that Mr. Schrems doesn't contend for the 15:47 invalidity of the SCCs. And that's true in this strictly limited sense; Mr. Schrems says and we say that if Article 4 means what it appears to mean, well, then the SCCs aren't invalid, precisely because they allow for a form of safety valve in which the DPC can 15:47 make orders adequate to protect the rights of EU citizens who are affected by or potentially affected by the transfer of data from the EU to the US.

So there's a structure in the SCCs themselves that 15:47 allows for Charter rights and Directive rights to be protected. And to that extent and in that way, I don't argue for the invalidity of the SCCs. But if I'm wrong about that and if the court takes the view that no, Article 4, for whatever reason, doesn't apply, well, 15:48 then of course I *do* say that the SCCs are invalid and must be struck down. Because the consequence of that would be, I suppose, reasonably obviously, that the SCCs would not provide for the adequate protection of

the rights of EU citizens. And I think that must follow, Judge, from the first point that I make.

So can I move on, Judge, to the second part I want to say, of what I want to say? And we address this at the 15:48
foot of page six and the following pages. So we make the point, Judge, that without prejudice to the point I've made that it didn't form part of the reformulated complaint and only insofar as is determined that the exercise of the Article 4 powers isn't permissible or 15:48
required, well, then we agree that the SCC decisions don't allow for adequate protection of EU citizen data rights and that those decisions ought to be declared invalid.

15:49

I just want to pause now, Judge, under the next heading to deal with two points that seemed to be central to Facebook's case on these issues and that's, first, their argument in relation to national security, in which they said that the actions of which the court has 15:49
heard in the US are simply not subject to data protection law at all. And they said that, Judge, as I understand it, because of the provisions of the TFEU excluding national security from the purview of the Treaty and the provision of the Directive, following on 15:49
from that, providing that it applies only to issues covered by the Treaty.

And then they made a related but different argument,

Judge, in which they said that the proper comparator here, if you come to *make* a comparison, is not between EU law on the one hand and US law on the other hand, rather it's between the laws of the Member States on the one hand and US law on the other hand. And I respectfully submit they're wrong on both those points. 15:50

The national security issue, Judge, perhaps need not greatly detain the court, because although it's taken up a great deal of discussion before the court, I think we've actually all arrived at a position in which we agree, or at least agree for the purpose of the court's consideration of the matter. I'll just break it down into stages as to what I say about it. 15:50

The first point I make is this, Judge, that the exclusion of national security from the purview of the Treaty I suppose self-evidently is an exclusion of EU Member States' national security. The EU *never* purported to legislate for the national security of *any* area other than that covered by its Member States. Well, perhaps only a statement of the obvious, Judge, but the national security *exclusion* mentioned in the TFEU I think is self-evidently an exclusion relating to the national security of Member States. But that doesn't follow, for reasons that I'll explain in a moment, Judge, that the national security concerns of the US are exempt from scrutiny. They are, but for a different reason. 15:50 15:51

So the next point is this, Judge - and on this I think we probably ultimately agree, or at least agree for the purpose of these proceedings - that although the EU doesn't have competence in the area of national security, it doesn't follow from that that the laws of Member States are not subject to scrutiny when they ostensibly -- sorry, they're not subject to scrutiny, my apologies, when they ostensibly relate to national security. 15:51

So it's not a sort of a trump card, it's not a joker; Member States can't simply say 'This law is passed in the interests of national security, this measure is taken in the interests of national security, it is now exempt from examination'. It's clear, Judge, from the cases that you've seen that at least as far as the CJEU in its decisions to date is concerned, restrictions on Charter rights on the grounds of national security are permitted only to the extent that they're strictly necessary and proportionate. 15:52

And, Judge, we set out in footnote 19 in particular references to some of the material that the court has seen which we say makes that clear. So we refer to the Charter itself and then to **Watson**, the **Tele2** decision, which the court said at paragraph 96: 15:52

"*Due regard to the principle of proportionality also*

derives from the Court's settled case-law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary". 15:53

MS. JUSTICE COSTELLO: Mr. Gallagher said that that was fine, because it clearly fell within the scope of EU because it was in a criminal sphere which had been brought into the scope of the EU purview, as opposed to the national security area which remained outside the 15:53 purview of the EU.

MR. McCULLOUGH: Well --

MS. JUSTICE COSTELLO: If I've summarised him correctly. And I doubt I have, but anyway.

MR. McCULLOUGH: Well, Judge, I don't think it alters 15:53 what is said. It certainly is said in **Schrems**, Judge, but also in **Watson**, so perhaps one can just rely on Schrems ultimately, Judge. I think it's clear, Judge, that there is a strictly -- there's a proportionality requirement and, therefore, a strictly necessary 15:54 requirement which follows on from the proportionality requirement. And I don't think there's any dispute between us, Judge, that at least *this* case can be determined on that basis, that restrictions on Charter rights and, in due course, Directive rights can be 15:54 justified only insofar as they are proportionate and, therefore, strictly necessary.

Now, Mr. Gallagher says, Judge, that ultimately if he

ever arrives in the CJEU, he'll take a different point of view. And that's fine, Judge, of course he's entitled do to do that. His contention there will be that the entire area of national security is exempt from scrutiny. So he'll have a more difficult time answering his North Korea question there than he did here, because I don't actually *think* he has an answer for it. But nevertheless, Judge, he can deal with it there. For the moment, Judge, you heard clearly from Ms. Hyland's answer to the question posed by the court just before lunch that it *is* accepted for the purpose of these proceedings that there is a requirement of strict necessity. 15:54 15:54

And that's perhaps particularly so, Judge, in this case, where, not actually dealing with processing -- and we're not primarily dealing with processing by Member States themselves, we're dealing with processing by data processors and a stream of actions by data processors, that's to say the export from Ireland to the US, the making available in the US, the passing of material, of data from Facebook Ireland to Facebook, they're all acts of data processing. And the real question here, Judge, is whether the US law that imposes, if you like, limitations on the rights of data subjects in respect of that processing is or is not valid in accordance with EU law. 15:55 15:55 15:55

So certainly, Judge - we address this at paragraph 20 -

the Directive itself, the Privacy Shield Decision, the **Schrems** decision, indirectly **Watson** all make it clear that EU law provides that national laws governing the activities of providers can be legitimised within the EU on the basis of national surveillance solely to the extent such restrictions are strictly necessary.

If the court just pauses for a moment, Judge, to think of this; I mean, what can the Commission and the US Government have been doing when they were talking about the Privacy Shield and the long passages in it which talk about US national security unless they accepted at least that premise? And it follows also, Judge, from **Schrems** - and we've set out at footnote 22, I suppose, a citation that is perhaps more directly relevant, because **Schrems** *is* a decision in precisely the same space, in which the court said at paragraph 92:

"*Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary.*"

And that's what -- if you like, Judge, that's the position *in* the EU; you can derogate from privacy rights, so Article 7 and Article 8 rights under the Charter of Fundamental Rights, only insofar as strictly necessary, whether national security is your reason or

another aim of the State is your reason, they must all be proportionate and strictly necessary.

And in this case, Judge, it follows from that that the transfer of data to other countries whose laws impose 15:57
restrictions on the rights of data subjects is permitted only if and to the extent that the protection in those countries is effectively equivalent to that in the EU and that it doesn't breach the Charter rights of EU citizens. And that's really what lies at the heart 15:58
of **Schrems 1**, Judge, and that's what this case is about.

Perhaps again it seems obvious, but it has taken us, I think, a long time, Judge; I think the undisputed 15:58
question here is -- well, there's no doubt that this is a statement, Judge, I think, with which the parties agree, that you can transfer data to the US only if and insofar as US law gives you protection that is effectively equivalent - I'll come back to the meaning 15:58
of that in a moment - to that available under EU law and that doesn't breach EU citizens' Charter rights.

In other words, Judge, a restriction in this case, a restriction that the court has heard a lot about, any 15:59
of these restrictions, is permissible if and only if and to the extent and only to the extent that a similar restriction would be acceptable if it was imposed by a Member State in the EU. That's the comparison the

court is making - are all these restrictions in the US restrictions of a sort that would be acceptable in the EU and do they breach EU citizens' Charter rights?

MS. JUSTICE COSTELLO: And in assessing that question, is the jurisprudence opened by Ms. Hyland from the Court of Human Rights, European Court of Human Rights the appropriate test? 15:59

MR. McCULLOUGH: Well, it's not -- I suppose the jurisprudence of the Court of Human Rights informs any analysis of Charter rights, Judge. But they're not in precisely the same terms. I mean, there isn't in fact an equivalent of both Article 7 and 8 in the... 16:00

MS. JUSTICE COSTELLO: No, but you know the test, it was quite, in relation to national security law she was labouring -- emphasising the point that there was quite a, what was it, margin of... 16:00

MR. McCULLOUGH: A margin of discretion, Judge, yeah.

MS. JUSTICE COSTELLO: Of discretion, yes.

MR. MURRAY: Appreciation.

MS. JUSTICE COSTELLO: Appreciation. I knew it was an unusual phrase. 16:00

MR. McCULLOUGH: A margin of appreciation, my apologies. So that's a margin to the States, Judge. I suppose a margin of appreciation point may not apply quite as much in relation to the Charter as it does in relation to the Convention. But the basic principles of proportionality, Judge, as analysed in the Court of Human Rights - I should say the component *parts* of the test of proportionality - are, I think, the same as the 16:00

assessment of proportionality that the court will find conducted at Charter level.

There are differences in the texts of the rights and there may be differences in the extent of the margin of appreciation, but the basic analysis of proportionality is going to be roughly the same, Judge.

So it's just four o'clock, Judge. 16:01

MS. JUSTICE COSTELLO: Yes, thank you.

MR. McCULLOUGH: May it please the court.

MS. JUSTICE COSTELLO: I think the parties, if you wouldn't mind, should make plans for Tuesday and, by the look of it, Wednesday as well.

MR. MURRAY: Very good, Judge. 16:01

MR. GALLAGHER: Thanks, Judge.

THE HEARING WAS THEN ADJOURNED UNTIL FRIDAY, 10TH MARCH AT 11:00

B

C

D

E

F

G

J

M

N

O

P

Q

R

S

T

U

V

W

Y

Z

—