THE HIGH COURT - COURT 29

COMMERCIAL

Case No. 2016/4809P

THE DATA PROTECTION COMMISSIONER PLAINTIFF

and

FACEBOOK IRELAND LTD.
AND DEFENDANTS
MAXIMILLIAN SCHREMS

HEARING HEARD BEFORE BY MS. JUSTICE COSTELLO

ON WEDNESDAY, 1st MARCH 2017 - DAY 13

13

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

_____

_____

GWEN MALONE STENOGRAPHY SERVICES

APPEARANCES

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

FOR DIGITAL EUROPE:	**MR. MICHAEL CUSH SC** **MS. NESSA CAHILL BL**
Instructed by:	**A&L GOODBODY** **28 NORTH WALL QUAY** **NORTH WALL** **DUBLIN 1**
FOR ELECTRONIC PRIVACY INFORMATION CENTER:	**MR. COLM O'DWYER SC** **MS. GRAINNE GILMORE BL**
Instructed by:	**FREE LEGAL ADVICE CENTRE** **13 DORSET STREET LOWER** **DUBLIN 1**

INDEX

WITNESS **PAGE**

THE HEARING RESUMED AS FOLLOWS ON WEDNESDAY, 1ST MARCH 2017

MS. JUSTICE COSTELLO: Good morning.

REGISTRAR: In the matter of Data Protection Commissioner -v- Facebook Ireland Ltd. 11:05

MR. GALLAGHER: Judge, before Prof. Vladeck resumes, and this may not suit the court and it will be perfectly understood if it doesn't, he is hoping to catch a flight at four and if we were close to finishing his examination at one o'clock would it be possible to sit on for 15 minutes, maybe the court has another commitment at that stage and, if so, that's perfectly understood. 11:05

MS. JUSTICE COSTELLO: Well, we'll see how we go. 11:05

MR. GALLAGHER: Exactly.

MS. JUSTICE COSTELLO: My other commitment can move.

MR. GALLAGHER: Well, sorry, nobody wants to interfere with that. We'll see how we go. Thank you, Judge.

MS. HYLAND: Prof. Vladeck, please. 11:05

PROF. VLADECK, WAS CROSS-EXAMINED BY MR. MURRAY AS FOLLOWS:

MR. MURRAY: Now we'll try professor to move this along and get you out. To that end can I ask you please to look at your report at page 23 paragraph 79. 11:05

MS. JUSTICE COSTELLO: Sorry, Mr. Murray, these have been put in the wrong place, just give me a second.

1 Q. **MR. MURRAY:** Certainly, Judge. Professor, in this part of your report you proceed to identify aspects of the DPC Draft Decision with which you take issue in various different ways; isn't that right?

A. Indeed. 11:06

2 Q. And you identify *eight* points over the following nine pages of the report; isn't that correct?

A. That's correct.

3 Q. These were the only eight, and I use the word *criticisms* in the most general way for the moment, and 11:06 we'll look at them in detail, but these were the only eight criticisms you had of the DPC report; isn't that correct?

A. In my report these were the eight I focussed on. My instructions, as I think I mentioned yesterday, were to 11:07 focus on the discussion in the DPC report of remedies and standing and the like. So I did not pay nearly as close attention to the discussion, for example, of European law, Mr. Murray.

4 Q. No, of course. 11:07

A. Yes.

5 Q. Absolutely.

A. Yes.

6 Q. But these are the eight criticisms you have of the DPC's consideration -- 11:07

A. Quite.

7 Q. -- of the adequacy of remedies in US law; isn't that correct?

A. That's correct.

8 Q. Okay. And indeed this is what you were asked to do?
A. Quite.
9 Q. Your brief was to take, read, consider and critique the DPC's report, is that fair?
A. And amplify it where possible. 11:07
10 Q. Correct, okay. Now I want to look at these points, many of them we have considered and we can move through very quickly, many of them are very brief?
A. Hmm.
11 Q. But before I do that can I just ask you this question: 11:07
Professor, as we know, and as you found out on Friday and we found out the night before last, the US government made comments on a draft of your report?
A. Mm hmm.
12 Q. Facebook have already given us comments on, some 11:08
comments from the US government on the report, do you personally, subject to Facebook, have any difficulty with our seeing the comments of the US government on your report?
A. As long as I'm not speaking for counsel, on my behalf, 11:08
no.
13 Q. On your own personal behalf, and it's a matter obviously for Facebook through their counsel to adopt a position on that?
A. But if it was just up to me, Judge, I would be fine. 11:08
14 Q. Of course. Just before I leave that can I ask you this question: Yesterday when we were discussing the comments of Carrie Cordero as recorded in your report, you were, if you don't mind me saying so, quite

emphatic that in your report you had alerted the reader to the fact that you had elsewhere made critical comments of what Ms. Cordero had said; isn't that right?

A. I had, although, as you quite rightly pointed out, Mr. Murray, I was misremembering my report. 11:08

Q. Well, no, you were misremembering, but you were actually pretty sure that you had it in your report to the extent that at lunch you went, as you told us, to find them and they weren't there and I think you were a bit surprised they weren't there? 11:09

A. Yes, although if what you are insinuating, Mr. Murray, is that they were in an earlier draft and were deleted, that's not correct.

Q. I see. Do you have any other explanation as to how you thought they were there and were not? 11:09

A. I guess I had just mistakenly thought that in my more general comments about my scepticism, Judge, that I had included a note on the intelligence committees.

Q. Yes. And, just to be clear, and I'm sure you didn't mean it in this sense, the word *insinuating* is perhaps a derogatory one I was about to -- 11:09

A. Oh, I am sorry, I did not mean it pejoratively.

Q. I was about to ask you had they been in an earlier version but you were absolutely certain that they were not? 11:09

A. I'm positive.

Q. So you never even recorded in any version of your report the fact that you had made these adverse

comments of Ms. Cordero's comment which in turn is without qualification recorded in your report?

A. Indeed. I mean, Mr. Murray, if they had been in the earlier draft they would have been in the final draft. It was my omission from the beginning. 11:09

20 Q. I see. Now can we move on then to look at the eight points that you make, Professor, and thank you for that.

So in paragraph 79 you refer to the substantial oversight and accountability mechanisms described above, and I think we discussed at that some length yesterday. *"US law"*, you say: 11:10

"*Provides an array of remedies for abuses of government surveillance authorities. In the DPC Draft Decision, Commissioner Dixon concluded that 'remedial mechanisms available under U.S. law' are 'not complete,' and that the 'standing' doctrine 'operate as a constraint on all forms of relief available.' This conclusion was based on the Morrison Foerster memo.*" 11:10 11:10

Then you say this: "*On closer inspection, although there are defects in the existing remedial scheme - and you helped us yesterday identify those defects - it fails to take account, the DPC Draft Decision, for several of its key features while misinterpreting several others and, as a result, presents a rather incomplete version of contemporary law.*" 11:10

And that's your verdict on the DPC report; isn't that correct?

A. It is, that's correct.

21 Q. And the first of them is the criminal remedy or the facility for criminal prosecution provided for by section 1809; isn't that right? 11:10

A. Yeah.

22 Q. Yes. And I don't think, and please correct me if I'm wrong, Professor, but I don't think you are for a moment suggesting that this is a judicial remedy to which a person affected by unlawful surveillance can have resort in the manner in which you advocate remedies in your papers? 11:11

A. Not at all.

23 Q. No. 11:11

A. I think it was there only as part of the larger conversation in my report and elsewhere of opportunities for courts to reach the merits of these questions.

24 Q. Fair enough. But of course, as you I'm sure will be the first to acknowledge, this institution of criminal proceedings is dependent on a decision of the government to prosecute? 11:11

A. Quite.

25 Q. The government may have good reasons for not doing so. Am I also correct in thinking that this offence is subject to a *defence*? 11:11

A. It could be subject to a defence. I mean I think we, as you know, Mr. Murray, there have not been cases

under section 1809 and so we don't have good case law. I would not want to --

26 Q. **MS. JUSTICE COSTELLO:** Sorry, when you say there is no cases, do you mean none at all?

A. I am unaware, Judge, of prosecutions under section 1809. 11:12

MR. MURRAY: Exactly.

A. I think the reason why it is held out by people like me frankly as a relevant part of the scheme is because the hope is that it's a deterrent, right, that having this criminal penalty on the books is actually having some salutary effect on the conduct of government officers. We don't, as Mr. Murray I think is about to point out, have examples of it. 11:12

27 Q. No. There are a number of interpretations one can pursuit on the fact that there have been no prosecutions, is that fair? 11:12

A. I agree.

28 Q. All right. But from your knowledge of the criminal law, insofar as relevant to this area, would it surprise you if the offence had a defence applicable where the officer was acting in good faith under a warrant? 11:12

A. It would only, Mr. Murray, because it requires a wilful or intentional breach. And so it would seem to me that in that circumstance it would be difficult for an officer to mount a good faith defence. But again, you know, we haven't seen this play out in practice, so I'm only speculating. 11:12

29 Q. But it is an offence, as with all criminal offences of course, which would require mens rea?

A. Quite.

30 Q. Yes. And the offence arises where a person engages in electronic surveillance under cover of law, except as authorised? 11:13

A. Which would mean, for example, Judge, that I as a private citizen could not violate this, even if I surreptitiously recorded a conversation that would otherwise trigger the definition. 11:13

31 Q. Yes. And the statutory defence, because there is one, is that:

"*It's a defence to a prosecution under the subsection that the defendant was a law enforcement investigative officer engaged in the course of his official duties and the electronic surveillance was authorised and conducted pursuant to a search warrant or court order*". 11:13

A. Yes, and that's what the statute says. I guess, Mr. Murray, I am allowing for the possibility that the warrant itself was obtained through bad faith. 11:13

32 Q. I see.

A. And we have, not in the FISA context, but in the ordinary law enforcement context, Judge, there are examples where a warrant who is obtained through knowing and intentional misrepresentations by law enforcement officers can still be the basis for some kind of after the fact liability. 11:14

33 Q. Well I think we can move from it because I think you

accept it's an observation you make on the report --

A. Yes, quite.

34 Q. -- fully understood but not in fact an error nor in fact a new judicial remedy of the kind which we all agree should be present. 11:14

Now, the second point you make relates to APA, and we discussed this again yesterday, and maybe if we can just, Professor, clarify precisely the issue in relation to APA and the scope of the section. A lot of 11:14
this is what we have already said and what you said in your report but just to be absolutely clear.

Provision creates a remedy, not a substantive cause of action, the remedy is declaratory and injunctive 11:14
relief, not damages; declaratory relief itself is a remedy of limited resort, you explained yesterday, the limitations arising that it will not be granted in respect of something which is purely historical, as I understood you to say it, and will only be granted in 11:15
relation to something in the future if there is a likelihood of that event recurring in the future, is that a fair summary?

A. And ongoing of course.

35 Q. Yes. 11:15

A. I don't mean to miss that.

36 Q. No, of course. And obviously that present, actual or likely future event is similarly a precondition to the grant of injunctive relief?

A. That's right.

37 Q. Yes. It does not -- it can be ousted, APA?

A. Yeah. Just the doctrinal term is *precluded*.

38 Q. Okay, fair enough. It can be precluded obviously expressly but also by implication and that implication has been held to arise where there are other remedies provided by Congress meaning that it is the waiver of sovereign immunity through the grant of those remedies which governs the statutory provision rather than the more general one under APA? 11:15

A. That's right. I might just tweak that explanation one iota which is just to say: In that context I think the assumption is that the more specific remedy will trump the more general remedy, right. And so that if Congress has thought to occupy a more specific field, that will be held to displace the APA. 11:16

Again, as we have seen in the Second Circuit **Clapper** decision, the courts require a fairly specific showing of an intent to preclude because of this background presumption of judicial review. 11:16

39 Q. All right. Now, in **Jewel -v- NSA**, a decision you are familiar with, it was held that the APA was ousted in respect of claims under the SCA and Wiretap Act; is that correct? 11:16

A. That's my understanding.

40 Q. Yes. Well is that correct?

A. Yes, that's correct.

41 Q. And that is because there was a claim for damages under

section 2712 or, as it is otherwise described, section 223 of the PATRIOT Act; is that right?

A. That's correct.

42 Q. Okay.

A. And, if I may, and because, Judge, 2712(d) has an express exclusivity provision, right, that makes quite clear Congress's intent that that remedy for damages against the government be the exclusive remedy in that context. 11:16

43 Q. And if I wish to claim damages under FISA what is the statutory provision that gives me that entitlement? 11:17

A. 1810.

44 Q. And what is the effect of section 2712 on *FISA* damages claims?

A. So 2712 allows three kinds of FISA damages claim, Judge. In 2712(a) it refers to three provisions of FISA. These are the minimisation requirements of classic FISA, Title 1, of the pen and register and of the trap and trace authorities. So those can also be encompassed, Mr. Murray, within 2712. 11:17 11:17

45 Q. Yes. And it would seem to follow from **Jewel -v- NSA** that APA would be ousted in respect of or precluded in respect of those also?

A. I believe that would follow for those three very specific provisions of FISA. Now, importantly, the courts have read, Judge, 2712(a')s reference to those three provisions of FISA as quite deliberate on Congress's part and so have not read 2712 to preclude claims arising under *other* parts of FISA. For example, 11:17

as Mr. Murray knows, in the section, pardon me in the Second Circuit **ACLU -v- Clapper** case, the government argued that those same provisions in 2712 preclude an APA claim to challenge the phone records programme and the Court of Appeal said, no, because that's not one of those three specific provisions of FISA, we don't find preclusion here. 11:18

46 Q. Yes. But certainly aspects of the FISA régime are also clearly precluded as well as the SCA and the Wiretap Act? 11:18

A. I agree.

47 Q. Yes.

A. I agree. The three specific aspects that are cited by section in 2712(a).

48 Q. Yes. We had a discussion yesterday about **ACLU -v- NSA**, that's also a preclusion case, you seem to think it was a standing case? 11:18

A. I had always understood it as a standing case, Mr. Murray. The problem from the Sixth Circuit's perspective was that the allegations were unsubstantiated and so it was impossible to show that the allegedly unlawful warrantless wiretapping was the kind of final agency action necessary to trigger the APA. 11:18

49 Q. I am sorry because I'm getting ahead of myself, just to close off preclusion first: It is clear that, certainly in relation to a number of the circumstances with which the court is concerned, APA is precluded? 11:19

A. Hmm, I would say certainly in the circumstances

specifically mentioned in 2712(a) there would be a strong argument for preclusion. I wouldn't feel comfortable saying beyond that, that it's clear that it would be precluded.

50 Q. And **ACLU -v- Clapper**, a substantial part of the claim was of course directed to a challenge to the constitutional validity of the programme? 11:19

A. And also the statutory. I mean the case went up on the statutory validity as well, that's indeed how it was decided. And because 215 itself, the source of the phone records programme, wasn't one of the provisions covered in 2712, I think that was very central to the Court of Appeals explanation for why that challenge wasn't precluded. 11:19

51 Q. Yes. But that was a case about the 215 programme -- 11:19

A. Correct.

52 Q. -- which is no longer live?

A. That's right.

53 Q. Yes. Now you obviously, aside from those limitations on APA which we have discussed, again just to be clear, you have to establish Article III standing, you have to establish prudential standing? 11:20

A. Which as I think we briefly discussed yesterday means there is something called the zone of interest test, that you are one of those in the zone of interest that the statute was meant to protect. 11:20

54 Q. And you've to establish final agency action?

A. Correct.

55 Q. And it was final agency action, and if we can give the

professor Tab 31 in Book 1 or 2 of the authorities, it was the final agency action which featured in **ACLU -v- NSA** which you appear to categorise yesterday as a standing case?

MS. JUSTICE COSTELLO: Sorry which tab again, Mr. Murray? 11:20

MR. MURRAY: Tab 31, Judge.

MS. JUSTICE COSTELLO: Thank you. (SAME HANDED TO THE WITNESS)

A. Thank you. 11:21

56 Q. I think we will find in this case, will we not, Professor, a fairly extensive discussion of final agency action. You recall what this case was about?

A. I do.

57 Q. Yes. And here, in bringing a challenge, civil liberties organisations sought relief for declaratory judgments against the NSA challenging the terrorist surveillance program of data mining and warrantless interception; isn't that right? 11:21

A. That's correct. 11:21

58 Q. What provisions was that done under?

A. The allegation was that there was actually no statutory authority for the TSP and that it was conducted by the President, Judge, pursuant to his inherent constitutional authority under Article 2 of the US Constitution. 11:21

59 Q. Yes. And if we go to page 26, Professor?

A. Of the printout?

60 Q. Of the printout, yes, please, the numbers are on the

bottom right-hand corner of the page.

A. Mm hmm.

61 Q. We see the definition of agency action?

A. Mm hmm.

62 Q. *"The whole or part of an agency rule, order, license, sanction, relief or the equivalent or denial thereof, or failure to act. This definition is divided into three parts beginning with the list of five categories, decisions made or outcomes implemented by an agency."* 11:22

11:22

And then it's explained, by reference to authority: *"That all of these categories involve circumscribed discrete agency actions as their definitions make clear, an agency statement of future effect designed to implement, interpret, or prescribe law or policy, final disposition in a matter other than rule making, permit or other form of permission, prohibition or taking of other compulsory or restrictive action or a grant of money assistance and so forth."* 11:22

11:22

They then proceed: *"The second part of the agency action definition, the equivalent or denial thereof, must be a discrete action or a denial of a discrete action, otherwise it would not be equivalent to the five listed categories."* 11:22

And the final part of the definition: *"A failure to act is properly understood as a failure to take an agency action. Under Supreme Court precedent classic*

examples of agency action include the issuance of an agency opinion."

And then they said: "*Here, however, the plaintiffs are not complaining of 'agency action' as defined in APA, and the record contains no evidence that would support such a finding. The plaintiffs challenge the NSA's warrantless interception of overseas communications, the NSA's failure to comply with FISA's warrant requirements."* 11:23

So it wasn't, it was also a failure to comply with the *FISA* order; isn't that right?

A. As alleged in the complaint. I mean there is so much secrecy -- 11:23

63 Q. I didn't understand you to mention that, but that was an aspect of the complaint, you remember that now?

A. I did not remember that until you brought this passage back to my attention.

64 Q. Oh, I see. Sorry, I had understood from your evidence yesterday that this was a judgment you had recently reviewed and were well familiar with? 11:23

A. It was. I had not re-read the complaint.

65 Q. I see. Well this is not the complaint, this is the judgment? 11:23

A. I know.

66 Q. "*The plaintiffs challenge the NSA's warrantless interception of overseas communications, the NSA's failure to comply with FISA's warrant requirements, and*

the NSA's presumed failure to comply with FISA's minimization procedures. This is conduct, not 'agency action'. Furthermore, there is no authority to support the invocation of the APA to challenge generalised conduct." 11:24

Do you agree with that?

A. So I would just make two quick points, if I may, Mr. Murray. The first is, I might draw the court's attention to the very first paragraph of the opinion on page 2 where Judge Batchelder says: 11:24

"*Because we cannot find that any of the Plaintiffs have standing for any of their claims, we must vacate the district court's order.*" 11:24

So this is part of why I had always assumed that this was a standing case.

67 Q. Oh, I understand that, Professor.

A. But, if I may, the second point, Judge, is I think it's important to stress the difference in the programmes that were being challenged. The TSP, as I have just tried to explain, was alleged to have been a completely unilateral programme carried out without statutory authority, right. The contrast in my mind, and I think the contrast between this decision and the Second Circuit's analysis in **ACLU -v- Clapper**, is where Congress is by statute authorising concrete actions by particular agencies. I think that comes much closer to 11:24 11:24

satisfying the test for agency action and I think that's why you see the difference between these two cases.

68 Q. Let's test those comments against what the court said:

"*Looking at the 'five categories' of enumerated 'agency action', the NSA's surveillance activities, as described by the three facts of record, do not constitute, nor are they conducted to any agency rule, order, license, sanction or relief.*" 11:25

Do you see that?

A. Mm hmm.

69 Q. "*Although the Plaintiffs labelled the NSA's surveillance activities as 'the Program' and the district court labeled it the 'TSP', the NSA's wiretapping is actually just general conduct given a label for the purpose of abbreviated reference. The plaintiffs do not complain of any NSA rule or order, but merely the generalized practice, which – so far as has been admitted or disclosed – was not formally enacted pursuant to strictures of the APA, but merely authorised by the President (albeit repeatedly, and possibly informally). Nor do the plaintiffs challenge any license, sanction, or relief issued by the NSA.*" 11:25

You see that?

A. I do.

70 Q. "*The plaintiffs do not complain of anything <u>equivalent</u>*

to agency action, which also requires some discrete action by the NSA. The plaintiffs are not challenging any sort of 'circumscribed, discrete' action on the part of the NSA, but are seeking to invalidate or alter the NSA's generalised practice of wiretapping certain overseas communications without warrants."

You see that?

A. I do.

71 Q. And then he continues, and if you look at the last sentence in that? 11:26

A. She, sorry.

72 Q. I am terribly sorry, thank you for that. The last sentence in that paragraph: 11:26

"*Even assuming, arguendo, that the warrant requirement and minimization procedures are discrete agency actions, those procedures are replete with discretionary considerations, thus disqualifying them from this definition of agency action under the APA.*" 11:26

And if you just go over the column there is a quotation just above the reference to Title 3 and the last three sentences of that, after the highlighted quote to 117, Supreme Court 1154 says: 11:26

"*Because the NSA's surveillance activities do not constitute 'agency action', the analysis of whether they are final agency action is strained and awkward.*

It nevertheless is clear the NSA's wiretapping does not consummate any sort of agency decisionmaking process nor does it purport to determine the rights or obligations of others."

11:26

Is that a reasonable encapsulation of the test of agency action in your opinion?

A. I think it is.

73 Q. Yes.

A. I think it is an encapsulation that was being applied to a very different fact pattern, and I think that the difference in fact pattern is relevant. 11:27

74 Q. But it does show that in the very type of situation with which the court is concerned, the final agency action requirement under the APA itself can be a preclusion on the invocation of that remedy, I don't think you disagree with that? 11:27

A. Or an obstacle. I wouldn't say, preclusion is when Congress has over --

75 Q. I am sorry. 11:27

A. Yes.

76 Q. I know you are using that term as a term of art, it is a substantial, if not fatal obstacle in certain complaints?

A. If, Judge, and I want to be as clear on this as I possibly can. If we had another circumstance where we had a similar challenge to a surveillance programme, not where you had the kind of detailed statutory authorisation and statutory procedures that we see, for 11:27

example, with Section 215 and with Section 702 of FISA, but with the programme like the TSP where the whole, if you'll forgive me, sort of gestalt of the programme is that the government is conducting it through the unilateral auspices of the President's authority. And part of the issue is that there's not a lot of definition in that context.

77 Q. **MS. JUSTICE COSTELLO:** And how does that differ from an executive order?

A. So executive orders are more policy dictates, right, they are not actually the programmes themselves. And so an executive order would be the President saying 'here is how I understand my authorities'. There is presumably, or at least there was presumably, an executive order underlying the terrorist surveillance programme, the TSP. In contrast to the far more, if I can say, crowded legal régime for the programmes we're more familiar with today, for the phone records programmes, for 702, for PRISM and Upstream.

78 Q. But nonetheless - sorry, in **Klayman -v- Obama** as well it was found that the APA had been impliedly precluded; isn't that right?

A. Yes, although I think, as we discussed yesterday, I think that analysis is both deeply vulnerable and in any event no longer on the books.

79 Q. Yes. And what challenge was that to, what was that a challenge to?

A. To the phone records programme.

80 Q. Yes. The **Bangura** case that you refer to, that really

was a very unusual case. That was a case of a married woman wishing to assert or to obtain a marital immigration visa. Her husband was a naturalised US citizen, she was not and the issue was whether she was within the zone of interest for the purposes of the prudential standards part of the test; isn't that right?

A. That's correct.

81 Q. Yes. And it was found she had no standing, actually; isn't that right? 11:29

A. On the facts of that case.

82 Q. Yes. I'm not sure by --

A. But not simply by dint of the fact that she was a non-citizen.

83 Q. Yes. So I think we can agree, Professor, insofar as this second observation you make about the DPC's decision is concerned, the Administrative Procedure Act remedy is one which has very many limitations attached to it of relevance to the matters with which the court is concerned? 11:30

A. It certainly has limitations. I think we might quibble over the adjectives.

84 Q. Okay. It's not something which we have been able to detect in certainly the writings that we have put to you which address remedies? 11:30

A. Well, again I mean, Judge, as I said yesterday, I'm not aware of a piece I have written in my career that tried to offer the kind of assessment of all of the available remedies in this context. I'd be happy to furnish the

court with a copy of my core syllabus where I spent two days in federal courts on the APA and associated remedies.

85 Q. All right. And that's a general federal court remedy?

A. Quite. 11:30

86 Q. And Prof. Swire, as you will have noticed, made no reference to it either?

A. Indeed.

87 Q. Okay. Now the third point, Professor, if I can ask you to return to your report. 11:30

A. Please.

88 Q. The third comment you make about the DPC Draft Decision relates to the remedy provided under section 1810?

A. Mm hmm.

89 Q. And if we can just look at what you say about this. 11:31 You say:

"*With regard to damages the DPC Draft Decision, like the Morrison & Foerster, is sceptical of the remedy because, as it correctly notes, 'this provision does* 11:31 *not operate as a waiver of sovereign immunity which means the US cannot be held liable under the section'.*"

You see that?

A. I do. 11:31

90 Q. Okay. You quote the **Al-Haramain** Islamic Fund case and you say:

"*But the DPC Draft Decision proceeds to suggest 'that*

the utility of pursuing individual officers may is [sic] questionable', without providing any substantiation."

And then you see use this phrase: "'*Officer suits' have always been the most common mechanism for obtaining discharges under US law when suing government official within their official capacity - entirely because of sovereign immunity concerns."* 11:31

Isn't that so? [No audible answer] 11:32

Then over the page: "*There is nothing untoward about the specter of suing an individual officer - for example the Director of National Intelligence - for unlawful surveillance, under section 10."*

Now, is that correct? Does the Director of National Intelligence not have *official* immunity?

A. So again I don't, we haven't had a lot of cases to test out this proposition. Official immunity, Judge, is a doctrine that's usually available at common law and so there would be a question under section 1810, if the fact that Congress had provided an express cause of action for damages for intentional or wilful misconduct was consistent with what has at common law been a good faith defence. 11:32 11:32

I can't answer that one way or the other because there

hasn't been a case specifically reaching that question.

91 Q. Is this not a problem you have highlighted and considered in your writing?

A. It is. I mean official immunity, Judge, as I mentioned yesterday, is a problem that comes up in many cases seeking damages against government officers. Even when sovereign immunity is not a problem, official immunity, the test the Supreme Court has articulated is that it must -- I am sorry. The officer must have violated clearly established law, that's the term in the case law, of which a reasonable officer would have known, so it's an objective test. 11:32 11:33

And I guess the only question I have, Mr. Murray, is in 1810. If you have a knowing and intentional violation, a context in which there is only liability if the officer has knowingly and intentionally violated FISA, it's not clear to me that defence would be automatically available. 11:33

92 Q. I mean you're talking about suing here the *director*. I mean the director isn't out implementing warrants, is he? What's his individual or her individual culpability? 11:33

A. I mean I think the question would simply be what is the violation? Is the violation a rogue officer on the line who has simply implemented his authority in a manner that's unlawful in which case obviously he or she would be the proper defendant, or is the challenge in fact to a larger programme that is itself being 11:33

enforced in a manner that is intentionally in violation of FISA, where, for example, some of the allegations against the Bush Administration were that the government was conducting these programmes knowing they were violating the statute based on a claim that the statute could not rein in the President's constitutional authority.

93 Q. Okay. Sorry, maybe I have misunderstood this, Professor, and please forgive me. You can have a range of different possible defendants? 11:34

A. Quite.

94 Q. You can start off at the top with the United States of America, that is --

A. So under 1810, not for damages, that's **Al-Haramain**.

95 Q. Precisely, because of sovereign immunity? 11:34

A. Correct.

96 Q. All right. You can go down the line, we'll say you will sue the director of the Central Intelligence Agency because this occurred on his watch?

A. Mm hmm. 11:34

97 Q. He will have, will he not, official immunity unless he is personally implicated in the wrongdoing of which you complain?

A. That's correct.

98 Q. Okay. So similarly the Director of National Intelligence is going to, who is the example *you* give in your report? 11:34

A. Hmm.

99 Q. Is going to have *official* immunity, save and insofar as

he or she is personally culpable for the actions of which the litigant complains; isn't that correct?

A. Yes, I agree.

100 Q. Okay. And then you come down the line again to the individual law enforcement officer who fails to execute the warrant properly or doesn't have a warrant or should know that the warrant is defective et cetera et cetera? 11:35

A. Or more realistically, Judge, in this context the operator at the National Security Agency who is knowingly violating perhaps the minimisation rule. 11:35

101 Q. Yes. So what are the circumstances in which the example *you* have chosen to give of the Director of National Intelligence going to be a defendant?

A. I mean I think it would be a context, Judge, where you had a programmatic allegation, that the government was not just collecting my data unlawfully but that the entire programme was being carried out in a way that was wilfully without regard to the relevant legal constraints. 11:35 11:36

102 Q. But in that circumstance a significant issue, on which you have written at some length, would arise as to the ability of the Director of National Intelligence to rely upon official immunity would arise?

A. That's right. 11:36

103 Q. Yes.

A. So Justice Kennedy has suggested in the context of **Bivens**, which we discussed yesterday, damages suits directly under the Constitution, that senior national

security officials might be especially entitled to defences in the context of these kinds of programmes unless you could show personal culpability. But again I mean personal culpability is a *merits* trigger to 1810 in the first place, right. You would have to show intentional and wilful conduct to even get in the court in the first place. 11:36

104 Q. Well, can we agree on this: Obviously none of this is relevant except insofar as you're talking about damages claims, the damages claims themselves are available, and I think you agree with the DPC evidence in this regard for wilful violations? 11:36

A. Mm hmm.

105 Q. And, even if you overcome that, you are going to potentially face issues with sovereign immunity and official immunity, depending on the nature of your claim, which may themselves present substantial obstacles to obtaining relief, would you agree with that? 11:36

A. I agree with all that. 11:37

106 Q. Okay. You say, incidentally, at paragraph 85 that: 11:37

"*In virtually every case in which section 1810 could apply the federal court government would almost certainly indemnify the officer defendant.*"

And you referred, if I understood your evidence correctly yesterday, to provisions in contracts, have you seen these contracts?

A. I've seen one. They are often referred to in literature and in scholarship. I have heard government officials refer to them in public. They are not generally publicised, Mr. Murray.

107 Q. And what do they say? 11:37

A. My understanding is that, the one I saw, and which I understood to be representative, is that the government holds harmless their officers for misconduct for damages liability that they incur. The term is within the scope of their employment. 11:37

108 Q. Yes. So an officer who, for example, decides to, to go back to the example that the judge or an analogous example you gave during the hearing, an officer who decides to obtain information or place surveillance on a person or disseminate information on a person for 11:38 entirely malicious and personal reasons is unlikely, I would suggest, to be acting within the scope of their employment even having regard to the broader definition of that term to which you referred yesterday, would you agree? 11:38

A. Maybe. I mean we discussed the torture example yesterday, Judge. I don't know the answer to that question. But I should just say, if we get to a point where we are outside the scope of the indemnification cause, we may also be outside the scope of any official 11:38 immunity defence, if at that point the officer has acted so wantonly conducted and recklessly as to have basically deprived himself of the cloak of official protection.

109 Q. But the obvious consideration that it depends on having an officer who is worth suing?

A. Indeed. I mean I assume, Mr. Murray, you would, I hope, Mr. Murray, you would agree with me that, even if the damages judgment is relatively minimal, the precedent it would set would be useful. 11:39

110 Q. Well, I have yet to meet the litigant who is interested in setting precedent.

A. Without regard to the bottom line.

111 Q. Can we move on to your fourth criticism which is the utility of the suppression remedy. And I think you agree with the DPC that this is really not something that affects her calculus at all, this is not a remedy that a person can voluntarily assume and agitate in the courts? 11:39

A. I agree with that, and I think I said that quite transparently in paragraph 86. I think, Judge, the point that I was trying to make here and frankly yesterday is that it seems like a consideration of whether US courts are in a position to provide remedies ought to at least account for, not give undue weight to, but at least account for circumstances in which the legality of the surveillance programmes are in fact being fully aired. 11:39

112 Q. All right. 11:40

A. And fully ventilated.

113 Q. Well maybe if we look at it this way: If you were providing for an academic audience and setting out to provide a comprehensive account of all possible

remedies which might enable clarification of the law, striking down of statutory provisions, invalidation of programmes, you would want to include these. You would want to include your criminal prosecutions, you would want to include your suppression remedy because, as we have seen in the **Mohamud** case, that can operate as a vehicle by which the law is determined? 11:40

A. And the internal remedies within FISA, the adversarial review that we saw in the **Yahoo** case, for example.

114 Q. Yes. Which I thought you thought might itself fall short of Article III because it doesn't go far enough in terms of creating a case or controversy? 11:40

A. Oh, I am sorry, no. When you actually have a meaningful adversary, Mr. Murray, I don't think there is any Article III problem. 11:40

115 Q. But anyway we'll stay on track, as it were.

A. I'm sorry.

116 Q. But you might include that in your academic commentary, but of course you understand the DPC was concerned with something else, which is the remedies available to an individual European who did not want to be prosecuted before they had the right to go to court and to that extent perhaps the suppression remedy is, as you describe it yourself, of limited use, you agree with all of that? 11:41 11:41

A. I do.

117 Q. Yes, okay. Let's move on then, the fifth point. I don't know that this is a criticism or omission, it's more an observation and it relates to Executive Order

12333. What you say here is that:

"*The DPC suggests existing remedies provide no basis for challenging the collection of data under non-statutory authorities such as EO 12333. 'It is not possible, the DPC concludes, to assess whether or not the remedies outlined above are sufficient to address the full extent of the activities of the intelligence authorities in question'. But, as described above, the non-statutory collection of authorities in question simply do not apply to EU citizen data held by US companies within the United States.*" 11:41 11:41

Is that absolutely true?

A. So if you are referring to the Transit Authority discussions? 11:42

118 Q. Yes.

A. I think that is well covered by the expert document, Judge. I think that statement, Mr. Murray, is true, right. That if the data is physically held by US companies in the United States, that's not a Transit Authority situation. 11:42

119 Q. Okay. But certainly, insofar as transit intrudes, so does Executive Order 12333?

A. And I think you have, and I join without any hesitation the expert document discussion of Transit Authority in that regard. 11:42

120 Q. And also, I think, join without any hesitation in comment on the absence of any effect of judicial

remedies over the executive order?

A. True.

121 Q. Yes. Do you think the Privacy Shield provides a bulwark against surveillance under Executive Order 12333? 11:42

A. I think it's better than nothing.

122 Q. Very good. Okay, thank you.

A. I think -- you know I, as you pointed out yesterday, Mr. Murray, I have more faith in judicial remedies in this context. 11:43

123 Q. Yes, very well and it doesn't provide one full stop. Can we move on to your sixth point which is Article III standing and we addressed this --

A. We haven't discussed this nearly enough.

124 Q. We addressed this yesterday and for the very reason suggested by your comment, Professor, with which I suspect *nobody* in court will disagree -- 11:43

A. That's a first.

125 Q. -- we're going to very briefly, only very briefly just reprise on this before we move on to your seventh criticism. Because I think at the end of the day, and please disagree with me if you do, that at the end of the day the difference between you and the DPC might not unfairly be characterised as one of emphasis? 11:43

A. I think emphasis may undersell it a little bit, if you'll give me one moment to elaborate. 11:43

126 Q. Of course.

A. The problem that I had with the DPC's discussion, Judge, and I hope this comes through in my report, is

that it's not that standing isn't a consideration, it's that we have to be very specific about which part of standing doctrine is the problem. You heard a lot of discussion yesterday about the actual or imminent prong versus the concrete and particularised prong. It seems to me that the special focus of the DPC draft was the former, was the actual or imminent prong, where again I think the critical point is how that would play out in the different stages of litigation. Then we had the additional questions about concreteness raised largely by the November memo by Mr. Serwin and by the expert report by Mr. Richards - sorry, Prof. Richards, I don't mean to demote him - where I think that's a related but distinct concern. 11:44 11:44

And so it's not just point of emphasis, if I may. I think it is understanding the different work that the concerns that folks like I share right in this field, how that cashes out when you get to a real case with standing. 11:45

127 Q. And we agree, clearly as we all must, **Clapper** governs, we know what the test is, certainly impending. You used a formula yesterday *"has or will shortly survey"*, that test, could I respectfully submit to you or suggest to you, were it the test would have resulted in a different outcome in the **Wikimedia** case, and I suspect you are arguing that the **Wikimedia** case was wrong for that reason, but in fact, and the court has heard of the **Wikimedia** case, again probably too often 11:45

at this stage, but certainly the district court decision is not consistent with your formula?

A. I completely agree with that. And if I may, Judge, just to make this as concrete as I can, I don't mean that in the standing sense. The flaw in the district court decision in the **Wikimedia** case is missing the distinction that we have adverted to between the motion to dismiss stage and the summary judgment stage. The district court in the **Wikimedia** case was very troubled by the plaintiff's inability to demonstrate various points that at the motion to dismiss stage they really only have to allege, right, and quoted **Clapper** where, because it was at the summary judgment stage, that was a proper concern. 11:45 11:45

So this is part of why I think we could get a very, frankly limited, reversal by the Court of Appeals, not holding that the plaintiffs have standing, but, as in **Valdez** and **Schuchardt**, holding that they at least had enough to survive a motion to dismiss and then, per our discussion yesterday, we would get to discovery. 11:46 11:46

128 Q. In any event, Professor, as you said we have discussed it at length, but we come to this point of agreement which is that it's a substantial obstacle?

A. Quite. 11:46

129 Q. I just want to draw your attention to one decision really for the sake of completeness because, you may be aware of this, that the United States district court in eastern district of Pennysylvania has very recently, as

in the last couple of weeks, adopted a different conclusion to that adopted in the **Microsoft** case regarding the implication of electronically transferring data from a server in a foreign country, I just want to draw your attention very quickly to one --

A. Thank you.

130 Q. -- passage in it which is, if you turn to - sorry this is a search warrant and the number is given to Google. If you turn to page 20 of that, hoping that your version is the same as mine, you should have a page that begins *"electronically transferring data"*? 11:47

A. I do.

131 Q. And this follows a consideration of the **Microsoft** case: 11:47

"*Electronically transferring data from a server in a foreign country to Google's data centre in California does not amount to a seizure - obviously under the Fourth Amendment - because there is no meaningful interference with the account holder's possessory interest in the user data.*" 11:47

You recognise that language, Professor, and you will understand jurisprudentially where it comes from and why that is used? 11:47

A. I do.

132 Q. "*Indeed according to the stipulation entered by Google and the government, Google regularly transfers user data from one data centre to another without the*

customer's knowledge. Such transfers do not interfere with the customer's access or possessory interest in the user data. Even if the transfer interferes with the account owner's control over his information, this interference is de minimis and temporary." 11:48

And I just draw that to your attention, conscious obviously that the **Microsoft** case posited a different conclusion, but perhaps with a view to getting your, to getting you to agree at least with this: That there is, around issues such as retention, around issues such as transfer as opposed to access certainly questions as to the extent to which these are, and I know this is, you would say, a merits rather than a standing issue, these are cognisable harm, would you agree with that? 11:48

A. With the caveat you just mentioned, then I think that's a question of the merits of the Fourth Amendment concern, Judge, and not an obstacle to allege of a violation sufficient to allow a court to reach the merits. Yes, of course. These are, as I think I mentioned yesterday, there are, the academic in me would say fascinating and the litigator in me would say troubling open questions about how the Fourth Amendment applies here, but I really do think it's important to stressing that those are merits questions. 11:48 11:49

133 Q. Your seventh point, which is forward at page 96, because we discussed the various decisions to which you refer, your seventh point is about Rule 11. And I think you do understand the point which Mr. Serwin is

making here, he elaborated upon it in the course of his evidence, that it's, I suppose, a chilling effect, as he sees it, for attorneys. If someone comes to you and says 'I have an objectively reasonable apprehension that I am being surveyed' and you say 'well, have you anything more' and I say 'no', then perhaps some attorneys might say 'well there's a Supreme Court case that says that won't work and I'm not putting my name or my personal assets on the line to sign your writ'? 11:49

A. Mr. Murray, I don't know doubt that there is some attorney that will say something, of anything of that sort. The point I was just trying to make about rule 11 is I have never heard it referred to by an attorney in this context, I have never seen it invoked in a court in this context and so it struck me as an odd point of emphasis for the DPC. 11:49 11:50

134 Q. All right. Then, finally, your eighth and final point relates to the Judicial Redress Act and the Privacy Act. I don't think you disagree with the substantive conclusion posited by DPC, you simply make an observation that perhaps there's a confusion between merits, harm and standing? 11:50

A. And if I may just add one piece to that and that perhaps the DPC in focussing on the difficulties that plaintiffs will have under **FAA -v- Cooper** establishing damages, assume that that would also be a difficulty to injunctive or declaratory relief. 11:50

135 Q. Certainly. But you certainly and don't for a moment dispute the difficulty of obtaining damages because of

those decisions?

A. After **Cooper**, certainly.

136 Q. That really seems, Professor, to take us to the following points of conclusion on your eight points: Two of them are matters in which we appear to agree, subject to the proviso you have just made in relation to your interpretation of the DPC's interpretation of **Cooper**, but we appear to agree in fact on 12333 and the JRA and Privacy Act; isn't that right, that's two of them? 11:51

A. I think so.

137 Q. That leaves six. Two of them relates to provisions which are not judicial remedies of general application at all, the criminal prosecution and the suppression remedy, okay, that so leaves us with four; one relates to standing, which we agree is a substantial obstacle, one relates to the APA, which you agree has limitations and I don't think you disagree significant limitations attached to it? 11:51

A. Again I don't know about the adjective. I think we can certainly agree on limitations. 11:51

138 Q. Well, the court has heard all of the limitations?

A. Indeed. They certainly *can* be significant.

139 Q. Yes, and I'm going to submit to you that they are significant. One relates to immunity and damages which are hard to get anyway, we agree with that, and the last one relates to Rule 11? 11:52

A. Mm hmm.

MS. HYLAND: I think there might have been a question

there that Prof. Vladeck didn't get an opportunity to answer. I think he was asked in relation to, Mr. Murray said one relates to immunity and damages which are hard to get anyway, we agree with that.

MR. MURRAY: And he nodded. 11:52

MS. HYLAND: And the last one relates -- well...

A. I did not, I'm sorry. Yes, I mean I think that our colloquy articulated why I think they are hard to obtain but not impossible. 11:52

And if I can just, if you don't mind my just making one reflection. The point I think is perhaps that Mr. Murray, and I don't think there is as much daylight as it seems, but I would have liked to have seen all of these points articulated by the DPC, that is to say 11:52 'yes, perhaps these remedies aren't as robust as I would like them to be', 'yes perhaps the obstacles that Mr. Murray is worried about are still present'. It struck me that the DPC Draft Decision that I read didn't walk down any of these paths in nearly 11:53 sufficient detail to explain exactly where the real problems are, Mr. Murray, and where I think it is overgeneralising in ways that are unhelpful.

140 Q. **MR. MURRAY:** Yes. Well, you bring a particular perspective to those questions -- 11:53

A. I do.

141 Q. -- and look at it from a particular perspective, but the one thing we do agree upon, although we may use the words in different ways, is that the remedies are not

adequate, and you said that yesterday?

A. They are not adequate to my taste.

142 Q. Thank you.

A. I will leave to the court whether they are adequate for relevant purposes. 11:53

MR. MURRAY: Thank you, Professor.

A. Thank you.

PROF. VLADECK, WAS CROSS-EXAMINED BY MR. McCULLOUGH AS FOLLOWS:

143 Q. **MR. McCULLOUGH:** Professor, you divide your report into three parts, one dealing with US collection authorities, one dealing with constraints on those authorities and then, thirdly, remedies for abuses? 11:53

A. Mm hmm.

144 Q. I don't want to ask any questions about the third, you and Mr. Murray have covered that in some detail, and I have just a few questions about the first and second.

A. Please. 11:54

145 Q. The main US collection authorities you summarise at paragraph 52 of your report, that's section 2703(d) orders under the Stored Communications Act, National Security letters, FISA warrants and Section 702 of FISA? 11:54

A. Just to clarify, Judge. As the introductory text of that paragraph suggests I was referring to the key authorities for data of EU citizens that would be held by US companies within the US. There are of course

other authorities relevant to other contexts.

146 Q. And the main extant authority that you discuss in your report that is used to collect intelligence on non-US persons by electronic surveillance is really Section 702? 11:54

A. 702 of the data is in the United States, certainly.

147 Q. All right. I just want to look very briefly at the structure of that to see if we agree, and I don't think there is any disagreement here, Professor. Section 1881(a) sets out a very basic structure? 11:55

A. Would you mind if I just got it in front of me?

148 Q. Sure, yes.

A. Can you point me to where in the authorities it is.

149 Q. Yes.

A. I just don't want to mess anything up. 11:55

MR. McCULLOUGH: I'm going to have it in a different place to you now, Professor, so you'll just have to wait for a moment.

MS. JUSTICE COSTELLO: I think it's Tab 3 of Book 1 of the US authorities. 11:55

A. Thank you very much. I am sorry. Thank you, Judge. Okay, yes, I'm there. It's page 249 on my copy.

MS. JUSTICE COSTELLO: Hmm.

150 Q. **MR. McCULLOUGH:** All right. And the basic structure permits surveillance on any person reasonably believed to be a non-US person as long as a significant purpose is to obtain foreign intelligence? 11:55

A. That's correct.

151 Q. All right. And there are two programmes under

Section 702 the extent of which we are aware; isn't that correct?

A. Yeah.

152 Q. And it follows that there may be more?

A. I don't know that it follows, Judge. I think there are two programmes which we are aware. I have some faith that if there were additional programmes, we have benefitted from many leaks in US law in the last five, six, seven years, so I am cautiously optimistic that if there was a third programme we would have heard about it. But obviously I'm not in a position to answer that definitively. 11:56 11:56

153 Q. And certainly we can't know whether more aren't going to be created in the future?

A. Of course. 11:56

154 Q. And it's quite likely that a feature of further programmes if they are created is that we won't be told about them?

A. Maybe, although it is worth stressing in this regard that my concerns about the USA FREEDOM Act, notwithstanding there were a couple of salutary developments for transparency, and that there may in fact be at least some marginal pressure to publicise more about these developments going forward given the consequences we have seen from the secrecy that surrounded these programme previously. 11:57 11:57

155 Q. We only know about PRISM and Upstream because Mr. Snowden told us about them really; isn't that right?

A. We only know about Upstream because of Snowden. I think we knew that there was something like PRISM. I mean after all **Clapper -v- Amnesty International** was predicated on the notion that there was a programme like PRISM, we just didn't know what it was called. 11:57

156 Q. Sure. If you just look at what you said in your 2014 article that you were given yesterday, and I don't know if you still have a copy of that. I will just read out what you said at page 569?

A. Mm hmm. 11:57

157 Q. And you were talking about a **Clapper** fix. This was a legislative proposal that you put in your article whereby the problem in **Clapper** might be fixed?

A. Yeah.

158 Q. And you continued: *"Ultimately the larger problems with such a **Clapper** fix are not legal but practical. For starters there is little reason to believe disclosure of the programme such as PRISM are going to become a recurring feature of American public discourse, or even that we now know about all of the potentially unlawful secret surveillance to which US persons are currently being subjected."* 11:57 11:58

A. That's right. Judge, the only thing I would say is I wrote that before the USA FREEDOM Act which, as I mentioned in my colloquy with Mr. Murray, I have been critical that it didn't go far enough. But I think that there are some beneficial reforms that Congress has adopted that I hope but obviously can't say with confidence will lead to more public awareness of future 11:58

programmes.

159 Q. All right. And one of the risks to which you pointed in your article there is the possibility that the future of such programmes might be created on the basis of statutory authority less clear than Section 702? 11:58

A. Which we what we saw with the phone records programme. I mean the real controversy about the phone records programme wasn't the underlying conduct because it was metadata, it wasn't content. The controversy was that it was so difficult to interpret the statute the way 11:59 that the government apparently did. And so at least among lawyers the real objection to the 215 programme was the legal interpretation. This is why there has been so many attention to increasing adversarial litigation before the FISA court to make sure that 11:59 there is meaningful opportunity for the judges to receive contrary interpretations of the same text.

160 Q. Let's just be clear: Section 702 doesn't forbid the creation of future programmes; isn't that correct?

A. That's right. 11:59

161 Q. Different programmes?

A. That -- I mean nothing in 702 says you cannot have another programme called Downstream.

162 Q. Exactly.

A. Right? The key is whether the judicial review, I don't 11:59 mean that as a term of art, whether the role of the FISA court in supervising this new programme would be aided materially by the new amicus, by the new transparency rules or whether we could have a repeat of

what happened with the phone records programme.

163 Q. And, as you say in your 2014 article, there is also a risk that programmes will be created otherwise than under Section 702?

A. Of course there's a risk. 12:00

164 Q. Yes. As you say, I'll just read it out: *"And to the extent"* --

MS. JUSTICE COSTELLO: Sorry, what page are you on again, please, Mr. McCullough?

MR. McCULLOUGH: Page 569, Judge, of the 2014 article. 12:00

MS. JUSTICE COSTELLO: Thank you.

A. This is the standing and secret surveillance?

MR. McCULLOUGH: Standing and secret surveillance. The foot of that page, Judge.

MS. JUSTICE COSTELLO: Yes. 12:00

MR. McCULLOUGH: "*And to the extent that current or future programmes are based upon statutes not remotely as clear in their potential scope as Section 702, the absence of such disclosures would likely be fatal to the ability of plaintiffs to satisfy even the lower* 12:00 *standing threshold proposed above*".

And what you had in mind there was (a) that there might be future programmes created otherwise than under Section 702, (b) that you might never hear about them? 12:00

A. Mm hmm.

165 Q. And (c) that naturally that means that you would never achieve standing; isn't that right?

A. Certainly I think it would be very difficult, Judge,

contra my colloquy with Mr. Murray where I think in a 702 Upstream case now we know enough to easily survive a motion to dismiss. I do think it would be much harder to survive a motion to dismiss if my allegation was simply that I believed that my communications were being collected pursuant to a completely secret programme no one had ever heard of.

Now without slamming the door on that, though, I would like to refer the court back to the **Valdez** case. The claim in the **Valdez** case is, to my mind, somewhat fantastical, right, but that the National Security Agency was engaged in a comprehensive domestic surveillance programme in and around Salt Lake City in the run-up to and during the 2002 Winter Olympics. There is *no* public data to support that claim and yet even those allegations survived a motion to dismiss.

So I think the question would simply be whether there is enough plausibility given the history to survive motion to dismiss and then we would get, Judge, back to discovery where we have the same question about the ability to discover the information. Just to finish the thread, it's possible then that state secrets would become a larger issue in the context of a completely secret programme versus in the context of 702 and PRISM.

166 Q. I don't want to go back over all the territory with Mr. Murray?

A. I am sorry.

167 Q. That's all subject to all the discussion about standing that you have already heard; isn't that correct?

A. Correct, quite.

168 Q. Just look then at the two programmes of which we do know. 12:02

A. Mm hmm.

MR. McCULLOUGH: You describe those as paragraphs 45 of your report.

MS. JUSTICE COSTELLO: I think we just need to change stenographer. 12:02

169 Q. **MR. McCULLOUGH:** Yes. At paragraph 44 and 45 of your report. At paragraph 44 you discuss PRISM. And that's a programme under which the government sends a selector, such as an e-mail address, to a United States 12:03 electronic communications service provider and the provider is compelled to give the communication relating to that selector back to the NSA, isn't that correct?

A. Mm hmm. 12:03

170 Q. Then there's Upstream, that you describe at paragraph 45. As I understand Upstream, again just to, I suppose, reduce it to shorthand, Upstream has two phases; first, there's a phase at which *all* the internet traffic passing over a particular internet 12:03 point is analysed so as to extract the material, is that correct?

A. That's my understanding of it.

171 Q. And then secondly, the extracted material is then

retained by the NSA for further analysis?

A. Subject to the targeting and minimisation rules, yes.

172 Q. Subject to the targeting and minimisation rules, to which I'll come. But they are largely designed to protect US persons, isn't that correct? 12:03

A. They are.

173 Q. All right. And we'll just look at what you say about what *is* collected under Upstream. There's "to" and "from", isn't that correct?

A. Indeed. 12:04

174 Q. And then there's "about". And the PCLOB report says that an "about" communication is one in which the selector of a targeted person is contained within the communication but the targeted person is not necessarily a participant in the communications. 12:04 That's "about", is it?

A. Yeah.

175 Q. Then what's an MCT?

A. So an MCT is a multiple communication transaction. I think Prof. Swire talked about this a bit, Judge. Just 12:04 the way internet traffic is routed, you'll have a number of items bundled together, right, a number of e-mails or chats or whatever. And so in an MCT, it's not possible at the moment of collection to segregate the individual items, that you collect the packet and 12:04 then extract from the packet the relevant triggered material.

176 Q. All right. And in addition to those that you mention in your report, I think you agree with Mr. Murray that

EO12333 also *does* have a relevance?

A. Only in the context of the transit authority, Judge, which I think the experts' document talks about. And I think it's just worth stressing, transit authority is, for lack of a better word, transitory, right, that if the issue is about the actual collection off of servers in the US, I think we're really talking about 702, not 12333. 12:05

177 Q. Well, let's just look at what you say in your report about 12333. You mention it at paragraph 38, but perhaps more again at 88. 12:05

A. Mm hmm.

178 Q. At paragraph 88 you're setting out one of your seven criticisms of the DPC's draft decision, and you say:

"*But as described above, the non-statutory collection authorities in question simply do not apply to EU citizen data held by US companies within the United States.*" 12:05

You've modified *that*, I think, in the expert report, isn't that correct? 12:06

A. So, Judge --

179 Q. Or the joint experts' report.

A. -- I hope I was clear before, but just to take one more shot at it. I think this sentence is still correct, right? That is to say, if the data is physically held by technology firms, by Facebook, by other service providers in the US, that's not transit authority, 12:06

right, that's 702. The transit authority issue is while the data is physically in transit. And so I think the expert report helpfully explains that that is also a relevant consideration. I don't think that changes the voracity of the statement. 12:06

180 Q. I understand that. But 12333 is relevant to the issues under discussion in this case, because it's relevant to electronic surveillance of EU citizens' data in the US?

A. So, I would just say it is relevant of EU citizens' data en route to the US. Once it's in the US, I think there's no question, Judge, that 702 applies. 12:06

181 Q. We'll just look at what the joint experts' report says about that on page nine, item six. You're talking about the relevance of EO12333.

A. Yes. 12:07

182 Q. And the agreed position, I think, is that that programme is generally conducted outside of the US, it is *not* conducted within the US, with the exceptions for transit authority and certain radio collection discussed elsewhere in the chart. 12:07

A. That's right.

183 Q. All right. So just tell me what you know about the transit authority and the radio communications?

A. So I mean, this is, I should confess, Judge, this is more Prof. Swire's bailiwick than mine, so I have more of an amateur knowledge. But the transit authority is the ability of the government, while information is literally en route across fibre optic cables, while it's physically outside the United States, to at least 12:07

attempt to collect some of it while you might have -- and it's sort of tied to radio communications, because you might be intercepting over-the-air radio signals, back in the day where we still used those.

12:07

So these are certainly *relevant* to the conversation. I think they're -- part of why I think they're not at the heart of *my* report is because I think the general fear in the context of data transfer is that it's going to be when the government goes to the firm to acquire the 12:08 data that the issues are going to arise, not -- we're not aware, to my knowledge, of transit authority being used in this manner.

184 Q. But you get it directly from firms?

A. To get it directly from firms. 12:08

185 Q. Sure. Just look at what is said at page 12 as well, item 12.

A. Mm hmm.

186 Q. The agreed position is:

"*The experts agree that Transit Authority under EO12333 is an exception to the general rule that EO12333 applies to collection only outside of the US. The experts' understanding is that transit authority would apply, for instance, to an e-mail that went from a foreign origin, across the telecommunications network within the US without having a US destination, and then went to a foreign destination. Transit authority would likely not apply to the e-mail if its destination was a*

corporate server in the US that forwarded the e-mail to a destination outside the US".

A. Mm hmm.

187 Q. So we're talking about traffic that goes across the US, intending to be routed out of the US. 12:09

A. And never really lands in the US, if I can use that metaphor.

188 Q. All right. And as I understand it - and you may or may not know about this - it could easily *be* the case that as far as *I'm* concerned, I'm sending a communication 12:09 from here to somebody else in Dublin, but in fact it may go across the US?

A. Indeed. And I think I -- I don't remember if I cite this in my report or not, but there's a very good article called "The Unterritoriality of Data" that I 12:09 think has a very useful discussion of this problem.

189 Q. All right. So a lot of data that appears to the ordinary person never to go near the US may *in fact* go through the US and then be subject to 12333?

A. Well, yes. Although, Judge, just to be clear, I mean, 12:09 if a Russian national is communicating with another Russian national, it's the same regime either way, right? So let me just elaborate. Two Russian friends, one in Moscow, one in St. Petersburg e-mailing with each other, they may know/they may *not* know that the 12:10 nature of the servers they use routes the traffic through the US or not. I think everyone would agree that if the material never went through the US in the first place, the relevant US surveillance regime would

be 12333 - we have non-US persons outside the United States communicating only with each other through non-US media.

And so I think in that regard, transit authority is simply accounting for the interoperability of modern data transfer, where if it's unbeknownst to those two Russian citizens the data is routed through the US en route from Moscow to St. Petersburg, 12333 is still the relevant regime. So in other words, the fact that it's routed through the US, transit authority fills the gap in that regard, it doesn't create a new problem from my perspective. 12:10 12:10

190 Q. And I think you agree, as you said to Mr. Murray, that there's no effective legal remedy in relation to 12333? 12:10

A. Certainly.

191 Q. All right. Then in the second part of your report you talk about certain constraints. I just want to look very briefly at them. At paragraphs 55 and 56 --

A. Sure. 12:11

192 Q. -- you talk about the Fourth Amendment.

A. Mm hmm.

193 Q. And in essence, the Fourth Amendment is unlikely to play any role in the discussion that is in issue in this court, I think, isn't that correct? 12:11

A. I'm not sure. I mean, Judge, I hope I've been clear that there's an open question about whether, if the data is held in the US and, if I may, *known* to be held in the by a non-US person where the Fourth Amendment

might still apply, that's an open question in the courts. Certainly I mentioned the **Hernandez** case a couple of times, Judge, where there's an open question about whether the Supreme Court is still going to follow the brightline on/off switch at the border for Fourth Amendment protections. What I hope was clear from my colloquy with Mr. Murray is that certainly the precedent *right now* would seem to disfavour application of the Fourth Amendment to a non-US person in that context, but that the law is evolving. And I want to hopefully not hide the ball on how it is evolving. 12:11 12:11

194 Q. And you cover that in paragraph 55. You say in the context of the data -- context of data of EU citizens held by US companies, the Fourth Amendment is *less* likely to play a role. 12:12

A. Mm hmm. Quite.

195 Q. And that's precisely *because* of authorities such as **Verdugo**, isn't that correct?

A. Indeed.

196 Q. Then in the final sentence of that paragraph you say the Supreme Court hasn't addressed whether the Fourth Amendment might apply to searches of these individuals' data for data located within the United States. The prevailing assumption is the answer is no. And if the answer is no, well, then the Fourth Amendment really doesn't play any part, isn't that right? 12:12 12:12

A. If the answer is no. You know, I'm cautiously optimistic that the Supreme Court won't be able to take such a, if you'll forgive me, Westphalian approach to

data, because I think data poses challenges to that very traditional sovereignty driven model.

197 Q. Certainly we can agree that the prevailing authority --

A. Yeah, quite.

198 Q. -- the Supreme Court authority, suggests the answer is no? 12:12

A. I agree.

199 Q. All right. And then you deal with constraints on Section 702.

A. Mm hmm. 12:13

200 Q. Now, Section 702 in itself, I think, contains a few protections for non-US persons?

A. That's correct.

201 Q. It's designed primarily, insofar as it *has* protections, to protect US persons, isn't that right? 12:13

A. That's correct.

202 Q. And you say at paragraph 62 that that is so, but that one of the central reforms of PPD-28 is to expand the application of those principles to collection of non-US person data as well. And you refer to section 2 of PPD-28 and then below that you refer to section 4 of PPD-28. 12:13

A. Mm hmm.

203 Q. And I just want to talk about that for a moment, if I may? You'll find PPD-28 in book three, tab 43. 12:13

A. I think I have it. Just give me one moment.

MS. JUSTICE COSTELLO: What's the tab again, sorry?

A. Tab forty --

MR. McCULLOUGH: Tab 43, Judge.

A. 43. Yeah, I see it.

204 Q. **MR. McCULLOUGH:** Just before we look at the parts of it to which you refer, it's a Presidential Policy Directive.

A. That's correct. 12:14

205 Q. What's the difference between a PPD and an EO?

A. Formally, there's not that much of a difference. A PPD tends to be more targeted towards a very particular substantive field. It tends to be -- as its language suggests, it's a directive to agencies that this is how 12:14 they're supposed to comport themselves going forward. And so it has the same force as an Executive Order. I think, Judge, if anything it's just a little more targeted and specific.

206 Q. It's not a legislative act? 12:14

A. No.

207 Q. And it's open to be changed tomorrow by the President, if he so wishes?

A. Certainly.

208 Q. All right. And the first part of PPD-28 to which you 12:15 refer is section 2.

A. Mm hmm.

209 Q. And the first paragraph of section 2 says that the US must collect signals intelligence in bulk in certain circumstances. 12:15

A. Mm hmm.

210 Q. Then it's the next paragraph I think to which you refer in your report.

A. Yeah.

211 Q. "*In particular, when the US collects non-publicly available signals intelligence in bulk, it shall use that data only for the purpose of detecting and countering.*"

12:15

And then it gives six purposes for which bulk signals -- sorry, signal intelligence collected in bulk may be used.

A. Mm hmm.

212 Q. Now, in fact I think as far as the US Government is concerned, neither PRISM nor Upstream fall within this category, isn't that correct? 12:15

A. Fall within the category of PPD-28.

213 Q. Yes, fall within the category that is protected by section 2? 12:16

A. So the US Government does take a strange definition of what "bulk" is. But I had always understood the government to nevertheless believe that it had to ascribe to the same purposes when collecting under PRISM -- that it couldn't collect for arbitrary reasons under PRISM and Upstream. 12:16

214 Q. Well, PRISM, at least as far as the US Government is concerned, is targeted, isn't that correct?

A. Yes.

215 Q. All right. So it doesn't -- 12:16

A. Through the selectors.

216 Q. -- it doesn't appear to fall within the definition of bulk collection, isn't that correct?

A. Not the way the government defines it, no.

217 Q. Yes. And do you see footnote five is referenced in the first paragraph of section 2?

A. Yeah.

218 Q. If you look at footnote five, if you wouldn't mind turning to that? 12:16

A. On page 12? Yeah.

219 Q. Page 12, yeah.

"*The limitations contained in this section do not apply to signals intelligence data that is temporarily* 12:16 *acquired to facilitate targeted collection. Reference to the signal intelligence collected in bulk means the authorised collection of large quantities of signals intelligence data which, due to technical operational considerations, is acquired with any use of* 12:16 *discriminants, that is specific identifier selection terms.*"

So the first sentence, "*The limitations contained in this section do not apply to signals intelligence data* 12:17 *that is temporarily acquired to facilitate targeted collection*", that looks as if - at least as far as the government is concerned - section 2 doesn't apply to Upstream either, isn't that right?

A. It may not. Although I guess, you know, in that regard 12:17 it's important that I think section 4 doesn't have the same caveats.

220 Q. All right. Well, let's just look at section 4 then. The parts of section 4 to which you referred are under

policies and procedures.

A. Yeah.

221 Q. That's 4(a)(i), "Minimisation". And there's two bullet points on page seven. I think they're the ones you were referring to in particular, is that right? 12:17

A. Mm hmm.

222 Q. And they provide for certain protections for the dissemination and retention of material for non-US persons. I think that's what you were referring to in your report, is that right? 12:17

A. It was, that's right.

223 Q. So these say that:

"*Dissemination. Personal information shall be disseminated only if the dissemination of comparable* 12:17
information concerning US persons would be permitted under section 2.3 of Executive Order 12333.

Retention. Personal information shall retained only if the retention of comparable information concerning US 12:18
persons would be permitted under section 2.3 of Executive Order 12.3 and shall be subject to the same retention period as is applied to comparable information concerning US persons. Information on 12:18
which no such determination has been made shall not be retained for more than five years unless the DNI expressly determines that continued retention is in the national security interests of the US."

Let's just deal with retention for a moment, if I may?

A. Please.

224 Q. As I read that, Professor, it's suggesting that you get the same -- PPD-28 says you should get the same protections for a non-US person as section 2.3 of Executive Order 12333 provides? 12:18

A. That's how I read it.

225 Q. All right. But it appears also to be saying that at least as far as retention is concerned, if no determination in that regard is made in favour of the non-US person, you can still retain it for five years, is that right? 12:18

A. So, you know, I guess I've always wondered what that sentence meant in this context. I think it's certainly true that it seems to suggest that there are some categories of such information. But I guess it's not clear to me what the determination that that sentence is referring to is. 12:19

226 Q. Well, on the face of it, Professor, it appears to be referring to the determination made above, that's to say whether you are, if you like, entitled to the protection for which section 2.3 of 12333 provides. 12:19

A. Oh, I see, if it was entitled to the same -- right. And "*no such determination has been made shall not be retained for more than five years.*" So I guess I had understood this language to be setting basically a default destruction rule, that whatever else, whatever other authorities there were for retaining that information, once you reach five years there is no 12:18

continuing justification. And then the question becomes whether there's still a reason at that point, and the DNI has to certify.

227 Q. All right. So it looks as if *anything* can be retained for five years, or *longer* if the DNI thinks so, is that right? 12:20

A. I mean, I think retained perhaps, but with the caveats that section 2.3 of 12333 require.

228 Q. Sure. All right. Can I just then look at the protections for which -- 12:20

A. Sorry, Judge, just to be clear, part of we're talking about here is not just retention. It's easy enough to put the data on a server and lock it away until the five-year clock runs. The question is who's going to have access to that data during this time period and for what purposes? And those are the subjects that, if memory serves, section 2.3 are at least trying to address. 12:20

229 Q. Well --

A. I'm sorry, I didn't mean to go on a tangent. 12:20

230 Q. No, no, not at all. Can we look at 12333 then? And you'll find that at tab 45.

MS. BARRINGTON: Judge, I wonder if I might just intervene at this stage to say that it has come to *our* attention that the version of 12333 which is in the documentation is an old version. It has been amended on a number of occasions and we have the up to date version in court that we can hand in, Judge. 12:20

MR. McCULLOUGH: All right. Well, let's hope it's not

very different, Judge, because I've certainly been working off the old one.

MS. JUSTICE COSTELLO: I take it the parties have no difficulty --

MR. MURRAY: Well, subject to seeing it, Judge, certainly. But it can be handed up and we'll -- 12:21

MR. GALLAGHER: No, it says December 4, 1981. And there have been later versions.

MS. BARRINGTON: Yes, it was amended most recently in 2008. And the version we have, Judge, is the amended version. 12:21

MS. JUSTICE COSTELLO: Very good, thank you.

(DOCUMENTS DISTRIBUTED)

12:21

231 Q. **MR. McCULLOUGH:** So let's just summarise --

MS. JUSTICE COSTELLO: Sorry, the witness hasn't got it yet.

232 Q. **MR. McCULLOUGH:** Sorry, my apologies (Same Handed). So let's just summarise where we are. 12:22

A. Yeah.

233 Q. The impression that one *might* have gained from your report is that the effect of PPD-28 is to give non-US persons the same protections as those for which FISA otherwise provides. 12:22

A. Mm hmm.

234 Q. Whereas in fact the effect of PPD-28 is to give non-US persons the same protections as those for which section 2.3 of Executive Order 12333 provides, isn't that

correct?

A. So I mean, I guess, Judge, I don't -- looking at my report, I don't think I said they were the same. And I think there are important distinctions, as Mr. McCullough has pointed out. I think the key to PPD-28 is that prior to its promulgation there were, to my knowledge, *no* comparable minimisation requirements of any kind for non-US person data. And so what I tried to do in my report in paragraphs 61 through 64 was to spell out how there are new protections, that may or may not be commensurate - I mean, I think they're *not* commensurate. 12:22 12:23

235 Q. But they're not. Exactly. And that's what we need to look at, Professor, just to make it quite clear that they're not at all commensurate. If we look at 2.3 - and I don't think this is different in the new version, in the time that I've had to compare them. 2.3 is the relevant part of it. This isn't paginated, I'm afraid, so we'll just have to find the page. Section 2.3 is the part to which reference is made in PPD-28, isn't that correct? 12:23 12:23

A. Quite, yeah.

236 Q. So 2.3 provides:

"*Elements of the Intelligence Community are authorised to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or the head of* 12:23

a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. These procedures shall permit collection, retention and dissemination of the following types of information."

And then it sets out (a) to (j).

A. Yeah.

237 Q. So (a), for instance, is: 12:24

"*Information that is publicly available or collected with the consent of the person concerned;*

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organisations."

Can we can just pause for a moment, Professor, and if you wouldn't mind moving forward to the definitions? 12:24

A. Sure. In the Executive Order?

238 Q. In the Executive Order. Which you'll find some pages forward. Three pages forward, I think.

A. Yeah, 3.5. 12:24

239 Q. Do you see the definition of foreign intelligence?

A. I do.

240 Q. This is, I think, a wider definition even than you find in FISA?

A. It is.

241 Q. It says:

"*(e) Foreign intelligence means information relating to the capabilities, intentions and activities of foreign governments or elements thereof, foreign organisations, foreign persons, or international terrorists.*"

So at its minimum, foreign intelligence means information relating to the activities of foreign persons. That's foreign intelligence. 12:25

A. As the Executive Order defines it, Judge. The only point I would make is there are agency specific minimisation procedures, several of which I reference if my report, that are in some cases narrower. But yes, the Executive Order does define it very broadly. 12:25

242 Q. Well, the PPD merely requires that you comply with section 2.3.

A. Mm hmm, that's correct.

243 Q. 2.3 requires you to comply with procedures. And the procedures must at least do *this*, isn't that right? 12:25

A. Yes.

244 Q. And the least that the procedures must do is ensure that collection, retention and dissemination of the following types of information is permitted, that's information constituting, inter alia, foreign intelligence. And we know that that means information relating, for instance, or by example, to the activities of a foreign person? 12:25

A. At least as it's defined.

245 Q. All right. So if that's so, that means that all that 12333 provides is that you have procedures that permit you to retain information of, information relating to the activities of a foreign person? 12:26

A. So I still -- I mean, my understanding, Judge, is that there's still a requirement that there be some legitimate purpose - I believe the Executive Order uses the word "legitimate" - that it can't just be because we can. And if I recall President Obama's speech about 12:26 PPD-28, I think he said something to similar effect, that there has to be *some* legitimate reason for the collection. Now, I assume that reason could be very broad, but that it can't just be 'We have the ability to do it, therefore we *will* do it'. 12:26

246 Q. No, in fairness, we can go back to look at PPD-28. There are limitations on PPD-28 as well.

A. (Pause to Read).

247 Q. So if you look at section 1.

A. Mm hmm. 12:27

248 Q. The part that you may have had in mind was (d): "*Signals intelligence shall be as tailored as feasible*"?

A. Yeah.

249 Q. But nobody could claim that's a very strict standard or 12:27 a very well defined standard, could they?

A. I agree. And I didn't hear myself to say it was strict.

250 Q. No, no, you didn't. All right. So that appears to be

the extent of the protection for which PPD-28 -- that PPD-28 provides must be provided for non-US persons, is that correct?

A. Mm hmm.

251 Q. All right. And then that's all I want to ask you about that, Professor. You also deal in your report with the Privacy Act and the Judicial Redress Act. 12:28

A. Indeed.

252 Q. And you've discussed this with Mr. Murray. But I think the net upshot of what you say in your report at paragraph 68... 12:28

A. Mm hmm.

253 Q. ... is that the Privacy Act doesn't apply to the NSA?

A. Just to be technically correct, that the NSA has availed itself of its statutory authority to exempt itself. 12:28

254 Q. Yes, exactly. All right. And these programmes that we're talking about are, of course, conducted by the NSA, aren't they?

A. For the most part. 12:28

255 Q. Yes, all right. And that really means that the Privacy Act is not of any particular relevance to the discussion that we're having, isn't that correct?

A. I mean, as I hope my report makes clear, I have not seen and do not see the Privacy Act as a key feature of the remedial regime in this respect. 12:29

256 Q. And the same thing applies to the Judicial Redress Act?

A. Indeed.

257 Q. The Judicial Redress Act can only provide whatever the

Privacy Act can provide?

A. That's right. Although if I may just take one moment to tie things together, Judge? That's part of why I disagree rather firmly with Mr. Serwin's suggestion that the Judicial Redress Act has some bearing on the APA, right - just to help keep things in perspective - because of its narrowness in this context.

258 Q. All right. And indeed the Judicial Redress Act specifically provides for designated agencies. And the NSA is *not*, in fact, a designated agency -- 12:29

A. Not *yet*.

259 Q. Not yet, all right. Under the Judicial Redress Act. And then in the remaining part of your report from 68 onwards you really deal with a series of administrative procedures, I think, isn't that correct -- 12:29

A. Yeah.

260 Q. -- which are constraints? But you've made it clear that --

A. And if I may?

261 Q. Of course. 12:29

A. *And*, just to be complete, *and* the internal review within the FISA court, which I wouldn't call administrative.

262 Q. All right. It's the internal review, which I don't want to ask you anything about, the judge knows all about that I think. And the rest of what you talk about are administrative procedures. And you've made it clear that as far as you're concerned, they simply aren't adequate? 12:30

A. I wouldn't make it at that level of generalisation. I think certainly the oversight procedures, Judge, are not sufficiently robust to my mind. You know, the internal procedures, I guess the question is -- I don't think I said I believe that the interpretations are, by themselves, inadequate; I think I would like to see more robust oversight and accountability. Because internal procedures may be as adequate as they can be, Judge - I still, at the end of the day, want at least someone on the outside. 12:30

263 Q. All right. Your more fundamental point is that they're not adequate by definition, judicial redress is what one looks for in order to assess adequacy?

A. Certainly they're not adequate on their own, right, that it's part of a larger puzzle that has a larger future, as a larger series of measures. 12:30

MR. McCULLOUGH: Thank you.

A. Thank you.

PROF. VLADECK WAS RE-EXAMINED BY MS. HYLAND AS FOLLOWS: 12:31

264 Q. **MS. HYLAND:** Prof. Vladeck, can I just ask you to deal with a few things that were raised this morning and yesterday? Can I ask you first just to look at a case or two that were handed up to you? 12:31

A. Please.

265 Q. In particular can I ask you to look at the case of Google that was just handed up this morning, about, I think, 11:45 by Mr. Murray?

A. Yeah, I have it.

266 Q. And you'll recall that Mr. Murray identified page 20 for you and he identified, I think, the statement that electronically transferring data from a server in a foreign country to Google's data centre in California does not amount to a seizure, because there is no meaningful interference. And I wonder, could I just ask you to look at some other aspects of that case and please comment on the case as a whole in respect of its implications for privacy? And in particular can I ask you to start please at page 18 -- first of all, can I ask you have you read this case before? So you're just looking at it for the first time, so I'm conscious you're at some disadvantage in that respect. But if I could just perhaps ask you to look at a number of points? 12:31 12:31 12:32

A. Sure.

267 Q. So page 18. Do you see there that there's a reference to the **Microsoft** case? And we spoke about that before.

A. Quite. 12:32

268 Q. And you'll see there that the court is holding that:

"*The disclosure by Google of the electronic data relevant to the warrants at issue here constitutes neither a 'seizure' nor a 'search'.*"

And you'll see the court says it:

"... *agrees with the Second Circuit's reliance upon*

Fourth Amendment principles, but respectfully disagrees with the Second Circuit's analysis regarding the location of the seizure and the invasion of privacy. The crux of the issue before the court is as follows: Assuming the focus of the Act is on privacy concerns, Where do the invasions of privacy take place?"

Then you'll see page 20 -- well, sorry, I should continue with that sentence:

"*To make that determination, the court must analyse where the seizures, if any, occur and where the searches of user data take place. This requires the court to examine relevant Fourth Amendment precedent. The court recognises that the cases discussed below address seizures and searches of physical property. However, these cases are instructive, and binding.*"

Then we go on to page 20 that you've already been asked to look at by Mr. Murray. And then if I could just ask you to go on please to page 22? 12:33

A. Mm hmm.

269 Q. And just where you take up the passage:

"*The court's Fourth Amendment analysis does not end there, however, for the court also must examine the location of the searches in the instant cases. As noted supra, pursuant to Fourth Amendment precedent, a 'search occurs when the government violates a*

Subjective expectation of privacy that society recognizes as reasonable'... When Google produces the electronic data in accordance with the search warrants and the Government views it, the actual invasion of the account holders' privacy - the searches - will occur in the United States".

A. Mm hmm.

270 Q. Then turning over the page: "*Under the facts before this court, the conduct relevant to the SCA's focus*" - and I think that is the Stored Communications Act, isn't it? 12:33

A. It is, yeah.

271 Q. "*Will occur in the United States. That is, the invasions of privacy will occur in the United States; the searches of the electronic data disclosed by Google*" --

A. Ah.

272 Q. -- "*pursuant to the warrants will occur in the United States when the FBI reviews the copies of the requested data in Pennsylvania. These cases, therefore, involve a permissible domestic application of the SCA, even if other conduct... occurs abroad.*"

And I wonder could you just comment on those parts of the case, I suppose, having regard in particular to concreteness and also privacy as a right protected? 12:34

A. Sure. So I am coming to this fresh, Judge, so forgive me if I'm not as rehearsed as I would've like to have been. My reaction to this is that what the court is

effectively saying -- the problem in this case is the same as in the **Microsoft** case; you have data that is initially stored on a server overseas - usually here in Ireland - and the data, the variable is why it's moved, but it's moved to a server in the United States, at which point the government accesses it, right? 12:34

I take the District Court to be saying here that it's not the movement of the data that creates a privacy interest, because that's just Google, right, internally transferring data from one server to another - it may be without my, the Google user's knowledge - that the privacy interest accrues at the moment the government seeks it, right? And so this was critical here, because the Stored Communications Act has a domestic hook, right, it requires that the order be executed in the United States. The problem in the **Microsoft Ireland** case was that Microsoft had not yet moved the data. And what the government was seeking was to compel Microsoft to move the data from Ireland to the United States so it could be searched. 12:34 12:35 12:35

My understanding from my very quick perusal of this case, Judge, is that Google *had* moved the data and that it was once it was *in* the United States that the government was seeking to search it. That's why the Stored Communications Act analysis came out differently, right? Because the court *has* the power to go to Google and say 'This data is here in the United 12:35

States, produce it to the government'. And the Second Circuit in the **Microsoft** case said 'The data is still in Ireland. The court does not have the power to compel Microsoft to move the data from Ireland into the United States'. I hope that distinction makes sense. 12:36

So my reaction to this is it's actually, I think, deeply consistent with my colloquy with Mr. Murray about how there's a question about a private company's pure movement and retention of data and whether that 12:36 would be a concrete injury which Google moving data from Ireland into the United States the court says may not be here, but that once the government comes into play, there's no concreteness concern, right? Once the government is requesting the data, regardless of where 12:36 it is, that's the point at which, from a concreteness perspective, the privacy harm has occurred.

273 Q. Just picking up on that point, do you think in principle there's a difference between a user consenting to have its data transferred to, let's say, 12:36 its phone company and a user having data given to the phone company, *then* taken by the US Government, in principle?

A. I do. So I think we talked yesterday briefly, Judge, about the third party doctrine and this is an open 12:36 problem in US jurisprudence; the Supreme Court has held, albeit in cases older than I am, that once I give data to a third party - to my phone company - I no longer have any expectation of privacy in what the

phone company does with that data. But some of the more modern cases have resisted that - we talk about the **Jones** case and the GPS tracker, the cell site location information cases. I actually believe, and I have written previously, that there is a different expectation of privacy once the government comes into play, because the government is in a unique position not just to take data from one firm, but from many firms, right, that the government has the ability to, as I think I said yesterday, aggregate across the data streams in ways that Microsoft may not, in ways that my phone company may not. 12:37 12:37

274 Q. Thank you. Now, can I ask you to take - do you remember you got a yellow book yesterday --

A. Mm hmm. 12:37

275 Q. -- from Mr. Murray with some cases?

A. Yeah.

276 Q. And I think they were being handed to you to seek to demonstrate in some way that **Spokeo** had changed the law or was a seismic change or something of that nature. Can I just ask you to look at tab five please? 12:38

A. Mm hmm.

277 Q. That's a case of **Kamal**. And can I just ask you please to look at page two of that? And you'll see there under the heading "Discussion" there's a reference there to Article III and there's a reference to the **Lujan** test. 12:38

A. Yeah.

278 Q. Do you see that?

A. I do.

279 Q. Then do you see under the heading "Governing Caselaw" there's a reference to the fact that the action was stayed in December 2015 pending the Supreme Court's decision in **Spokeo -v- Robins**. The decision confirmed that an injury-in-fact must be concrete, even where Congress has authorised a private cause of action. And then do you see the next line, **Spokeo** did not disturb the circuit's standing jurisprudence and there's a reference to **In Re Nickelodeon**? 12:38

A. Yeah. 12:38

280 Q. Would you agree with that?

A. I would. And we also, Judge, talked about the **Horizon** case, which was also a Third Circuit case.

281 Q. Yes.

A. You know, I think what's interesting to me, Judge, about all of this is I think this is a lot of fighting over a really not important point. Whatever affect **Spokeo** had, everyone agrees that there is a concreteness inquiry and that the concreteness inquiry is going to depend to some degree on the nature of the 12:39 privacy harm and on the status of the violator - that is to say, is the violator a private defendant or is the violator the government, is the nature of the privacy harm something that looks analogous to something at common law, or is it something that 12:39 Congress invented by statute? I believe that was clear in the case law before **Spokeo**. Either way, we end up in the same place, which is with the same understanding of concreteness.

282 Q. Yes. And can I ask you just to turn over the page then and you'll see there the first full paragraph:

"As the defendants argue, the alleged injury here entails increased risk of suffering fraud or identity theft sometime in the future, not a manifest violation of a traditional privacy interest." 12:39

And there is a reference there to **Reilly** and **Nickelodeon**. 12:40

A. Mm hmm.

283 Q. Then it goes on to say: "*The purpose of credit card truncation*" - and that means, I think, only giving, let's say, five numbers on your credit card, as opposed to all the numbers on your credit card. 12:40

A. Yeah.

284 Q. "*Is to limit incremental risk of fraud or identity theft, not safeguard one's freedom from injurious disclosure as to private matters or intrusion upon the domestic circle or some other traditional privacy interest.*" 12:40

And there you see cited the very famous Warren and Brandeis article which I think in fact Prof. Richards, in his book, his non-legal book, places great emphasis on as the birth of privacy, isn't that right? 12:40

A. Certainly the birth of modern privacy law in the United States.

285 Q. Yes. Then the court goes on to say:

"*The essential question is whether, in light of Congress' decision to authorise private suits under FACTA, printing ten, rather than five credit card digits on a sales receipt elevates the risk of fraud enough to work a concrete injury. If the harm is not concrete, the court lacks subject matter jurisdiction and must dismiss the case*".

A. And so, Judge, just to walk through it, right? So note the two steps of the analysis, right? First is to say this is not a traditional common law privacy harm, right, printing of ten digits versus five digits. And second, the second **Spokeo** or **Lujan** question, however you want to frame it - did Congress nevertheless have the ability to make this a concrete injury simply because of the *risk* of identity theft? And it's because the court discredits, right, that risk in the context of ten digits versus five digits that they find no concreteness here because of the specific way that statute operated. Again I think this would be a very different case if it were the government holding onto more data than it was supposed to. 12:40 12:40 12:41 12:41

286 Q. Yes, thank you. Can I just go back then to some of the matters discussed this morning?

A. Please. 12:41

287 Q. There was, I think, a discussion of the APA. And can I ask you whether, in your view, the APA could potentially apply where there's a breach of Section 702?

A. I don't think there's any question. And so Mr. Murray is right to identify that one of the questions a court would have to ask in that context include whether the Plaintiff is in a zone of interest, include whether the challenged action is final agency action and include whether there is preclusion. I actually think, Judge, there's no question how the preclusion analysis comes out; there *is* no alternative remedy that I think could be argued to override the APA in the context of 702, with the possible exception, Judge, of a recipient of a directive, right? If I'm Yahoo, I actually have an express remedy in the statute. And so that's the one context where I could see a court saying 'You have this express remedy', right, 'React to the directive, go to the FISA court. Therefore, we're not going to give you the APA'. For everybody else, I don't think preclusion would be the issue, it would just be those zone of interest and final agency action questions. 12:42 12:42 12:42

288 Q. And just talking about agency action and final agency action, in your view, would a directive or a certificate under Section 702 likely come within the definition of agency action? 12:42

A. So I think we discussed this yesterday, Judge. I think there's no question a directive would. And I would point to the Second Circuit's discussion in **ACLU -v- Clapper** of a production order as a comparable example of what final agency action is. On the certificate or the certification, you know, Judge, I think the question is just the timing, right? That is to say, has 12:42

the agency actually acted pursuant to the certification? And so to my mind, the easier case would be to challenge the Directive. And the certification would be harder simply because there might not have been a concrete step the agency took pursuant to the certification. The certification is very much the jumping off point.

289 Q. Thank you. Now, I think in this -- I'm going to quote something you said this morning and I think it was in contradistinction to the legal regime where the terrorist surveillance programme was at issue - I think that was in **ACLU -v- NSA**. And you went on to say that in respect of the APA application, it would be potentially different in a "crowded legal regime" for Section 702 and phone records. What did you mean by a "crowded legal regime"? 12:43 12:43 12:43

A. So I think, Judge, the sensitivity courts have in the APA context is that they don't want to look like the APA is allowing them to review exercises of executive branch discretion where the field is not occupied with a clear set of rules and procedures, where it looks like the President and/or his subordinates are exercising authority where there's a lot of, if you'll forgive the idiom, wiggle room, where there's a lot of flexibility. The APA is not a great remedy in those contexts, because it's not clear what the specific crux of the claim is going to be. 12:44 12:44

The reason why I both feel more confident about 702 and

215 and why the courts *have* been more confident is because Congress has provided far more guidance on what the relevant authorities are, on how they are to be used, on what the procedural and substantive requirements are, and indeed on other avenues of judicial review. And all of those things, I think, would weigh in favour of a court looking at surveillance under these far more statutorily fleshed out programmes as the kind of reviewable agency action that is the heart of the APA. 12:44

If you'll forgive a sort of crude analogy - immigration; the President's decision whether to deport or not deport a particular group of individuals is not something the APA is going to be interested in. Whether the immigration authorities have provided the statutorily protected review and the statutorily protected assessments of the individual immigrants *is* something the APA is going to be interested in. And I think in this context, because of how much Congress has done to demarcate the relevant lines of authority, as the **ACLU -v- Clapper** case shows, there's much more room for the APA to have a rule. 12:45 12:45

290 Q. So the detailed statutory framework makes a difference?

A. It does. Now, that can go too far, Judge - that's where the preclusion issues comes up; if Congress has done so much, have they actually manifested an intent to crowd out the APA? But we have a very strong judicial presumption in favour of judicial review, and 12:45

so we require, usually, some clear indicia that Congress met for the APA to not be available, once we have a regime where Congress has acted at all. In the **ACLU -v- NSA** case where you have the TSP, where there was no statute, it was hard to figure out what Congress wanted in that situation. 12:46

291 Q. And I think the presumption of judicial review is identified in **Clapper -v- ACLU**?

A. Indeed.

292 Q. Can I move on to the declaration point? I think Mr. Murray and yourself had a debate about when a declaration would or not be granted. Can I ask you, *can* it be granted even when the violation has ended? Is it possible as a matter of law? 12:46

A. It *is* possible. I think I said this yesterday and if I was inartful, I apologise; declaratory relief is usually about ongoing illegality, it *can* cover completed illegality if the plaintiff can show some reason to believe that the conduct is likely to recur. So that's to say it will not frustrate the court's ability to issue the declaration just because for the moment the complained of conduct has ceased if there's some reason to believe that it might resume in the near future, right? So it's not a categorical backward looking/forward looking, it's more a subjective assessment of what is likely to happen now. 12:46 12:47

293 Q. Thank you. Just then coming to sovereign immunity. I think you distinguish between, for example, what you described as a rogue officer and where the violation

might be in respect of a larger programme. Can I just ask you to look, physically look at the case, although I know we've all seen it many times, of **ACLU -v- Clapper**, just with a view to identifying who the defendants were in that case? 12:47

A. Would you mind directing me to that?

294 Q. Sorry, it's tab 15 of your book of US law, or US materials.

A. Book one?

295 Q. Yes. 12:47

A. Thank you.

296 Q. And you'll see there that the defendants were James Clapper, in his official capacity as Director of National Intelligence; Michael Rogers, in his official capacity as Director of NSA and Chief of the Central Security Service; Ashton Carter, in his official capacity as Secretary of Defence; Loretta E. Lynch, in her official capacity as Attorney General; and James Comey, in his official capacity as Director of the FBI. 12:47

12:48

And I think at page 799 we see there that one of the allegations, apart from the constitutional one, was in respect, if you look at the second column under the heading "Procedural History" and you look about two-thirds of the way down, you see there's a reference there: "*The Complaint asks the court to declare that the telephone meta-data programme exceeds the authority granted by Section 215*", and the constitutional claim as well. I wonder could you comment on those 12:48

defendants in the context of the sovereign immunity discussion you had earlier please?

A. Sure. So I hope this came through, Judge, but just to try to tie it all together, sovereign immunity is *never* an issue, categorically *never* an issue if the claim is not seeking damages, right? And that's because of the APA - the APA has expressly waived the sovereign immunity of the United States Government in any claim for relief other than damages. What that means in practice is that in a case like this one where the plaintiffs are seeking declaratory and/or injunctive relief and not damages, Judge, they're free to name any and all relevant government officials in their official capacity without running into sovereign immunity. And if the question is why is there no sovereign immunity, the answer is Congress waived it in the APA. 12:48 12:48 12:49

297 Q. Yes. And in the 1810 context, is there a case deciding the question that you identified this morning, i.e. in relation to a programmatic, if you like, breach where -- 12:49

A. I'm not aware of such a case.

298 Q. I was going to ask whether or not it's official, a person in their official capacity can be sued or in their personal capacity?

A. I mean, the problem is we just haven't had a lot of 1810 cases. 12:49

299 Q. Yes.

A. Right? I mean, **Jewel**, I think, alleges an 1810 violation, if my memory serves, **Al-Haramain** does, we

just, we haven't gotten a full judgment. But on the sovereign immunity point, Judge, I mean, the key is if it's not damages, there's no sovereign immunity problem. If it *is* damages, we look to see is the defendant either the United States itself or a federal officer in his or her official capacity? And if so, then we look to see whether Congress has waived that sovereign immunity. **Al-Haramain** says that in 1810 Congress has *not*. In 2712, in contrast, Congress *has*. So that's the steps of the analysis. 12:49 12:50

300 Q. Thank you. Just coming to the PPD point, I think it was put to you that PPD-28 did not cover bulk collection. And could I just ask you to look please at the Litt letter? And you'll find that at, I think it will be book 13, the first book 13, tab 13 as well. 12:50

A. Book 13, tab 13?

301 Q. I think so. I hope so.

MS. JUSTICE COSTELLO: Sorry, did you say book one, tab 13?

MS. HYLAND: Oh, sorry, yes, Judge. 12:50

A. Okay, thank you.

302 Q. **MS. HYLAND:** Book one of 13, yes, Judge. I think those books are headed "Agreed EU-Irish Authorities". (To Witness) Prof. Vladeck, do you see that there? And so I'm going to ask you to look then internally at page 91. It's annex six. 12:51

A. One moment please.

303 Q. Yeah. It's quite near the end.

MS. JUSTICE COSTELLO: Do you mean book one of the EU

--

MS. HYLAND: I'm sorry, I should've said that. I'm sorry, Judge, you got book one generally, I mean of the EU-Irish authorities.

A. Ah, yes. Okay, I have it. Sorry. 12:51

304 Q. **MS. HYLAND:** Do you see there Prof. Vladeck there is, under the heading "PPD-28", then the second paragraph, you'll see there's a reference to the application of PPD-28. And it states that it sets out a series of principles and requirements that apply to all US 12:51 signals intelligence activities and for all people regardless of nationality or location. I wonder could you comment on the applicability, if any, of that to the bulk collection issue?

A. So I had understood Mr. Litt's letter, and it's part of 12:51 why my report referred - I mean, I had actually relied on Mr. Litt's letter in drafting my report - that the language of PPD-28 in exempting bulk collection does not mean that there's no consideration given to these minimisation rules, and indeed that Mr. Litt represents 12:52 in this letter that these concerns are very much applied and taken seriously in the context of minimisation, the language of PPD-28 notwithstanding.

305 Q. Yes, thank you. Now, can I just turn to yesterday, the topics that were discussed yesterday? And just in 12:52 relation to **Bivens**, just so there's no misunderstanding, can you just very briefly describe to the court what exactly the **Bivens** doctrine is and where does it apply?

A. Certainly. So the **Bivens** doctrine is a very narrow doctrine. The basic idea, Judge, is Congress has never provided a stand-alone cause of action for a victim of a federal constitutional violation by a federal officer. So if the FBI breaks into my house without a warrant, there's no statutory cause of action for me to sue the relevant FBI officers for damages. There is if they are state police, right? So this is a weird disconnect in American law. 12:52

12:53

The **Bivens** case is a 1971 Supreme Court decision that basically says that there *will* be circumstances where, even without Congress, the courts themselves should recognise what is, in effect, a common law cause of action for damages, because otherwise it would be impossible to fully vindicate the underlying constitutional interest. The **Bivens** doctrine is very specific, it is only about damages claims against federal officers for federal constitutional violations. And it has been controversial in the United States as many of our Supreme Court justices have become more skeptical of common law causes of action, of judge-made remedies. It's still there - I mean the **Hernandez** case we've talked about, one of the questions is: 'Should there be a **Bivens** remedy in this context?' 12:53 12:53

It is subject to two critical exceptions, and that's where almost all of the work is today. The first exception, which Mr. Murray alluded to - actually

referred to directly, I don't mean to misstate - is special factors; are there special reasons why courts should stay their hand before recognising a cause of action in this context? And in the Supreme Court we've seen that most often when the plaintiff is in our military, where the courts have said it's not really the courts' job to resolve internecine disputes within the military, that that's a special factor. The lower courts have gone further, but the Supreme Court has not. Then the other sort of caveat is if Congress has provided an alternative - the idea being that courts should not jump over a statutory remedy Congress has provided. 12:54 12:54

In the fourth -- 12:54

306 Q. Prof. Vladeck, I'm so sorry to interrupt you, but I'm just wondering - and I know I asked you - but for this purpose, the EU citizen, is it relevant to the EU citizen?

A. So I'm sorry, I didn't mean to belabour the point. I don't believe it is, as my report suggests, because an EU citizens with no voluntary connection to the United States, as we've discussed, probably doesn't have Fourth Amendment rights. The only point I was trying to make in my report on this front, Judge, is that I don't see that as a critical difference between an EU citizens and a similarly situated US person because of how hard it's been even for a US person to avail themselves of **Bivens** in this context. That was the -- 12:54 12:55

I didn't mean to overexaggerate the importance.

307 Q. Yes. But in the context of what we're looking at here, the EU citizen, I think unless **Hernandez** changes the law about reliance on the Fourth Amendment, I think it has no application, is that right? 12:55

A. I agree. The only thing I would say is again, Judge, as a merits defect, not a standing defect.

308 Q. Yes. Now, can I just ask you to look at paragraph 78 - you don't have to go back to it - but paragraph 78 of your report? I think there was some criticism of you by 12:55 Mr. Murray in respect of the reference to the external oversight by the House's Senate Intelligence and Judiciary Committees yesterday. And can I just ask you, I think when I was examining you, you did indeed make specific reference to the Judiciary Committee and 12:55 you said it was important. Can you just very briefly explain why you think that is important?

A. Certainly. So, Judge, we mentioned this a bit yesterday, but the Judiciary Committees, by tradition - and they've been around much longer than the 12:56 Intelligence Committees - I think it's safe to say are much more aggressive in the exercise of their oversight function, that they tend to be much more rigorous in policing perceived abuses by the government and that they are much more zealous in protecting what they view 12:56 as their obligation to the Constitution, in ways that I think have not been true of the Intelligence Committees.

And so one of the, to me, points that may have gotten lost in my colloquy with Mr. Murray is that my critiques of the Intelligence Committees are *not* also of the Judiciary committees. I actually think that most of the useful things Congress has done in this field have been spearheaded by the Judiciary Committees - indeed one of the proposals has been to increase beyond where it even is now the role of the Judiciary Committees in oversight of the Intelligence Community. 12:56

309 Q. Yes, thank you. So this article that was identified to you yesterday **(INDICATING)**, that, I think, is it fair to say it's *not* about the Judiciary Committee? 12:57

A. At all.

310 Q. I see. Can I just then go on please to the state secrets doctrine? 12:57

A. Mm hmm.

311 Q. And I think you have identified that if an individual is making a claim under Section 702, there would be a good argument the government would *not* be able to invoke the state secrets privilege - I think you say it in the last paragraphs of your report. Just for the sake of clarity, can you just identify why you say that there would be that argument? 12:57

A. So the argument - and we've actually seen this to some degree already in the **Jewel** case, Judge - is that it would have been -- let me just back up one step, I'm sorry. The state secrets privilege is generally viewed as a common law evidentiary privilege, much like spousal privilege or priest/penitent or what have you, 12:57

the idea being that as a common law privilege, it is subject to statutory modification and indeed perhaps abrogation. Just to be clear, Judge, there are some who argue it's actually constitutionally grounded and so would *not* be subject to such statutory override. That's the minority view. It's quite, I think, the prevailing view that it's a common law privilege.

Then the argument is that when Congress creates express remedies for violations of a statute like FISA, where the entire subject matter is going to be inextricably bound up with national security secrets, one cannot reconcile leaving the state secrets privilege intact with Congress' intent that these remedies go forward, right? And so the argument that has been made - and at least so far accepted by the District Court in **Jewel** - is that Congress' decision to provide at least some remedies for violations of FISA should be taken as overriding the state secrets privilege as applied to those contexts. 12:58

312 Q. Yes, thank you. Now, just one short sentence; Mr. Murray said yesterday he was hypothesising a situation and he said "If I get discovery and I do not discover that I'm under surveillance, I will not survive a motion for summary judgment." Can I ask you just to comment on, I suppose, whether that's a reasonable position for a court to take or what's your view of that? 12:59

A. Yes, I mean, I think at that point, Judge, there's no

merit, right? That is to say, if we've gone through discovery and if I actually cannot adduce any evidence substantiating my claim that my rights have been violated, I would very much hope that the court would dismiss the case at that point, because there's no leg to stand on. And so the key that I was trying to communicate, Judge, is that's not a standing problem, that is a merits problem, that is that the plaintiff has utterly failed to make his or her case. 12:59

313 Q. Yes. 12:59

A. Which I imagine in all circumstances we should want a court to say 'Thank you and have a nice day'.

MS. HYLAND: Yes. Judge, I'm conscious it's just coming up to one o'clock. I'm not going to be more than ten minutes, but I don't know whether the court -- 12:59

MS. JUSTICE COSTELLO: No, no, fine.

MS. HYLAND: Very good.

A. Thank you, Judge. I appreciate it.

MS. JUSTICE COSTELLO: There's a flight to be caught.

314 Q. **MS. HYLAND:** Thank you, Judge, I appreciate that. 12:59

(To Witness) So there was a reference, I think, to footnote 26 of your report yesterday, the **Neiman Marcus** case - and this was a case in respect of fraudulent transactions on credit cards following a hacking - and Mr. Murray said that you omitted one detail, which is 13:00 that the plaintiffs had transactions placed on their credit cards - in other words, because of the fraudulent activity - and he said that's not an insignificant detail perhaps. And he went on to say it

would've been surprising if your credit card bill increased as a result of a data breach and you *didn't* have standing to complain. But in fact, when one looks at the case, it's quite clear that the plaintiffs had been reimbursed before they brought the proceedings -- 13:00

A. Ah.

315 Q. At page 692 they say: "*The plaintiffs concede they were later reimbursed and they allege standing based on two* imminent *injuries.*" Because if you remember, your footnote was about **Clapper** and immanence. And the two 13:00 imminent injuries were the increased risk of breach of fraudulent charges and the greater susceptibility to identity theft. And ultimately the court upheld their standing claim in respect of imminent injuries because the District Court had interpreted **Clapper** to say that 13:01 no future injuries could be relied upon. And in that context, I wonder could you comment on the passage that you chose to put in the footnote for which you were criticised?

A. So I mean, the passage, I think, Judge, is just there 13:01 to say, right, that there's still the possibility that future harm of itself will suffice to satisfy the actual or imminent harm requirement of the injury-in-fact requirement. I didn't mean to take a broader position on the case and I think that came 13:01 through in my colloquy with Mr. Murray. But just insofar as that, to me, clarifies again what was my animating purpose all along, which was just to give context to the DPC draft report, right, that the DPC

draft decision, I think, takes too glum a view of future harm as a possible basis for establishing an injury-in-fact.

I take the Seventh Circuit decision, as I take many other post-**Clapper** decisions, as actually being quite clear: No, future harm is still very much a possible trigger, it just requires the kind of allegations that we've seen in these cases. 13:01

316 Q. Yes. And then I think Mr. Murray posited again a hypothetical question to you about remedies and he said "Where the breach has occurred and it has stopped in a retention context, what would the remedy be?" And I suppose I'll ask you to consider whether -- what *is* the wrongdoing, if any? In other words, there's an allegation of unlawful retention, the breach has stopped, by which I take it to mean there is no longer unlawful retention; *is* there a wrongdoing there, in your view, and if so, is there a necessity for a remedy? 13:02 13:02

A. So if the retention has ceased, right, if there literally is no data in the government's continuing possession at that point, it's not clear to me what a prospective remedy *could* accomplish in that context. What I tried to suggest, again perhaps inelegantly, yesterday was that we've seen claims in this context for prospective relief for discharge of *any* records the government might still have of the wrongfully obtained data in the first place. 13:02

317 Q. **MS. JUSTICE COSTELLO:** In "discharged", you mean erasure, or...

A. Erasure, any other -- erasure or destruction, however it works. I'll leave it to the technical experts to sort that out. So just to be clear, I had taken Mr. Murray's question to be if we are past that, if there is literally nothing more in the government's possession, can there be a forward looking remedy? At that point, no, because I don't think there's anything in the future at that point *to* remedy. 13:03

318 Q. **MS. HYLAND:** Yes. Can I just ask you, finally, to look at your two articles please, the 2014 article and the 2016 article?

A. Mm hmm.

319 Q. I think the 2012 article -- well, I should just ask you to confirm, I think the 2012 article, insofar as it was identified as relevant by Mr. Murray, it was in respect of the **Bivens** doctrine, isn't that right? 13:03

A. Mm hmm. I will say this is the most, I think, anyone has ever read my scholarship. 13:03

320 Q. So the 2014 article, can I just ask you to comment on a number of points in there? And I think just a small point, but in respect of the quote about the death knell for standing, can I just ask you to turn to page 566 please? 13:04

A. Yeah.

321 Q. Because in fact I think what you said was, you said -- so I'm looking at page 566, under the heading "After Clapper (and Snowden)". You say:

"*The Supreme Court's decision in Clapper may well have sounded the death knell for suits challenging secret surveillance (if not all secret governmental programmes), but for the disclosures by former NSA employee Edward Snowden.*"

I think you may not have mentioned that that was the *actual* quote.

A. I'm sorry, I didn't mean to leave that part out. 13:04

322 Q. Yes. And then can I just --

A. Although I think -- I mean, Judge, I hope the gist came through anyway, that it was the disclosures and the subsequent declassifications that I think changed the landscape. 13:04

323 Q. Yes. Then can I then ask you to turn over the page to page 567 and can I just ask you to go down to the bottom of the page and starting with the words:

"*At the same time, one of the more underappreciated features of FISA is the cause of action it already provides for an 'aggrieved person' 'other than a foreign power or an agent of a foreign power [as Defined by FISA], who has been subjected to an electronic surveillance.' FISA proceeds to define 'electronic surveillance' somewhat convolutedly, but it nevertheless manifests Congress's intent, from the inception of FISA, to allow those whose communications are unlawfully obtained under FISA to bring private*

suits to challenge such surveillance. Simply put, Congress has already created a private cause of action for FISA suits; it has just never clarified how putative plaintiffs can demonstrate that they are, in fact, 'aggrieved persons'."

And how I read that, Prof. Vladeck, is that what you're identifying there is that --

MR. MURRAY: Well, this sound like a leading question on the way, Judge. 13:05

MS. HYLAND: Well, very good, I will try --

MR. MURRAY: I mean, Prof. Vladeck can say what he meant.

324 Q. **MS. HYLAND:** Yes. Well, very good. Perhaps, Prof. Vladeck, you would then say in summary what are 13:05 you distinguishing between there as, if you like, the problem?

A. Sure. I mean, I guess all I was trying to suggest in that context was that Congress had already taken a step toward opening the door to the kinds of suits that 13:05 **Clapper**, that the Supreme Court **Clapper** seemed to be disfavouring. And so what I was trying to suggest was that this is a very relevant part of understanding the remedial scheme, because it makes it, if you'll forgive me, a less of a heavy lift for Congress to then perhaps 13:06 make it even easier for plaintiffs to establish standing in this context going forward, given that they've already created an express cause of action.

325 Q. Yes. Then can I ask you to turn to page 570? And

there's a footnote there, just going back to the point about the state secrets privilege. You'll see there footnote 88, you refer to a case in respect of, I suppose, the thesis that you've been advancing as to whether state secrets privilege applies in a cause of action provided by FISA. Can you just comment on that case please?

A. Sure. I mean, I cite there, Judge, I think a case that's related to the **Jewel** litigation in that footnote where we've had multiple district courts all in San Francisco in the Northern District of California accept the argument that I was just referring to that in the context of claims under FISA itself there's an argument that the state secrets privilege has indeed been abrogated and that the government is not entitled to invoke it as a basis for getting rid of these claims.

326 Q. Yes. And can I just ask you then about, if you like, the notification issue and can I ask you to turn to page 578? I'm interested in just for you to respond to the importance or not of the notification issue in the context of national surveillance. If you see the last paragraph on 578: "*But if nothing else is clear*"; do you see that?

A. Yeah.

327 Q. And you go on to say:

"*It should hopefully be obvious that a truly comprehensive scheme for adversarial judicial review of secret surveillance programs may in fact be*

unobtainable, at least without sacrificing the very secrecy that arguably enables the success of such governmental foreign intelligence activities. That is to say, absent some meaningful shift in the Supreme Court's understanding of the... Article III case-or-controversy requirement imposes upon the adjudicatory power of the federal courts, or far greater (if not mandatory) participation in the FISA process by those entities that receive production orders and intelligence directives under the statute, it may not in fact be constitutionally possible to provide in all or even most cases for meaningful adversarial review."

Can I just ask you to comment on your passage, having regard to this issue you've identified of notification in this sphere? 13:07

A. So I mean, I think notification - and I hope this has come through - is an obstacle that manifests itself in a very particular place, right? And this, I think, ties together with Prof. Swire's discussion of the hostile actor problem. We don't want to notify the actual proper targets of foreign intelligence surveillance that they have been in fact been subjected to foreign intelligence surveillance. Indeed, Judge, remember yesterday I referred to the grand bargain, right? Part of the concern the government had was preserving its ability to not compromise its intelligence sources and methods by subjecting these activities to review. 13:08 13:08

That's why I think complete fully-throated adversarial review is not actually going to be possible in this space, because we're never actually going to want to give the target a lawyer and an opportunity to go before the judge and say 'No, you shouldn't be able to spy on me.' And so the question is: What's the second best solution? And my hope is that the remedies we've discussed - and if I ever got my wish, some of the proposals I've advanced - get us as close as we can. 13:08 13:09

Mr. Murray made a big deal out of my use of the word "adequate". And he's right - I mean, I don't think that from my perspective the remedies are as adequate as they could be. I think what I was trying to say in this article is that I don't think they could *ever* be completely adequate in the colloquial sense of the word if we actually take seriously the government's legitimate interest in conducting foreign intelligence surveillance. 13:09 13:09

MR. MURRAY: And the final part of that passage might be opened as well, Judge, on page 579, just so the whole piece is before the court.

MS. HYLAND: Yes. I had actually moved on to another article, but I am very happy for the court to read that. 13:09

A. I'll read it. I mean, I can just read it out.

328 Q. **MS. HYLAND:** Yes, very good. So can I just then ask you please to move on to your 2016 article?

A. Yeah.

329 Q. And just to identify, I think at one point in this article you state that disputes over counterterrorism policy ought to be left to resolution by the political branches. I think that's 1038. And can I just ask you what you many by "counterterrorism policy" in this context and also how it sits with what you told the court yesterday about your view of the importance of the judiciary in this sphere? 13:10

A. I'm sorry, can you just point me to the specific passage? 13:10

330 Q. Sorry, it's at page 1038.

A. Yeah. Which paragraph?

331 Q. It's the second paragraph and it's about the fourth line down. So you see the words "*More fundamentally*"? Do you see that? 13:10

A. Yes. So I mean, what I was just saying there was it's my view, Judge, of one of the sort of downsides of the absence of merits-based adjudication, especially outside of the surveillance sphere - so I talk about detainee treatment, extraordinary rendition, target killing as the three, I think, most prominent examples - is that it leaves the perception that the courts have nothing to say on these matters. That *hasn't* been true in the surveillance context, right? I mean, we know enough to know that we have meaningful, fully, you know, adversarial legal decisions about the legality of most of the most important US surveillance programmes that have been carried out since September 11th. 13:10 13:11

That's always why I thought there was a meaningful distinction to be drawn between the surveillance context and these other contexts.

332 Q. Yes. And I think on page 1037 in fact there's two other government actions, interrogation and watchlisting, as well which you list, isn't that right? 13:11

A. Indeed. I'm sorry, I treat interrogation as being under the umbrella of treatment.

333 Q. Thank you, yes. Then I wonder can I just ask you to look at footnote 28? 13:11

A. In the same article?

334 Q. In the same article, exactly, yeah.

A. Page 1044?

335 Q. Exactly. Page 1044, exactly. And the sentence there, that it's referable to -- you talk about, you're talking about a different case, the National Defence Authorisation Act and then you go on to say there was a far more compelling argument the plaintiffs in that case had been directly affected, and you refer to **Klayman -v- Obama**. 13:11 13:12

A. Mm hmm.

336 Q. And in fact, I think after that article was written, there was a third **Obama**, isn't that right? And I wonder could you briefly just address that?

A. We've talked a little bit, Judge, about this case. It started in the District Court, where the District Court had -- this was the same case where the District Court said the APA claim was precluded, but then went to reach the merits of the Fourth Amendment challenge to 13:12

the phone records programme, held that it was unconstitutional. On appeal to the DC Circuit, the Court of Appeals held that the plaintiffs couldn't demonstrate standing, at least at that very preliminary threshold, because of the nature of the claim at that point. And my report talks a bit about why I think that's not a convincing holding and why no one's followed it; it was a fractured opinion, there was no majority opinion. 13:12

But what's interesting is, even with the Court of Appeals expressing scepticism about standing, when that case went back to the District Court, the District Court once again said 'No, there is standing'. And so the sort of the final word, because the programme soon ended and so the cases were dismissed, but the final word of the courts was that that case could've gone forward because those plaintiffs *had* satisfied all of the elements of standing doctrine. 13:13

337 Q. Yes. And I think in fact an injunction *was* granted in that case and it required the government -- sorry, there was an injunction restraining the government from collecting data *and* there was a requirement for the government to aggregate -- I beg your pardon, to segregate any meta-data. That's at the very last page of **Klayman -v- Obama**. Are you familiar with those -- 13:13 13:13

A. I am.

338 Q. Can I just finish please, Prof. Vladeck, just by making reference to what was put to you yesterday? There was a

reference to a tweet that you - I'm not sure what the verb is - "did" - that probably isn't right.

A. "Sent" maybe.

339 Q. "Sent", yes. In December. And I think in the text of that tweet you also said that the PCLOB provided an important oversight, isn't that right? Do you remember that? 13:14

A. I do.

MS. HYLAND: Yes, very good. Thank you Prof. Vladeck.

A. Thank you. Thank you, Judge.

PROF. VLADECK WAS FURTHER CROSS-EXAMINED BY MR. MURRAY AS FOLLOWS:

340 Q. **MR. MURRAY:** Sorry, Judge, just one question arising from that. I'm trying to get a copy of it, but am I not correct in saying, Professor, that in the third **Klayman -v- Obama** case it was held that only *one* of the categories of plaintiffs had standing? 13:14

A. That's correct. 13:14

341 Q. That one of the categories of plaintiffs fell precisely within the **Clapper** formulation because of the fact that they could do no more than say that they were Verizon customers, but they could not establish that there was surveillance occurring over Verizon customers at the time they *were* customers, whereas if the second category, the Little plaintiffs I think they were - not in terms of a description of their size, but instead their names - the plaintiffs who were called Little 13:14

were entitled, *did* have standing because they could establish that they were customers in a three month period within which there was in fact surveillance?

A. That's right.

342 Q. Isn't that a correct distinction? 13:15

A. Because the order we were aware of, Judge, the order that became public was a three month authorisation. And so the issue was could you show that that you were a Verizon customers during those three months?

MS. JUSTICE COSTELLO: That period, yes. 13:15

343 Q. **MR. MURRAY:** Yes. But the other plaintiffs could not surmount the **Clapper** hurdle, isn't that right?

A. At least in the very preliminary posture of that case, Judge. But what I should stress is, as I've said in my report, that case had such a strange posture that I 13:15 wouldn't put too much weight onto any one piece of it.

344 Q. I think you've criticised *every* one of the decisions in it in fact.

A. I did.

MR. MURRAY: Yeah. Thank you. 13:15

MS. HYLAND: Well, just on that point, Judge, there's a number of important, I think --

MS. JUSTICE COSTELLO: There's a plane to be caught. But okay.

PROF. VLADECK WAS FURTHER RE-EXAMINED BY MS. HYLAND AS FOLLOWS:

345 Q. **MS. HYLAND:** Just to finish off on that though, because

I think there is some importance just on that very point Mr. Murray was identifying. I wonder could you look at page 186, if you have the decision? I'm sorry, it's tab 33 in the book of US law. Because in fact I think it's important the basis upon which those plaintiffs were given standing. And I'm sorry to ask you to go and look at one last case, Prof. Vladeck.

A. Tab 33?

346 Q. Yes, it's tab 33 of your US law books. Because I think it's quite clear there the plaintiffs who were given standing had not *actually*, I think, established that their record were collected, isn't that right? Because I'll ask you just to look at the passage. Page 106, second column -- 186, second column. You'll see there just down the bottom of that column the word "*Because*": "*Because the government has acknowledged that the VBNS subscribers*" --

A. That's Verizon business. Sorry, just...

347 Q. I'm sorry, say that again, Prof. Vladeck?

A. VBNS is Verizon business. I was just --

348 Q. Very good, yes.

"... *VBNS subscribers' call records were collected during a three month window in which the Little plaintiffs were themselves VBNS subscribers, barring some unimaginable circumstances, it is overwhelmingly likely that their telephone metadata was indeed warehoused by the NSA. The Little plaintiffs, then, have pled facts wholly unlike those in Clapper. There*

is no need to speculate that their metadata was targeted for collection, that the challenged Program was used to effectuate the metadata collection, that the FISC approved these actions, or that VBNS subscriber call records were indeed collected. Simply stated, Clapper's 'speculative chain of possibilities' is, in this context, a reality."

And I think it's fair to say there that the court was willing to make an assumption given -- is that correct? 13:17

A. I think that's right.

MS. HYLAND: Yes. Thank you very much.

A. Thank you for your patience, Judge.

MS. JUSTICE COSTELLO: Thank you very much. And bon voyage. 13:17

A. Thank you.

MS. HYLAND: Judge, I appreciate the court sitting late.

MS. JUSTICE COSTELLO: I think we might take it up at quarter past two. 13:17

MR. GALLAGHER: Thank you, Judge.

(LUNCHEON ADJOURNMENT)

13:17

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

MS. JUSTICE COSTELLO: Good afternoon.

REGISTRAR: Data Protection Commissioner -v- Facebook Ireland Ltd. and another. 14:16

MR. O'DWYER: Thank you, Judge.

SUBMISSION BY MR. MURRAY:

14:17

MR. MURRAY: Judge, just before Mr. O'Dwyer addresses you I have just been explaining to Mr. Gallagher that I wanted very quickly to update you, Judge, on an issue which you will recall from last week where we furnished you with correspondence we had sent to Mason Hayes 14:17 regarding Prof. Swire's evidence.

Just to again to remind you, Judge, that Prof. Swire disclosed on Thursday that changes had been suggested to his report. They had been suggested to Gibson Dunn, 14:17 the US attorneys, who had passed them on to him and he has accepted some of them and not others. You will recall that it began off as a number, a small number, and the following day 20 to 40 and the following afternoon it was 70 changes. We wrote looking for 14:17 those changes and we got a response, in fairness, from Mason Hayes Curran in the form of a table, which we will hand up to you, with the suggestions and those which have been accepted and those which have not.

Insofar as anything turns on that, I'll return to that when we make our submissions.

We were a little troubled by this for the reasons that I adverted to in the course of my cross-examination of Prof. Swire. Because we think that, first of all, this should have been disclosed to the court, and, secondly, we're, I suppose, puzzled by the role of the US government which has presented itself as an amicus to the court but it appears now, without disclosure to anybody, was receiving Facebook's expert evidence in draft form and was making suggestions in relation to it. 14:18

So for that reason we wrote to Mason Hayes Curran asking them whether by chance any other experts had undergone a similar process. And they responded to us on Monday night, and the letter I hope has been handed up to you, and in the course of that letter they explain that in fact for all but one of their experts the reports were sent to the US government in draft form, and that in the case of all but one of the experts whose reports were sent to the US government suggestions were passed on via Gibson Dunn to the experts, although, as you will have gathered from Prof. Vladeck's evidence, the experts did not know where the comments had come from. They were presented as comments of Gibson Dunn, but they were in fact in part informed by comments from the US government. So 14:18 14:18 14:19

that's what we have been told occurred.

We believe that it is appropriate that the court have full disclosure in relation to these matters and we think it should have been disclosed at the outset. 14:19
These people are being presented to you, Judge, as independent experts. I'm not for a moment reflecting on anybody's integrity or otherwise when I say this, but it's a matter that one in my respectful submission the court is entitled to know that in fact suggestions 14:19
have been made in relation to their reports by a third party with an interest in the case.

So what we propose to do is to write to, and I have just explained this to Mr. Gallagher but only as you 14:20
will have seen us coming in a very brief few moments ago, we propose to write to Mason Hayes Curran and ask them will the person in Gibson Dunn who was involved in this process swear an affidavit confirming what the comments received from the US government were 14:20
and what were passed on. In the event that that's acceded to the court will have all of the information; if it isn't then well have to consider what application, if any, we bring. We believe it's a matter that the court should have been told in the 14:20
first instance, it wasn't and we believe the information should be put before the court.

So that's the position. You have the correspondence,

Judge, and we will mention the matter again following the...

MS. JUSTICE COSTELLO: I have two questions for you: One, what impact, if any, do you say this may have in relation to the evidence adduced by Facebook; and, two, what impact, if any, this has on the role of the United States as an amicus? 14:20

MR. MURRAY: Well, it's very difficult to answer the first of those without knowing exactly what the information was. We know it in relation to Prof. Swire. It certainly discloses that there were a large number of inaccuracies in the first version of his report which was sent to the US government, something that we did not obviously know, and wouldn't in normal course be entitled to know. Of course in fairness draft reports are privileged and I'm conscious of that and indeed comments of counsel and solicitor are privileged and we're conscious of that as well, but this is a somewhat unusual situation where a third party has become involved. 14:21 14:21

Insofar as the US government is concerned we are not, and I emphasise this, we will not be asking you to exclude anybody from the proceedings or to take any step of that kind. I will not be asking you to exclude anybody's evidence from the proceedings, nor will I be taking any step of that kind. But I will be asking you, depending on what the responses are, to have regard to them as you consider the weight of the 14:21

evidence which is put before you. And can I just remind you of this, Judge.

Mr. Gallagher elicited from Prof. Swire that these changes had been made and he did that because he believed it was something that the court should have been told. There was no other reason for eliciting it. We think he was right about that, but a large number of Facebook's witness have never been the subject of notice to cross-examine and it's only because we wrote last week that we found out that this had occurred. I don't want to overstate it. That's why I emphasise we not seeking to strike anybody out, all we want to know is exactly what occurred in relation to the basis. Thank you, Judge. 14:22

SUBMISSION BY MR. GALLAGHER:

MR. GALLAGHER: Could I respond, Judge. I have to say we're taken aback by the position of the DPC in respect of this matter. We have written a letter, Judge, and I would like you to refer to it, if you would be kind enough, setting out the position. 14:22

Firstly, we made it quite clear that these communications are privileged, and that's a matter that we can elaborate on if necessary. Mr. Murray states and accepts that communications to an expert on the basis of draft reports from counsel and solicitors and 14:22

observations are privileged and entirely proper. In the particular case there were two reports that were part of the process of declassification. Prof. Swire's was part of the process of declassification and for completeness, not because in truth there was an obligation, but because the footnote did say that it had been sent for classification, we thought it appropriate to tell the court that comments had been made that were outside the declassification process, lest there be any misunderstanding. It was done out of an abundance of caution. 14:23 14:23

Mr. DeLong's report in paragraphs 9 and 14 sets out precisely what the position was and that he took on board comments by other parties, but all of the report was his own. 14:23

You have heard Prof. Swire who confirmed that and was punctilious about it to the extent that, on his own initiative, he corrected the number of corrections. 14:24

With regard to the other reports, they were sent to the US government that had an interest in this matter. We say it's covered (a) by litigation privilege and (b) by common interest privilege. They wish to know whether they needed to adduce evidence in this case. Of course any adduction of evidence was going to be subject to the court's ruling as to whether it was admissible. 14:24

Comments were made, not to the witnesses, the other witnesses, they were made to Gibson Dunn and Gibson Dunn took comments from various people, including counsel in the case, and passed on comments to the experts that were not identified as comments by the US government for the very reason set out in the letter. It was desired so the witness wouldn't feel under any pressure in relation to that. They never had any dealings with the US government so they were passed on as comments on the report in the normal way. 14:24 14:25

You heard professor --

MS. JUSTICE COSTELLO: Well I'm not quite sure if the normal way applies in this case, Mr. Gallagher. Surely it's unusual where solicitors who are acting for a party -- 14:25

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: -- in proceedings, and as far as I know it's Facebook Ireland who is the party in the proceedings here, not Facebook Inc. 14:25

MR. GALLAGHER: Yes.

MS. JUSTICE COSTELLO: So let's assume that the attorneys of Facebook Inc. are acting as Facebook Ireland's attorneys.

MR. GALLAGHER: Yes. 14:25

MS. JUSTICE COSTELLO: But they are passing on material in a case to the third party.

MR. GALLAGHER: Yes, but that's done, Judge -- oh, sorry.

MS. JUSTICE COSTELLO: Now, I am sure they are entitled to do that if they wish.

MR. GALLAGHER: Yes, absolutely.

MS. JUSTICE COSTELLO: But it's hardly in the normal way. 14:25

MR. GALLAGHER: No, it's not in the normal way but this isn't a case in the normal way. Firstly, the DPC was, from the very beginning, saying this wasn't an adversarial proceedings, they were putting the position up. Secondly, these were matters of great significance 14:25 both obviously to Facebook and to the US government and in particular that they would have an opportunity of considering whether they needed to call any evidence. That's the classic case of common interest privilege where both parties have an interest in the outcome. 14:26 Reports are frequently shared in litigation between parties with a common interest in order to ascertain whether they have any comments.

In the case of Prof. Swire he was gone through the 14:26 declassification process and comments were made but, as it turned out, and as he explained, that they weren't part of declassification, so to avoid any misunderstanding having regard to his report he clarified that. 14:26

In the case of Prof. Vladeck, he received comments, as the letter says, from Gibson Dunn. They were just comments generally in his report seeking clarification,

as he said, and expanding matters. So there was nothing unusual about that. He wasn't aware about it and neither he nor the other witnesses were told for the reasons stated in the letter that it was to come as asking him whether matters required clarification rather than any impression that the US government was suggesting particular changes. It was felt that that was the more appropriate way to do it so that he wouldn't be affected in any way by the source of these suggestions and that is set out in the letter. 14:26 14:27

In respect of the three other witnesses, Ms. - Herr Ratzel's [sic] report was sent and there were no comments made; in the case of Mr. Robertson, his report was sent, a comment was made but it was not passed on, it wasn't deemed necessary to get the clarification required; and in the case of Prof. Clarke, sorry Prof. Clarke's report wasn't sent to the US government as has been made clear. 14:27 14:27

So all that has happened, Judge, is that comments were passed on to the witnesses in respect of their reports, which is permissible to do. In the case of the two witnesses that had an interaction with the US government, it was clear that these were comments by the US government and there was no issue in respect of that. In respect of the others, they weren't so informed but it was just passed on as general comments that were sent to the witnesses in the normal way. 14:27

Now, two things arise, Judge. Firstly, comments from counsel, and these were vetted by counsel and decided whether it was appropriate to pass on, are privileged as Mr. Murray acknowledges. That is a fundamental part of litigation privilege and there is no entitlement to enquire into or examine those in any way. 14:28

Then the only other issue is the issue that you raised with me: Is that privilege affected by the fact that somebody else commented on the report? The law is clear on that, it's not affected. But, separately, there is common interest privilege and it is common in litigation where a party has a common interest with another party, another person, that doesn't actually have to be a party to the proceedings, that they obtain comments or views of that person if they might have anything relevant to contribute. That does not destroy the privilege in the draft report, and of course those comments can be passed on; in the same way very often that counsel or solicitor will seek comments from some other person who might have something relevant to say in relation to the substance of the report, whether to correct something or to add other information that might be relevant. 14:28 14:28 14:29 14:29

That's what was done, we can of course swear to it. What we have done, Judge, is we have said we are not waiving privilege because we think this is an

inappropriate inquiry, but, in the case of Prof. Swire, he did say that on Thursday night his team had put together a document identifying for him what changes were made and he did refer to that. Entirely without prejudice to our privilege we made that available to the other side, and we would be inviting you to look at it to see the sort of comment that was made. 14:29

So, for example, to give one example, Prof. Swire said something about the scope of the Judicial Redress Act and the comment was 'actually the point you make is too broad, it has a narrower scope'; in other words, it was making sure that the position wasn't put in a more robust fashion than was actually justified. 14:30

So those are the sort of comments, they are all set out there for you to see to show that there was absolutely nothing inappropriate involved in that at all. But the United States government has not made any secret of the importance of this case and of its concern in relation to the matters in this case. 14:30

This involves an attack on the adequacy of the US legal system and it would be surprising if the evidence put forward with regard to the US legal system in response to the DPC, that they wouldn't have some opportunity of seeing that and making a decision as to whether or not they required evidence to address the matter. 14:30

That is particularly so, Judge, given the Commission finding of adequacy in the context of the Privacy Shield and any upsetting of that finding, any casting doubt on that finding as we submitted could have very serious consequences indeed. So that is the position and we reject absolutely and vehemently any suggestion that there was anything untoward or that there was a requirement to disclose. 14:31

A witness does not in the normal way disclose the comments that are made on his or her report by anybody, that's part of the privilege. As I say Prof. Vladeck wasn't even aware of the source of some of those comments and it was put to him today rather surprisingly that he somehow might have changed his report in some way which he, as you saw, absolutely and utterly rejected and of course it's a matter for you to assess all of these witnesses, but he made it quite clear that that was so. 14:31

14:32

But in the case, as I say, of Prof. DeLong it was made absolutely clear, in the case of Prof. Swire, to avoid any possibility of any misapprehension on the part of the court in the light of the terms of his footnote, that was made clear to the court and it was made clear at the outset of the evidence. 14:32

But as I say entirely without prejudice to our position we will swear an affidavit, but we do reject vehemently

this criticism of the approach that has been taken, Judge.

SUBMISSION BY MS. BARRINGTON:

14:32

MS. BARRINGTON: I wonder if I might say, Judge, at this stage that I think it's regrettable that it should have been suggested that there was something untoward in the role that the United States has played in these proceedings and in particular in relation to this issue. I've seen, Judge, a copy of the letter from Mason Hayes & Curran, we haven't seen until just now the enclosure outlining the changes that were proposed by Gibson Dunn to Prof. Swire. So that's something we have only just become aware of.

14:32

14:33

But I can say to the court that the position as outlined in the Mason Hayes & Curran letter is entirely correct and as outlined by Mr. Gallagher. It was quite clear when we applied to join these proceedings, Judge, that the reason we were applying to join as an amicus was because of our central significance and importance in these proceedings, the proceedings are about the adequacy of our law. And, accordingly, Judge, it was indicated to McGovern J that we were extremely anxious to ensure that the court had an absolutely complete and correct picture before it of what US law provided for, in particular in the event that the matter were to go to the Court of Justice, that the Court of Justice

14:33

14:33

would be provided with a description of the full panoply of oversight provided for by US law and not just judicial remedies.

In those circumstances it was indicated to McGovern J that the United States might wish to adduce its own evidence in relation to the description of the laws in the event that it perceived any inadequacy in the evidence that was before the court. Perhaps I could just remind the court of the chronology of events because the court may recall that the orders made by McGovern J provided for a tight timeline in that Facebook was to provide its affidavits by, I think, 4th November and the amici were to put in their affidavits within two weeks by 18th November. 14:34

That was obviously a tight timeline within which the United States would have had to determine whether it was adducing any evidence. So it needed to know what evidence was going to be adduced describing American law. That was a perfectly legitimate and valid concern for it to have and the affidavits were provided to the US government on a confidential basis with a view to permitting the US government to determine the extent to which it did or did not decide to adduce evidence. 14:35 Ultimately it decided not to adduce evidence, conscious of the concerns also that might exist in relation to the role of the amici adducing evidence. And we have seen, insofar as EPIC was concerned, that unnecessary

work was carried out in putting in affidavits seeking to in effect duplicate the work that was done. So that was a perfectly legitimate and valid concern.

And, secondly, of course as the court will realise in respect of two of the witnesses, there were classification or declassification considerations that had to be taken into account, and I don't think anybody is suggesting that that was anything other than entirely appropriate. 14:35

And for those reasons, Judge, I support entirely what Mr. Gallagher says on this issue and would submit to the court that all the contact, which was contact directly with Gibson Dunn, what happened thereafter my client isn't aware of, but it's apparent from Prof. Vladeck's evidence that he wasn't aware of the source of the comments made to him that corrected factual issues in relation to the reports. And that contact with Gibson Dunn, Judge, in my submission was entirely appropriate. 14:36 14:36

SUBMISSION BY MR. MURRAY:

MR. MURRAY: Judge, the one thing that neither Ms. Barrington nor Mr. Gallagher have told you is why was nobody told that these communications were taking place. Mr. Gallagher gives evidence telling you 'oh, this is very common', this is not very common. This is 14:36

not common at all. This is not a situation of two defendants exchanging information. This is a circumstance in which a defendant is in communication with an amicus with a view, we had understood, and if I have heard what has just been said correctly, it appears that the information was given to allow the US government to decide whether to put in its own evidence, but in fact I don't know that that's evident in the letter from Mason Hayes & Curran. 14:37

Whichever way it is, the US government responded with its comments and in our respectful submission the one thing that is absolutely clear - clear let it be said from Mr. Gallagher's own vigorous cross-examinations of both Ms. Gorski and Prof. Richards - is that counsel are entitled to interrogate the independence of witnesses, of expert witnesses, and the court is entitled to be given and parties are obliged to give to the court all information relevant to its assessment of the independence of the witnesses, and the proof of the pudding is in the eating. 14:37

Because if you had been told, in respect of some or all of these witnesses, that their evidence had been changed consequent upon the intervention of the United States government, the first question the court would ask, and to which it would be entitled to an answer, is where did the changes occur, what were they? That's all we asked for and it's all we ask for, that the 14:38

information be given.
Mr. Gallagher's and indeed Ms. Barrington's criticism of me for raising the question speaks volumes. All we want to know is what occurred and what exchanges were there, not between counsel and witness, not between solicitor and witness but between an entirely different third party and those witnesses with the consequence of those communications making their way into their reports. Hopefully Mr. Gallagher will provide us with the information in the form which we will be seeking this afternoon and that I hope will be the end of the matter, Judge. 14:38 14:38

MR. GALLAGHER: Judge, sorry, I want to make -- excuse me.

14:39

SUBMISSION BY MR. O'SULLIVAN:

MS. HYLAND: On behalf of Mr. Schrems I should say that obviously we were very taken by surprise by this particular disclosure and we are quite concerned by it. That said, we haven't engaged in the correspondence between Philip Lee and Mason Hayes & Curran, nor have we adopted any formal position as of yet. I say it's very surprising in circumstances where McGovern J, as the court will have seen from his judgment in relation to the admission of the various amici, EPIC were barred from communicating with us and us with them because we were seen as too closely aligned, but that's a matter that the court can consider for itself. 14:39 14:39

We are reserving our right to address the matter, whether by way of correspondence, which of course we share with the court and with the other sides, or by way of our submissions in due course to the court. 14:39
Obviously if it's considered necessary or appropriate following consultation between Mr. McCullough, Mr. Doherty and myself, our solicitor and our client that we will participate in any application that Mr. Murray would make in due course then that will be 14:39
done, but I am reserving my position in relation to setting out a formal stance on this in due course.

MS. JUSTICE COSTELLO: Thank you.

SUBMISSION BY MR. GALLAGHER: 14:40

MR. GALLAGHER: Sorry, I just wanted to clarify one thing in case there was any misunderstanding, Judge. The affidavit that we are doing is going to confirm the contents of the letter. The comments are the subject 14:40
of privilege and those are not going to be identified for the reasons that I have already said, in the same way that comments made by Prof. Richards' assistants and anybody else are not disclosed or by solicitors or counsel on behalf of the DPC or anybody else. 14:40

Of course independence is an issue, but this is a separate matter. Comments on the reports that are by way of observations mediated through counsel are not

matters that require disclosure and are not matters that need be put before the court. So the affidavit will confirm the position as set out in the affidavit.

MS. JUSTICE COSTELLO: In the letter, I haven't read the letter. But we'll await the outcome. I have heard all your observations and comments and no doubt we will be hearing more in relation to it one way or the other, but certainly the affidavit is to be provided when. 14:40

MR. MURRAY: Well, and we didn't know Mr. Gallagher was going to provide an affidavit, so we can discuss that with him. 14:41

MR. GALLAGHER: Well, sorry, I think it was requested. So I said we would provide it.

MR. MURRAY: Yes.

MR. GALLAGHER: I'll have to take instructions with regard to the mechanics of it. 14:41

MS. JUSTICE COSTELLO: Very good.

MR. MURRAY: Thank you, Judge.

MS. JUSTICE COSTELLO: Well we'll leave it at that.

MR. MURRAY: Thank you, Judge. 14:41

SUBMISSION BY MR. O'DWYER:

MR. O'DWYER: I don't really want to get involved in the controversy, but I just might point out, because I suppose it is relevant, that when EPIC applied to be an amicus, one of the points raised, actually, as far as I remember, by Facebook was that we weren't independent of a party, being Mr. Schrems, because 14:41

Mr. Schrems is on an advisory board which, I can't remember how many members, many academics from around the world on it, as far as I know 30 or 40 people, and on that basis we had to provide - this is from memory, I didn't realise this was going to come up - but an undertaking that we wouldn't have any contact with the party, being Mr. Schrems, because we were an amicus and because of our position as an amicus. The court can make of that what it wishes, but that was the basis upon which we were joined. 14:41 14:42

Sorry, Judge, I suppose, if I may, I'll move on to what we were actually going to submit.

MS. JUSTICE COSTELLO: Yes.

MR. O'DWYER: Judge, I intended to use the tablet, if possible. 14:42

MS. JUSTICE COSTELLO: I have it.

MR. O'DWYER: And I'm going to, I suppose because of the restrictions in respect of us giving evidence, I'm going to rely very much on the amended submissions and they are, if the court want to look at those. 14:42

MS. JUSTICE COSTELLO: I have those in hard copy.

MR. O'DWYER: Or on paper, they are at A12-0 on the e-book. I intend to stick fairly closely to those, not quite read them out, but certainly to run through them. 14:43 There's a number of quotations and I hope the court will accept that they are accurate quotations from the various reports and I won't have to open, go back on the tab to the reports etc. There is really only one

case I want to open very briefly and I'll do that at the beginning and I'll point out where that is on the tab.

Sorry, Judge as I have already indicated to the court I think on the last occasion we were directly involved, EPIC is an independent US - or, sorry, I should say of course that I'm appearing with Gráinne Gilmore instructed by, well Sinéad Lucey solicitor with the Free Legal Advice Clinic (FLAC). EPIC itself is a US based public interest research and educational organisation which was established to focus public attention on emerging privacy and civil liberties issues in the information age. 14:43 14:43 14:44

It served as amicus in many data privacy cases in the US, including, I suppose particularly relevant to this case, **Clapper -v- Amnesty**, which is what's been referred to as the Supreme Court **Clapper**, **Spokeo** and indeed the **Nickelodeon** case which came up in the course of some of the expert testimony. 14:44

We were accepted as an amicus, as you can see from the decision of McGovern J, we were accepted because of, I suppose, the particular expertise in surveillance and privacy law in the US and also, as the judge said, to offer a counterbalancing perspective from the US government on the position in the United States with respect to privacy protection. 14:44

So, Judge, while it's not, I suppose arising from that, it's not really the role of EPIC to compare surveillance and data privacy laws of the EU with those in the US, but I think, just to give a little bit of context, I might just touch upon EU law to begin with as I say just to give us a context to look at what we are dealing with in respect of or when we are considering US law in practice. 14:45

Judge, the Plaintiff Commissioner has highlighted in her statement of claim that the standard contractual clause, the SCCs, associated with data transfers from the EU, in particular Ireland in this case, to the US could conflict with the fundamental rights enshrined in Articles 7, 8 and 47 of the Charter. 14:45

Article 7 of the Charter provides that everyone has the right to respect for his or her private life, family life, home and communications. Article 8 provides for the right to: 14:45

"*Protection of personal data and specifically provides that, one, everyone has the right to protection of personal data concerning him or her, such data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down in law, but everyone has the right to access to data which has been collected* 14:45

concerning him or her and the right to that rectified. Compliance with these rules shall be subject to the control by an independent authority", in this case being the Data Protection Commissioner.

Article 47 provides: "*Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy and this shall be to an independent and impartial tribunal previously established by law.*" 14:46

And, Judge, in respect of those provisions, we submit that the recent decision, the very recent decision of the court in **Watson**, may be of considerable assistance to the court in respect of how these provisions are interpreted by the CJEU. I'm just going to open that decision, if I may, Judge, and really at the end, I want to go to the very end of it and what the findings of the court were and I might open those briefly to the Court. In the tab it's A13 Tab - sorry in the electronic tablet it's A13 Tab 37B. I'm dealing with the very last page, Judge, containing the findings of the or, I suppose, the answers to the questions from the court in that case because I think they are particularly germane to this case. 14:46 14:47 14:47

Judge, the case in general terms concerned the compatibility of data retention of non-content, and I'll go into this in a little bit more detail later on,

but of non-content data such as location data, which is obviously an issue relevant to Facebook and many other data processors who now will keep information or have information about where one is located, when we're using, for example, Facebook, where are we and possibly through the maps applications but there is other ways as well in which they might know where we are. It might not be classified as personal data as such and certainly in the US, but can certainly have or we might consider it to be relevant to our privacy, that somebody knows where we are at any given time, what shops we're in, what restaurants we're in. 14:48 14:48

MS. JUSTICE COSTELLO: You're meant to be down in the Four Courts and somebody finds that you might not be.

MR. O'DWYER: Exactly. 14:48

MS. JUSTICE COSTELLO: It might be a court that's near a golf course for example.

MR. O'DWYER: Exactly, Judge, that's the very point; that even though one might refer to it as non-content it's certainly very important to people and may in fact, or certainly the European court has considered go to the very heart of privacy. 14:48

So, Judge, sorry, that's what the **Watson** case was dealing with. There was data retention I think in the UK for, I think in Sweden it was for six months and in the UK it was for potentially twelve months. And the reason the data was to be retained by the telecommunications service providers was that the 14:48

national authorities could examine it later on if they needed to, well in general terms for anti-terrorism purposes or, I suppose, serious crime, for investigating serious crimes and then obviously they could check by location data, and we have seen it in this jurisdiction to a certain extent, they can sometimes check where people were, were they made phone calls from, if they were there. I mean there is an obvious example in Ireland of where, through the use of triangulation et cetera, they are able to work out where somebody was and whether he or she was somewhere at a particular time. So that was the general purpose of it and the data was meant to be retained for that so that the authorities could look into it. 14:49 14:49

And what the court found, the Court of Justice in probably a quite far-reaching decision only in December was that, you can see at No. 1, in answer to the first question, the court dealing with the Data Retention Directive says that: 14:50 14:50

"*Both the Directive itself and the provisions of the Charter must be interpreted as precluding national legislation which for the purpose of fighting crime provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*" 14:50

And then the second finding or the second answer --

MS. JUSTICE COSTELLO: Sorry, just before you go further, we're not on the right page on the receiving page as far as I can see. Oh, sorry, you're dealing with paragraph 134, is that it, the rulings? 14:51

MR. O'DWYER: Yes, the rulings. And I am really dealing, well on paper, sorry, Judge.

MS. JUSTICE COSTELLO: No, no, it's okay, we have it now.

MR. O'DWYER: For myself I'm using the paper but it is the final page 31, 32. I think there is just a list of the judges following that. 14:51

MS. JUSTICE COSTELLO: Thank you, we are on it now. We were on a second, a heading that had *"second issue"* or *"second question"*. 14:51

MR. O'DWYER: The second finding is that: *"Access of the competent national authorities to the retained data for the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."* 14:51

So, Judge, without wanting to go too much into European Union law, you can see the direct relevance particularly of the second finding to everything that we have heard over the past couple of weeks; access not

being subject to a prior review by a court or an independent administrative authority, obviously being a key issue.

So that's really where, I suppose, one might say the Court of Justice, and given this is a case that may end up with a reference to the Court of Justice, that would seem to be the most, I suppose, up to date statement on the position of the Court of Justice in respect of these issues and the, I suppose, proportionality of national security or foreign intelligence type surveillance. 14:52

The court will be familiar with or more than familiar at this stage with **Schrems 1**, but in that the court held that, and I quote: 14:52

"*Legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7.*" 14:52

To move on to the position in the United States in respect of surveillance in privacy law, Judge. As we already heard from several of the experts, there are concerns about the adequacy and fragmented nature of privacy protections in the US. Prof. Richards explained in his report - and where I have included the 14:53

quote I have the footnote in the submissions, Judge - he said that:

"*Unlike the EU and virtually all industrialised western democracies, the US does not have a comprehensive data protection statute.*" 14:53

Furthermore, Judge, we say that, unlike under the Charter or indeed the European Convention on Human Rights, there is no explicit right to privacy under the United States Constitution. The US Supreme Court has to date declined to recognise the constitutional right to information or privacy. There is, therefore, no equivalent of Article 8 of the Charter within the US Constitution. 14:53 14:54

The Fourth Amendment to the US Constitution does provide protection against unreasonable searches and seizures by the government. This protection is subject to numerous exceptions. One of the most significant exceptions is the so-called third party doctrine which limits the protection of data shared with a third party such as a service provider and in particular non-content data. And I'll deal with that in a little more detail later on, Judge. 14:54 14:54

In respect of government access to personal data transferred to the US, EPIC submits that when a US citizen's personal data or private communications are

transferred from the EU to a data processor such as Facebook in the United States, the data can be accessed by the US government. EU citizen's personal data and private communications are also subject to lesser protections than apply to the personal data and communications of US persons. Section 702, which we have heard so much about, being one obvious example of where non-US persons are treated differently than US persons. 14:55

The US government can gain access to the personal data and communications from a data processor such as Facebook within the US through several different mechanisms. These mechanisms include formal request as well as administrative subpoenas, court orders and mandatory directives issued under Section 702. Alternatively, the US government can gain access to the data transferred to and from the US directly and without the data processor's cooperation or knowledge by intercepting the data en route. This can include compelling the assistance of internet backbone providers to assist in intercepting data streams. The interception of data en route can occur in the US under Section 702, the Upstream programme, or at or outside the US border pursuant to Executive Order 12333. 14:55 14:56

The Foreign Intelligence Surveillance Act of 1978, I'll move on to deal with. The Foreign Intelligence Surveillance Act was enacted to authorise and regulate

certain governmental electronic surveillance of communications for foreign intelligence purposes. As we have heard, Judge, the traditional or what's known as the Title I FISA provisions require the government to follow certain procedures when conducting electronic surveillance, including obtaining a FISA warrant in most cases from the Foreign Intelligence Surveillance Court, the FISC. In 2008 Congress added new provisions authorising access to international electronic communications to enable the targeting of non-US persons located outside of the US. This is what we now know as Section 702 of the FISA. 14:56 14:57

In essence Section 702(a) empowers the Attorney General and the Director of National Intelligence to jointly authorise the targeting of any persons who are not US persons, who are reasonably believed to be located outside the US with the compelled assistance of an electronic communications service provider in order to acquire foreign intelligence information. 14:57 14:57

The US government is thereby authorised under 702 to obtain or scan international communications even those involving US persons without a warrant, though significantly Section 702 directives are not subject to any prior approval by the FISC. There's no warrant requirement or prior judicial review of the targeting or scanning. 14:57

The Attorney General and the Director of National Intelligence need only certify that they have submitted to the FISC for approval targeting procedures and minimisation procedures that satisfy the FISA requirements. 14:58

Section 702 provides that: "*The FISC shall have the jurisdiction only to review the certification, the certification submitted.*" The FISC order approving the annual certification does not involve the establishment 14:58 of probable cause or involve a review of whether any target is an agent of a foreign power or engaged in criminal activity, nor does the government have to identify to the FISC the specific facilities or places at which the electronic surveillance is to be directed. 14:58

The government can collect or scan communications under Section 702 after issuing directives to communications providers. The providers are legally obligated to:

14:58

"*Immediately provide the government with all information, facilities or assistance necessary to accomplish the acquisition of the data or the private communications.*"

14:59

The providers are required to comply with these directives in secret and are not allowed to notify the users. They also face civil contempt charges if they refuse to comply.

There is two known or main programmes under Section 702, the first of which is PRISM. PRISM was the subject of review following the Snowden revelations. Under this programme the government sends 14:59
a selector such as an e-mail address or possibly a phone number to a United States based electronic communications service provider and that provider must return communications sent to and from the selector back to the government. Even individuals who are not 14:59
associated with the selector can have their communications collected by the US government if they are sending messages to the target or have received messages from the target.

15:00

The experts agree, and we have heard this, that the precise technological means by which the government transmits selectors to the providers and the providers send them the data or communicate the data back to them has not been made public. None of the experts, 15:00
however, dispute the description in the Privacy and Civil Liberties Oversight Board, the PCLOB, 702 report to which I think Mr. Gallagher referred to several times. This describes how the tasking process works using a hypothetical USA ISP company. 15:00

So we include a quote from the report, Judge. But the NSA applies its targeting procedures and tasks, and there's an example of an e-mail, johntarget@usa.com, to

Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact the internet service provider. The company has previously been sent a 702 Directive and instruct the ISP to provide the government all communications to and from that particular e-mail address. The acquisition continues until the government detasks johntarget@usa.com. 15:01

If I could pause there for a second, Judge. One of the things that arises from that is that while there was some play on the fact that it wouldn't be a *name* or that there may not be necessarily key words used for this searching as the selector, one can see - and I know even from my own e-mail address that very often of course the e-mail addresses are the person's name. That's the case for me and I am sure many other people have either their full name or some version of the name. So while they are not searching for the name by putting in the e-mail, obviously the name is revealed. 15:01

MS. JUSTICE COSTELLO: Hmm.

MR. O'DWYER: But that's how effectively it's done.

Two things are clear from that description of the PRISM process. First, the tasking of the selector occurs after the company had been served the 702 Directive; second, tasking is an ongoing process. And I think in fairness several of the experts have said that, 15:02

including the experts for Facebook.
The fact that it's an ongoing process implies that it involves some form of technological communication.
I think Prof. Richards spoke at length about this, that there needs to be some technological connection for this information to be passed to and from the data processors. Whether this process can fairly be characterised as direct access to the company's servers is clearly a matter of some dispute between the experts and the others working in the area. 15:02

In addition to the PRISM programme the Upstream programme, which is the second programme that we know about, is also conducted under 702. This involves the interception of communications without knowledge or assistance of what are termed the *downstream* data processors. So a company such as Facebook wouldn't necessarily know anything about this, even though it might be data that's going between Facebook Ireland and Facebook in the United States. But neither end may necessarily know about this at all because Upstream deals with the internet backbone, so otherwise the fibre optic cables in general that are crossing the Atlantic and are obviously coming on land in the United States. 15:03

And, as I said earlier, Judge, if it's on land, if it's within the territory of the United States then we would be looking at Upstream; but if it's offshore or

possibly even, but certainly could potentially be at sea or at junction points that arise on land that may not be quite, may not be US, United States territory.

MS. JUSTICE COSTELLO: Hmm.

MR. O'DWYER: But there is certainly the possibility that it's intercepted en route but that is outside the US so that's covered by EO 12333 because it's outside the United States. 15:04

So the access to private communications on the Upstream programme is significantly broader than under the PRISM programme because Upstream involves scanning all messages over a particular network, including so-called multiple communications transactions, in order to conduct searches for what are termed *about* communications. As explained by the PCLOB, an *about* communication is one in which the selector of a targeted person such as that person's e-mail address is contained *within* the communication but the targeted person is not necessarily a participant in the communication. 15:04 15:04

The important point about *about* communications, as I think several of the experts were at pains to point out, Judge, is that this involves a consideration of the content of messages. Because it's going, it by its nature is a search or a trawl or a scan through the message. It's not just to and from a particular e-mail address, it's whether that message contains the 15:05

selector at all or a reference to the selector. So if the e-mail address is in the body of the message or if it happens to be a phone number, if that's in the body of the message obviously to find that you have to search the messages. And this I suppose really is the crux of the matter and I think this is something that, there was a reason there was so much emphasis on this with Ms. Gorski. Because this does involve clearly searching through large numbers of messages and searching through their contents. 15:05 15:06

One of the other, I suppose, by-products of this type of searching or scanning is that what may be taken from the data stream as such can be an MCT, and I don't think we need to go through that all again. 15:06

MS. JUSTICE COSTELLO: Hmm.

MR. O'DWYER: But I think the court is alive to the nature of an MCT, but it turns out that there could be several other communications connected to the communications that are found either by way - I think Prof. Swire gave the relatively innocuous example of a chain of e-mails, but there may also be other types of communications connected to the communications they are taking from the data flows so that they found the particular selector in because of the nature of alternate transmission and packets. I am certainly informed that it can be more than just chain e-mails, that there can be other communications attached to the particular communications that are taken out with the 15:06 15:06

particular communications that happen to be about.

MS. JUSTICE COSTELLO: So you are saying it's wider than a mere change of e-mails?

MR. O'DWYER: It's wider. That is a perfectly legitimate example and an easy example for us to understand, but it's a little bit more complicated than that I suppose... 15:07

MS. JUSTICE COSTELLO: I think it was Prof. Swire but it may have been one of the others who said that it's like the envelope and then you open up the envelope and like inside the envelope you have got your chain of e-mails, but if you are opening it up you're then looking at the contents of it. But are you saying there might be something else in the envelope? 15:07

MR. O'DWYER: There can be other things, that's certainly my, I'm not an expert technologist. I am instructed that it goes, it certainly can go beyond simple chain e-mails. 15:07

But, Judge, I suppose, I was going to give that example just to try and explain the difference between Upstream and PRISM. It's a very good example or a very good way for many of us to conceptualise what's actually happening here if one is to compare the situation with letters. 15:07 15:08

I mean even the thought that all letters going over to the United States or a very large number of the letters could be opened and the contents of the letter

examined, even if it's by a computer, if the computer is scanning it and picking out would be something that most of us would be alarmed about. And that really is a good example because that is what is happening. These are the equivalent. I mean e-mails are only one part of the data that's involved, but, if we take that as a simple example, most of us would think that an e-mail is something akin to a letter, you are sending it to someone, you assume it's private. You may be writing about private matters of course and the e-mail goes. 15:08 15:08

What happens in relation to Upstream and EO 12333 is that that letter is opened and something, in this case a computer, looks at it, scans it and sees if there is anything that they think is relevant based on these selectors. But even the thought of that, I think from certainly a European point of view, is disturbing. Whereas in America one of the things that arises is that they don't generally, and we make this point later in the submission, they don't generally consider the scanning by a computer to be any form of real interference with the data. 15:09 15:09

They only, it's only when a human engages with it, otherwise when an agent comes to look at all of the communications that have been picked out of the flow or the data flow as such, that really there might be an issue. Whereas we in Europe would probably consider, 15:09

I think, that a computer examining all of our mails, scanning them for particular references, something that could be very wide. If one thinks about, depending on whose e-mail address they put in as the target or whose phone number, it could actually be a very wide trawl to get this information and it could generate a lot of information, and that's what's taken out, so that's after the scanning is done.

15:10

But I think Ms. Gorski first used the letters as a direct comparator and it's a good example of or it's certainly of assistance in conceptualising what's actually happening. The FISC itself has recognised -- Judge, I am sorry, I should have said I'm really referring to two documents and we're quoting from two documents that are both on the file.

15:10

The first is the PCLOB report on 702 and the second is the FISC opinion from 2011, also in respect of Section 702, if the court wished to look at those in more detail later on, but they are...

15:11

MS. JUSTICE COSTELLO: You have them in your footnote?

MR. O'DWYER: Yes, they are in. And in fact I think Mr. Gallagher referred certainly to the PCLOB report on several occasions with the experts.

15:11

MS. JUSTICE COSTELLO: We might just change the stenographers.

MR. O'DWYER: Judge, the FISC itself has recognised that the US Government's collection of "about" type

communications is fundamentally different than other types of 702 surveillance. In 2011, attorneys representing the US Intelligence Community revealed to the FISA court that "*acquisition of internet communications through the Upstream collection under 702 was accomplished by acquiring internet transactions which may contain a single discrete communication or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities.*" 15:12

The FISC found that - and the particular, the location of these quotations is in the footnotes, Judge - the FISC found that the "*NSA's Upstream internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from or about a task selector and transactions containing multiple discrete communications, not all of which may be to, from or about a task selector.*" 15:12

The FISC emphasised that "*as a practical matter, this means that NSA's Upstream collection devices acquire* any *internet transaction transiting the device if the transaction contains a targeted selector anywhere within it.*" 15:13

The PCLOB report on 702 concluded that the surveillance technique used by the NSA to conduct "about"

communications searches operates in such a way that "A *person's communication will have been acquired because the government's collection devices examined the contents of the communication without the government having held* any *prior suspicion regarding that communication.*"

In simple terms, in order to identify communications *about* a selector, the NSA device must necessarily scan *all* communications transmitted over that facility, although the PCLOB notes in the 702 report that the NSA first filters the communications. So the first filtering is to eliminate purely domestic communications, which clearly have nothing to do with EU nationals. Thus, the US Government has access to and is scanning e-mails and other electronic communications en masse at the internet backbone level in order to identify and intercept certain target communications based on their contents. 15:13 15:13 15:14

The PCLOB notes in the 702 report "*nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication*" - and this is the point about the letters, Judge - "*The government* cannot *listen to a telephone conversation without probable cause about one of the callers or about the telephone in order to keep recordings of those conversations that contain particular content.*" 15:14 15:14

So in this case they're comparing it to telephone conversations.

The FISC found - and I know there does appear to be some dispute about the *scale* of this operation, but I think this seems to be a figure that's repeated quite often by the experts - the FISC found in 2011 that the NSA acquires more than 250 *million* internet communications each year pursuant to Section 702. So this idea that this is some sort of small scale operation and that there's only a handful of people being checked, if that's correct we're talking millions and millions and millions of communications. And they're the ones, Judge, I think, in relation to the Upstream programme, I mean obviously they're the ones that they've *taken*. That's *not* including the possibly, the exponential number of communications they've actually *searched*. That isn't even *considered*. This is the communications they *acquire*. 15:14 15:15 15:15 15:15

So quite straightforward -- well, reasonably straightforward under PRISM; communications to and from, all of those communications, they acquire. Under Upstream, these are all the ones to, from and about. And that comes, it seems, to 250 million in a year. 15:16

I suppose, I mean, to put it in context, I know there was some effort to try and minimise this as if it was

only, you know, it was a very minor operation on the basis of the numbers, but, Judge, I respectfully submit the court would want to look very carefully at those numbers. Because this seems to be the highlight figure, or the main figure. To talk about how many actual users might have been targeted in a six-month period as a proportion of the vast number of users - I think it was about 1.8, even of Facebook I think there's 1.8 *billion* users - so even a very, a tiny percentage, if they were targeted through PRISM, if it's 0.001 that's still a large number. If that's 47,000 in six months, it's 90 odd thousand in 12 months. And that's the users. 15:16 15:17

But you've got to remember the users is not the key figure. The selector is not -- I mean, you might have X number of users that have been, I suppose, or that they're tracking or who are targets through 702. But then you're collecting all, even through PRISM, you're collecting all messages to and from them. So obviously that's going to explode up into a very large number very quickly, which I think this figure of 250 million probably reveals. 15:17 15:17

Judge, the only statutory limitations on surveillance under 702 are the acquisition limits the targeting procedures and the minimisation procedures refer to in the section. There are five acquisition limits. The first four limitations are based -- are aimed, sorry, 15:17

at limiting the intentional targeting of US person communications. The fifth limitation requires that the acquisition be conducted consistent with the Fourth Amendment. The Fourth Amendment, as *all* of the experts have now agreed, does not protect non-US citizens, or non-US persons should I say, with no substantial voluntary connections to the United States. These limitations do not, therefore, protect EU citizens outside of the US for surveillance conducted under Section 702. 15:18

The Attorney General, in consultation with the Director of National Intelligence, must also adopt both targeting and minimisation procedures under 702. These procedures are subject to judicial review for their compliance with statutory requirements. It is notable though that neither the targeting nor the minimisation procedures about which we've had so much discussion in 702 provide *any* specific protections for non-US persons. Indeed, Section 702 clearly discriminates between US and, by its nature, non-US persons and imposes restrictions primarily, or what restrictions there are relate primarily to collection, use and dissemination of US persons' communications and information. 15:18 15:19 15:19

I've already mentioned, Judge, Executive Order 12333. This sets out -- it's a little by bit wider, in our submission, that perhaps Ms. Gorski indicated. This

sets out -- this is quite an all-encompassing Executive Order. And it *is* only that; this is an important point about both PPD-28 and Executive Order 12333, that these are just Executive Orders, these are almost -- these are policies, they don't have the -- they're not statutes and they can change -- 15:19

MS. JUSTICE COSTELLO: Well, what do you say to the fact that they've been, if you like, they're part of the Privacy Shield Decision and that while, yes, as a matter of strict law and power the President could revoke either or both tomorrow -- 15:20

MR. O'DWYER: Yes. And in secret.

MS. JUSTICE COSTELLO: -- this would have implications for the agreement in Privacy Shield, as an example?

MR. O'DWYER: Yes, I mean, that could certainly -- I mean, I don't think there could be any dispute about that. But one thing, Judge, that maybe hasn't come across in the evidence so clearly is that not only can they be changed tomorrow, and given there *are* a number of Executive Orders that *are* being changed under their current -- under the new President, there is another point that I think Prof. Swire mentioned briefly but perhaps didn't go into in any detail about; he said that he would *imagine* that such changes would be made public, but the point being that they don't *have* to be. 15:20 15:20

So both Executive Orders, or certainly my instructions are that both Executive Orders and these directions or policy directions can be changed, they could be changed

in secret, so nobody knows they've been changed except the people, except --

MS. JUSTICE COSTELLO: Directly concerned.

MR. O'DWYER: Directly concerned. So *we* might not know anything about that and certainly we, as ordinary users of the particular service, may know nothing at all about that. They could be changed *now* for all we know. 15:21

Now, I'm sure Mr. Gallagher was correct that obviously the Commission is going to look at these things in a review and it really will cause problems, I mean, if the United States Government were not to reveal that they'd changed these. But that's a different issue. We don't *know* what's going to happen about that. I mean, I think that review is in the summer, isn't it, I think, the next review, or even after the summer. So we have to deal with the situation as it is now. 15:21 15:21

But yes, but I mean, I think the important point is that we're aware that these can be changed like that tomorrow and that they can be changed in secret, they don't have -- they're not even the equivalent of statutory instruments in Ireland, which at least are recorded and, you know, there's a process through which they're changed and people are notified, or, well, at least you can find out that they've been changed. This is not the same thing at all. 15:22 15:22

But returning to 12333. This is quite an

all-encompassing order, dealing with a little bit more - I don't think Ms. Gorski intended anything by possibly limiting it to surveillance, it actually cover -- or particular types of surveillance. But it's actually the President's rules governing the activity of the entire US Intelligence Community. The Director of the NSA is authorised, through the order, to collect "*including through clandestine means, process, analyse, produce and disseminate signals intelligence, information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions.*" 15:22 15:23

The order grants broad authority to members of the US Intelligence Community to collect all forms of intelligence. The only collection limits imposed under the order are outlined in sections 2 and 3 -- or, sorry, 2.3 and 2.4. Under the order, "intelligence" includes foreign intelligence and counter intelligence. Foreign intelligence is defined broadly as information relating - this is under the EO12333- foreign -- 15:23 15:23

MS. JUSTICE COSTELLO: Yes, we had this this morning.

MR. O'DWYER: Oh, you had? So I won't go in into it. But so you can see that was very broad. Foreign persons is -- information about foreign persons *is* foreign intelligence. So there's, I suppose, a particularly wide and permissive definition. 15:23

Section 2.3 limits the collection, retention and

dissemination of information concerning United States persons by requiring that the Intelligence Community adopt procedures to limit the types of information collected to those specified in 2.3. Section 2.4 also imposes a general restriction on collection by requiring that members of the US community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. 15:24

As Prof. Vladeck explains in his expert report, EO12333 imposes fairly strict limits on surveillance within the United States, because as Ms. Gorski pointed out, it isn't *just* necessarily surveillance *outside* the US, there are certain circumstances in which there can be - this issue about transit and data transiting the US - there *can* be circumstances where it's applied *within* the US. But what Prof. Vladeck said in his expert report for Facebook was that EO12333 imposes fairly strict limits on surveillance *within* the US or directed against US persons abroad, leaving surveillance directed against non-US persons abroad subject only to more general collection restrictions. 15:24 15:25

Then, Judge, to move on to PPD-28. And this is Presidential Policy Directive 28. And again the comments I made in respect of the EOs applies to even greater extent to these policy directives, that they can be changed. But this was adopted by President 15:25

Obama and it does impose certain restrictions on US signal intelligence activities involving personal information *regardless* of the person's nationality or location.

15:25

The first section of the PPD-28 outlines four principles that are framed as *general* limits - so it's more of a general overarching limitation - general limits on signals intelligence collection.

15:26

The first principle requires that the collection be authorised by law or Executive Order and undertaken in a lawful manner. The court will probably be familiar with that there'll be something familiar to Article 8, European Convention on Human Rights might be applied, you know, in accordance with law. So the first test is that if, for example, a deportation order is made, is it made in accordance with law? And then we might move on to consider the proportionality of that. But the first point, that it's authorised by law and undertaken in a lawful manner. The second principle states that privacy and civil liberties shall be integral considerations in the planning of signals intelligence activities and prohibits collection for specified *improper* purposes. But I don't think they're particularly relevant in this case. The third principle prohibits the collection of foreign private commercial information or trade secrets in order to afford a competitive advantage to US companies. And

15:26

15:26

the fourth and final principle requires the collection be tailored as feasible.

So they're quite general in nature, that it isn't unlawful. And I'll move on to that, because there *is* an issue that we feel hasn't perhaps been developed to a great extent before the court so far, which is the idea of authorised and unauthorised and how important that is and what remedies you might have available. Because if it's authorised, so if it's under, for example, 702, the surveillance, if that goes through the procedures that Prof. Swire described, the in-house procedures shall we call them, it's *authorised*, it's allowed, there is a statutory provision under which it's allowed, there is various administrative -- 15:27

MS. JUSTICE COSTELLO: Just as the data retention in **Watson** was authorised by Sweden and the UK in --

MR. O'DWYER: Exactly, Judge. But that's the key point, that's why I felt it was important to open that case. This seems to be a really key difference between the two jurisdictions, that where it isn't -- that under EU law, clearly Mr. Schrems and Mr. Watson and Mr. Davis and all of these other people that were involved in these cases were able to challenge what is effectively *authorised*, *lawful* - lawful in the sense of it's permitted by law - surveillance or data retention, whereas that creates all sorts of difficulties with whatever limited protections they have in the US, nearly all of them we'll find - and this just hasn't

really been dealt with in detail by the experts, although they've mentioned it in passing - it requires that the surveillance is *unauthorised*.

The real difficulty is what do you do if you want to challenge it on a, I suppose, facial basis, if you want to say 'This is not' -- 'This is unconstitutional, they can't do' -- 'Even though it's lawful, it's provided for in the Act, they can't do this because this is a fundamental interference with my private life rights'? And that's a *real* issue, and it's definitely a point of difference between the EU -- 15:28 15:28

MS. JUSTICE COSTELLO: And do you make the point that, of coupling, if you like, this authorised challenges, if I can put it that way, or challenges to authorised acts in the context of the scope of what can be authorised? 15:29

MR. O'DWYER: Yes.

MS. JUSTICE COSTELLO: I just want to make sure I understand your argument. 15:29

MR. O'DWYER: And that makes it very difficult -- well, we do actually deal with it in a little bit more detail in the submissions. But effectively, many of the, or I think in fact *all* of the types of secondary private, the legislation that's been referred to by the experts, certainly Prof. Butler has produced an analysis - unfortunately we're not able to, we're not providing evidence as such - but *all* of them apply to, the idea is that they apply to *unauthorised*. 15:29

I mean, if you want to challenge face-on 702 because you believe simply that your data shouldn't have been interfered, it shouldn't have been copied, it shouldn't have been scanned, whatever it might be, you run into very different problems, primarily the problem that non-US -- or non-EU citizens can't, effectively, sue under the Fourth Amendment, so otherwise the constitutional right doesn't apply. Even if -- and there's a number of reasons it doesn't apply. But just as a non -- we've seen that, you have to have this connection to the United States. 15:30 15:30

And that's another key difference between the different, between the EU and the US, that you require that and, therefore, you're simply not able to bring that type of -- actually at a fundamental level. And I think in the end, even Prof. Swire accepted eventually in cross-examination by Mr. Murray that an EU national based in the EU, living in the EU, not living in America, can't have a Fourth Amendment type challenge in the United States, because they don't have the connection that's necessary. And that's a key stumbling, or a key, I suppose, stumbling block or whatever you want to call it, a key issue for EU nationals were we to *try* and get some form of remedy or something done about this type of surveillance. 15:30 15:30 15:31

So I was just, I was explaining about the fourth and

final principle, which *might* be seen as advantageous for everyone, really requires that collection be tailored as feasible. But in that context, Judge, the Director of National Intelligence has explained that "*Pursuant to the fourth principle, the Intelligence Community takes steps to ensure that even when we cannot use specific identifiers to target collection, the data to be collected is likely to contain foreign intelligence that will be responsive to requirements articulated by US policy makers pursuant to the process explained in my earlier letter and minimises the amount of non-pertinent information that is collected.*" 15:31 15:32

I suppose what's particularly significant about that statement is, Judge, that you can see that the Director of National Intelligence is saying that they do in fact engage in - we assume under EO12333 - that they do engage in, effectively, mass surveillance without discriminants. 15:32

Then, Judge, just lest there be any doubt about that, we know that section 2 of PPD-28 deals with bulk collection. So there can't legitimately be any claim that bulk collection *doesn't* take place. The only issue of real contention raised with Ms. Gorski, I think, was whether what happens under Upstream could be described as bulk collection, as opposed to bulk scanning. And to a certain extent, we would submit, certainly from a European point of view, that the 15:33

difference is quite subtle and wouldn't necessarily apply in Europe. So this idea that they're only scanned, as opposed to collected - and you may remember there was some debate about whether they were actually copied. 15:33

MS. JUSTICE COSTELLO: Mm hmm.

MR. O'DWYER: To a certain extent, I think that technologists would agree that there has to be *some* form of, even however brief, of copying, even in terms of cash. But whether there is something longer than 15:34 that, as Ms. Gorski was -- people simply don't know when they're doing Upstream. So otherwise, do they copy massive amounts of data for a very short period for the purposes of this scanning? What doesn't seem to be quite possible - and I think this is what she was 15:34 saying - was to literally pick it up as it passes by. So otherwise --

MS. JUSTICE COSTELLO: I think she said it would slow down the flow.

MR. O'DWYER: It would slow down the flow. But I mean, 15:34 nobody --

MS. JUSTICE COSTELLO: Well, she wasn't a technology expert, yes.

MR. O'DWYER: -- nobody here certainly knows exactly how it happens. But certainly it's more likely than 15:34 not that it does involve some form of copying it on the mass scale, so copying that to allow them to do that. Now, that's certainly, that *is* what we would describe as bulk collection. That does seem to be permitted and

it's specifically referred to under PPD-28. But whether that's relating back to Upstream or whether it's just to the offshore or non-US collection isn't entirely clear.

15:35

Finally, Judge, in respect of PPD-28 - and I know, I've been told you heard a lot about this this morning, so perhaps I won't dwell on it - but that it extended EO12333's limits on dissemination and retention of personal information, but did not extend the collection limits. And we include quotes, just what it says in respect of dissemination and retention. So otherwise, PPD didn't change the collection or didn't limit collection of data, but rather dissemination and retention of personal information, so otherwise *after* it's collected.

15:35

15:36

Then, Judge, if I move on to safeguards for EU citizens. It's submitted that US law fails to ensure an adequate level of protection for the personal data and private communications of EU citizens outside of the US. This is because -- and we've really three points in respect of this. First of all, the scope of application of privacy protections and the definitional scope of personal information in the US law are restrictive. And if I could deal with that first. US privacy law is characterised by particularly narrow conceptions of privacy and personal data, which in turn limits the scope of relevant constitutional statutory

15:36

15:36

and regulatory privacy protections.

Judge, I mentioned earlier about non-content, and we refer to a case called **Smith -v- Maryland** where the Supreme Court considered the use of a pen register device to record telephone numbers dialled by a criminal suspect but not the content of the calls. The court held that "*a person has* no *legitimate expectation of privacy in information he voluntarily turns over to third parties, such as telephone companies.*" 15:37

So that would at first, on a superficial level, would appear to mean they're just saying 'If you hand it over to Facebook or whoever it might be, hard luck, you've done it, you must have known that there'd be something involved with that'. Now, to be fair, that case is an old case related to non-content, but -- and as we point out, the practice in the US Department of Justice has been to *get* a warrant when seeking to obtain content of US persons' e-mail communications that are stored on third party servers in accordance with the decision in a lower, in one of the circuits - and I think this case has been referred to several times - **Warshak**. So even though the Supreme Court itself hasn't dealt with this issue or directly with the issue of content of e-mails and whether they are protected under the Fourth Amendment or not for US citizens or anyone else, certainly one can take it that **Warshak** *might* be the position that would be adopted. And I think that's the

general view even of the, even among the experts here.
MS. JUSTICE COSTELLO: And the practice of the government is to apply it?
MR. O'DWYER: Yes, and the government has in fact, seems to effectively apply **Warshak**. This is in respect of US citizens. But the point about third parties though certainly -- 15:38
MS. JUSTICE COSTELLO: And that's the Fourth Amendment point?
MR. O'DWYER: That's the Fourth Amendment point. But certainly the point, it is a very important point, that we're very much restricted to -- we're looking only at content then rather than non-content type data. Clearly, any reading of the **Smith -v- Maryland** case *doesn't* apply, the Fourth Amendment *doesn't* apply to non-content data. And indeed that's another point of very obvious comparison with **Watson**. 15:39 15:39

Even in cases where personal information and communications transferred from the EU *are* subject to protections in the US, these protections may not attach until the data is viewed, reviewed or disseminated by a government agent. I've made this point earlier on, Judge, and in fact there's a footnote to where we've included that with a quote from Robert Litt, who I believe was -- 15:39 15:40
MS. JUSTICE COSTELLO: Is that the same Mr. Litt that we've had?
MR. O'DWYER: Yes. A very senior figure. And he said

- sorry, this is just in our footnote - but "*If the government electronically scans electronic communications, even the content of those communications, to identify those it is lawfully entitled to collect and no one ever sees a non-responsive communication or knows that it exists, where is the actual harm?*"

So otherwise, if it's scanned by a computer, where is the harm? Whereas I think we would take a very different view in Europe to -- 15:40

MS. JUSTICE COSTELLO: We haven't read the article, but possibly he's looking at all the stuff we've been debating over the last few days about having to establish that you've suffered a harm. 15:40

MR. O'DWYER: Yes. But I mean, he is, he does seem -- I mean, I *think* what he is saying is, and I don't mean to try and interpret it from an Irish point of view as such, but I mean, he seems to be saying that where is the actual harm if no human views it? So otherwise this scanning that goes on, that that's done by computer. 15:41

The second point, Judge, point (b), is that personal data communications of non-US persons are excluded from important US privacy safeguards. Many of the privacy safeguard under US law in fact operate to the *exclusion* of EU citizens situated outside the United States. Firstly, it's submitted, as we already said, that the Fourth Amendment does not protect the privacy of EU 15:41

citizens outside the US. The experts in the case have *agreed* that the protections of the Fourth Amendment do *not* extend to individuals who have no "*substantial voluntary connections to the US*", such as physical presence in the country. US courts have found that the Fourth Amendment "*does not apply to searches and seizures by the United States Government against a non-resident alien in a foreign country.*" So there can't *really* be any dispute but that we are excluded, we, as EU citizens, are excluded in that way. 15:41 15:42

Secondly, US surveillance laws authorise the collection of foreign communications without the requirement of individualised suspicion or probable cause and in the absence of judicial oversight. Obviously we're referring back to Section 702. Section 702 specifically authorises broad scale surveillance of non-US communications without a warrant. The key limitations on 702 surveillance - namely, the acquisition limits, targeting procedures, minimisation procedures - effectively exclude non-US persons' communications from protection. 15:42 15:42

It *is* true that some limitations on 702 apply regardless of whether the target is a US person. For instance, collection is required to be conducted to the greatest extent feasible to minimise the acquisition of information not relevant to the unauthorised foreign intelligence purpose. However, the caveat of 15:42

reasonable feasibility is important. Even information that was *not* relevant to foreign intelligence could be lawfully captured in circumstances where it is not reasonably feasible to focus collection on relevant information because of technological or intelligence restraints. In any event, the relevance threshold is particularly low. It is noteworthy that there's no requirement for information to be *necessary* to the authorised purpose. 15:43

In addition, the US has, under Section 702, gained access to international communications in bulk and scanned or processed these communications without individualised suspicion or judicial oversight in order to target certain selectors. 15:43

(c), the third point in respect of that, Judge, is that many privacy rules are subject to executive branch modification or rescission. We submit, and I think I've already made this point, but that many of the rules and restrictions discussed in the expert reports submitted by various experts are not enshrined in law and can be modified or rescinded by the US executive at any time after discretion. This is a significant limitation on the long-term violability of these rules, especially during a change in administration such as is happening now. 15:43 15:44

Moving on to the redress for EU citizens, which I know

is a key issue, Judge. It's submitted that US law does not provide an effective means for EU citizens to seek redress for claims related to surveillance carried out in violation of their rights under Articles 7 and 8 of the Charter. Firstly, EU citizens with no substantial 15:44
voluntary connections to the US have no mechanism to challenge authorised surveillance programmes that could violate their fundamental rights. Second, even challenges to *unauthorised* surveillance have severely restricted remedies. Thirdly, data protection remedies 15:44
of access and correction are also restricted. Finally, the standing and state secrets doctrines are structural barriers that significantly restrict all forms of judicial redress in privacy cases.

15:44

I suppose, Judge, rather than go into too much detail on this, I'd say that EPIC, having both read the reports of Mr. Serwin and Prof. Richards and had the chance to hear their evidence, we would submit that their reports and their evidence provide a detailed and 15:45
accurate account of the limitations of civil remedies available under US law.

Judge, we make the point after that that maybe hasn't been drawn out so much by the experts that US law does 15:45
not provide EU citizens with effective redress for violations of their Charter rights arising from authorised surveillance. And we go through a number of the statutes that have been referred to by different

experts.

Judge, I just would highlight in respect of that from the submissions in respect of this point that we do have in the submissions that the Privacy Shield Ombudsman mechanism, actually the submissions say *does* provide a mechanism to seek judicial redress and what was meant to be said was that it does *not*.

MS. JUSTICE COSTELLO: Well, the version I got has the "not" in it. If you're quoting from paragraph 91? 15:46

MR. O'DWYER: I think it is, that would be correct, Judge. Let me just check...

MS. JUSTICE COSTELLO: Oh, I see what you mean. It's at the beginning of the paragraph it doesn't have a "not", but at the end of the paragraph it does. 15:47

MR. O'DWYER: Yes, Judge, it does go on. But just to make sure that the amicus isn't saying that it does. And indeed what we say about the Privacy Shield Ombudsman mechanism which *might* be available to EU citizens requires that EU citizens submitting inquiries 15:47 regarding access to their personal data for national security purposes must allege a violation of law or other misconduct to merit referral of their complaint to an appropriate US Government body. Even then, the only reassurance that the Ombudsman can provide to an 15:47 EU citizens is that their complaint has been properly investigated and, two, any noncompliance with US lawyers, statutes, executive orders, presidential directives or agency policies has been remedied.

The Privacy Shield framework thus does not provide -- Ombudsman framework should I say, does not provide any means to challenge *authorised* surveillance and contravenes -- that might contravene Charter rights. 15:48

And I don't want to over emphasise this point, Judge, but I think it's important the court sees, and you may when you're going through the evidence about the various statutes, you'll note - and we've gone into it 15:48 in some detail in the submissions - that they repeatedly refer to the idea of unauthorised. And to take the classic example, that's what we might term rogue agents. So otherwise, if somebody goes outside, does some surveillance, uses the various computer 15:48 systems to check up on somebody or to do something that hasn't gone through, I suppose, the various procedures that Prof. Swire in particular detailed and aren't really acting under, be it Section 702 or EO12333, that they're doing something outside of that, something, I 15:48 suppose, of their own volition or off their own bat. And for the reasons outlined, Judge, we say that the remedies that permit challenges to *unauthorised* surveillance are effectively untenable.

15:49

In respect of... We say that the US remedies available for *unauthorised* surveillance are so restrictive as to be untenable, as I said. The doctrine of sovereign immunity may entirely *bar* claims against the US

Government or agencies or government employees acting in their official capacity. As a result, 1810 only provides a means to seek redress against individual government agents acting ultra vires - again this idea of unauthorised for electronic surveillance. 15:50

We go through a number of the different statutes, as I've explained, Judge. And then, Judge, finally, if I could refer you to the more general points, which are the overarching barriers to redress likely to preclude 15:50 EU citizen claims involving US surveillance. And these, Judge, are the ones that even US persons will struggle, will very much struggle with. And I suppose I can put it fairly simply, that there are three major difficulties, or overarching difficulties that *anyone* 15:50 trying to challenge surveillance will have in the -- well, particularly at a facial level will have in the US courts. And those three are standing, state secrets and, of course, notice, which is a key issue, having been identified by Mr. Murray originally. 15:51

The problems about standing, the court has -- has been rehearsed before the court over several days, but I'd ask the court to consider **Clapper -v- Amnesty**, to look carefully at **Spokeo** and consider the knock-on effect of 15:51 that and where that leaves standing.

I think the state secrets doctrine has been already opened by the experts and perhaps the court might

review that, the evidence that's been given in respect of that. But that's another difficulty that *anyone* will experience trying to challenge surveillance in the United States court.

Then finally and probably most significantly, the notice, that how one is supposed to *ever* be able to challenge something under the United States standing doctrine when you have no notice that it's occurred or might occur and you can't find out, it becomes almost impossible to launch such a challenge. And that's a really key point, in our submission. 15:52

And when you think of these cases, **Amnesty** and **Clapper** -- or, sorry, **Amnesty** and **Spokeo**, these involved *US* citizens and *they* couldn't establish - or bodies based in the US in the case of Amnesty - and *they* couldn't establish standing for a number of different reasons, primarily because they hadn't got notice of proof that they were going to be -- 15:52

MS. JUSTICE COSTELLO: Well, I think Spokeo certainly had notice of what had gone wrong in his credit report.

MR. O'DWYER: Spokeo had. But **Spokeo** was a different point. But I know the court - I mean, I've been here most of the time - I know the court has heard endless evidence in respect of **Spokeo**. I can say that I suppose we have some particular knowledge of it because we were an amicus in the case, but I think in general terms we would certainly be, if it's a matter of 15:53

aligning ourselves - and I don't mean, as an amicus, to say that we are aligning with a particular party - but certainly the evidence, I think, of Prof. Richards in respect of **Spokeo** was probably what we would regard as the most accurate. 15:53

Judge, so they're really our final points, the standing, state secrets and notice. If I could just, I suppose, in conclusion and to summarise, if I can make the following three points. That there were a number 15:54 of general deficiencies in US privacy law; it's fragmented and many of the laws are subject to significant exceptions; that there's no constitutional right to informational privacy, the equivalent of the Article 8 that we've seen, it's very clear. 15:54

Secondly, that there's differential protection for non-US persons. It's clear that 702 differentiates between US persons and non-US persons; that the remedies that *might* be available are not effective; 15:54 that most of the remedies, or in fact *all* of the remedies that have been referred to, apart from the facial challenges, relate, in our respectful submission, to unauthorised type surveillance; that if one were to try and launch a face-on challenge to -- if 15:55 one were to try to launch a face-on challenge to the authorised, so therefore the one -- to surveillance that *has* passed through the relevant procedures and *is* permitted under Section 702 or EO12333, that one will

face, well, the obvious difficulty that as an EU citizen you can't rely upon the Fourth Amendment, because you don't have the necessary connection with the state. And even the provisions that might assist a person if they're trying to challenge unauthorised surveillance, that one comes across the what I've termed the overarching problems, the three I've identified: Standing, state secrets and notice. 15:55

They are my submissions. 15:56

MS. JUSTICE COSTELLO: Thank you very much.

MR. O'DWYER: Thank you, Judge.

MS. JUSTICE COSTELLO: Mr. Cush, would you like to start, or would you want to leave it until tomorrow?

MR. CUSH: Well, I'm certainly happy to start, I'm entirely in the court's hands. I was just going to ask for one favour, as it were, Judge. I will be quite short, in or about an hour, but if the court would accommodate me by not sitting before 11:15 tomorrow, I'd be very grateful. If that's possible? 15:56

MS. JUSTICE COSTELLO: Oh, no, absolutely. If you were going to ask me to sit earlier, it might've been an issue. But certainly. And we can sit through until quarter past one, just to make up the time.

MR. CUSH: Well, I certainly won't take it that far, Judge. 15:56

MS. JUSTICE COSTELLO: Well, very good, 11:15 then.

MR. CUSH: I'm very grateful.

THE HEARING WAS THEN ADJOURNED UNTIL THURSDAY, 2ND MARCH AT 11:15

B

C

D

E

G

H

I

M

N

O

P

Q

R

S

T

U

Y

Z

—