THE HIGH COURT

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, 15th FEBRUARY 2017 - DAY 5

5

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:	**McGRATH McGRANE** **SUITE 323** **THE CAPEL BUILDING** **MARY'S ABBEY** **DUBLIN 7**

INDEX

THE HEARING RESUMED AS FOLLOWS ON WEDNESDAY, 15TH FEBRUARY 2017

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

MR. MURRAY: May it please the court. Judge, Mr. Collins had just begun his opening of Facebook's expert evidence.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: And he had, I think, introduced you to Peter Swire's report which you'll find in trial Book 3, that's at Tab 5, Judge. And he had just concluded, I think, at the end of page 1-4, moving on to paragraph 14 on page 1-5. 11:06 11:07

MS. JUSTICE COSTELLO: Sorry. Tab 5 is the, that's the table of contents and everything? 11:07

MR. MURRAY: Yes. And, Judge, at the bottom of the page you'll see it's numbered 1-4, 1-5.

MS. JUSTICE COSTELLO: Oh, Yes, I have that. The biographical summary? 11:07

MR. MURRAY: Well, and if you go to the next page *"systemic safeguards in the US law and practice"*.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: Judge, just before going through the meat of this report, it just occurs to me that it may be of assistance to perhaps focus the court on what we say the aspects of the evidence which you are about to consider, what aspects of it are relevant and how they become relevant. 11:08

The material before the court and the experts in particular, this report is dense, it's detailed and it is lengthy. I suppose as one goes through it it's perhaps easy to lose sight of the fact that the critical relief which is being sought by the Plaintiff here is a *reference*. We're not asking the court obviously, nor can we, to make a determination that the SCCs are invalid. And it's clear that the test which you apply to that question is whether you share the Commissioner's doubts as to the validity of the SCCs. 11:08 11:09

If you have *any* doubt you must refer, in our submission, and I think that follows from paragraph 65 of **Schrems**.

11:09

Now, Judge, while there are disputes around important parts of US law, in our respectful submission, as you consider the expert evidence, there are a number of critical and easily identified features of it which we say, with respect, leave the court in a position where it cannot but have a doubt as to the validity and cannot but share the Commissioner's doubts. 11:09

First, it is clear that the standing doctrine applied by the United States courts in cases of alleged data privacy violation is not the same as that mandated under Article 47. It is not the same as that mandated by European law. The court has already heard one highly experienced expert witness explain the standing 11:09

doctrine of the United States in this context as an *extraordinarily* obstacle to data protection claims in the national court context. She said it was extraordinarily difficult for the Plaintiffs to establish standing. And indeed Facebook's own witness, Prof. Vladeck, whose report I will come to later in the morning, observes that the Commission, as he puts it, *rightly* raises concerns about Article III standing and that stands in *direct* contrast to the position in European law. 11:10

Second, the Court of Justice has made it clear in its **Watson** decision, which I will open to you when I come to make my closing submissions tomorrow, it has made it clear at paragraph 121 of the **Watson** decision that, where national authorities access the data of citizens, pursuant to warrant or these powers of compulsion which are considered in **Watson**, where that occurs they must notify the person whose data has been accessed as soon as that notification is no longer liable to prejudice the investigation. That's a mandatory obligation and it was related by the Court of Justice in **Watson** as you might expect to the fact that, without that obligation of notification, you don't have an effective remedy, you don't know. 11:11

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: And again the expert evidence you've heard already in the case last Friday was that in the United States the vast majority of individuals who are subject

to the government surveillance will *not* receive notice of that fact, and that indeed is part of the difficulty presenting itself with the US standing rules.

Thirdly, Judge, non-US citizens resident in Europe are almost certainly debarred from relying upon the Fourth Amendment to obtain free-standing relief in respect of data violations in the United States. They cannot bring a claim, and I think the expert evidence in this regard is close to unanimous, they cannot bring a claim in this context to obtain damages for violation of their constitutional rights. That again stands in contrast to the remedial position in European law. 11:12 11:12

Fourthly, the various statutory remedies, insofar as they allow claims for damages, in US law require actual damage. There's no compensation for the violation of the right, there's nothing to enable compensatory damages to reflect the inherent effect of the violation on the data privacy right. They require that the violations be wilful and intentional. 11:12 11:13

Fifthly, the statutory causes of action, in particular the Privacy Act and the Judicial Redress Act, are riddled with exceptions, with the NSA and CIA exempt from some or all of their provisions insofar as EU citizens are concerned. 11:13

Sixthly, state secrets privilege may debar plaintiffs

from claiming relief from the courts.

And, seventhly, as you have heard, there's very little control over the use of Executive Order 12333.

11:13

Now, while the Facebook evidence which as I said we're about to consider certainly presents the position that the remedies in US law for EU citizens whose data has been accessed by the state are in the round adequate, that's the, I think it's fair to say the pith of the case they advance; it is in our respectful submission very difficult to say, having regard just to those seven points which I have identified, that there is no doubt but that the SCCs are valid.

11:14

11:14

Facebook also, Judge, advance various objections which I suppose present issues of European law rather than US law. EU review is precluded because these are national security issues. You've already heard Mr. Collins refer to their construction of Articles 25 and 26. The suggestion that the, as it was described by the witness last Friday, Kafkaesque and non-binding Privacy Shield Ombudsman appointed and accountable to the executive is an adequate remedy, that there are adequate internal contractual remedies in the SCCs or that there is an interpretation of Article 47 which requires a broader analysis than we suggest, and those issues are presented in some of the expert reports.

11:14

11:15

Some of the expert reports from Facebook suggest that **Schrems** was wrongly decided; a proposition, which, if seriously pursued, one would have thought would prompt the embracing rather than opposing of a reference. But each of those issues in our respectful submission is an issue which, in its own terms, could only be resolved by the European court. Certainly as you look at Facebook's submissions around these issues, the court will be struck in my respectful submission by how removed they are from any clear authority establishing the propositions they advance. 11:15 11:16

So in our respectful submission, while obviously I will I hope fully and fairly open the expert evidence which has been adduced by Facebook, it should be viewed in the light of what the relief that is being sought is and what the test the court is applying in determining whether to grant the relief. 11:16

So, Judge, if I can begin at Mr. Swire's report page 1-5, *"Systemic Safeguards in US Law and Practice"*. In paragraph 14: 11:16

"*The US government is founded on the principle of checks and balances against excessive power. The risk of abuse is potentially great for secret intelligence agencies in an open and democratic society – those in power can seek to entrench themselves in power by using surveillance against their enemies. The US experienced*

this problem in the 1970's, when the Watergate break-in occurred against the opposition political party, the Democratic Party national headquarters.In response, the US enacted numerous safeguards against abuse, including the Foreign Intelligence Surveillance Act of 1978 (FISA).

In recent years, following the Snowden revelations that began in 2013, the US has enacted an extensive set of additional safeguards against excessive surveillance, as shown by the list of two dozen reforms discussed in my 2015 Testimony for European privacy regulators, and by additional safeguards put in place since then. Overall, many of the most effective protections for privacy, in my view, exist at the <u>systemic</u> level, rather than occurring primarily on a retroactive basis through an individual remedy."

And I would, Judge, just ask you to note that general description of the US remedies as Prof. Swire sees them. 11:17

"*This proceeding assesses the adequacy of the protections against excessive surveillance that occur when personal data that is in the EU is transferred to the US. When the US government conducts a wiretap or otherwise gains access to personal data in the US, the investigation within*

the US is governed primarily by either foreign intelligence or criminal rules.

[16] I do not discuss Executive Order 12,333 in detail due to my understanding of the scope of the proceeding, which concerns the adequacy of safeguards against excessive surveillance in the event of transfer of personal data from the EU to the US. Executive Order 12,333 is 'the principal Executive Branch authority for foreign intelligence activities not governed by FISA' and is, indeed, the 'principal governing authority for United States intelligence activities outside the United States'.

For data transfers, the US logically could collect the information in two ways. First, if the personal data is collected within the US, then collection is done generally either under law enforcement authorities or foreign intelligence authorities, notably FISA. Second, the US government could seek to gain access to the data while it is being transferred, such as through undersea cables. As discussed in Chapter 3, the EU Commission considered this possibility in its opinion on Privacy Shield, and found adequate protection. In addition, in recent years strong encryption has become standard for transmission of social network, web mail, and other types of communications, so any hypothetical access to undersea

cables by an intelligence agency would be difficult or impossible compared to access to unencrypted communications.

[17] My Testimony summarizes the detailed discussion in Chapter 3 of the systemic safeguards in foreign intelligence. Part A provides historical background for the system of US foreign intelligence law, as well as the fundamental safeguards built into the US system of constitutional democracy under the rule of law. Part B describes the systemic statutory safeguards governing foreign intelligence surveillance. Part C describes the oversight mechanisms, and Part D the transparency mechanisms. Part E describes administrative safeguards that are significant in practice and supplement the legislative safeguards. My Testimony also summarizes how these safeguards apply in a case study, set forth in Chapter 5, on how the Foreign Intelligence Surveillance Court has supplied these safeguards in practice.

[18] Overall, in my view, there has been an impressive system of oversight for US foreign intelligence practices. As discussed in Chapter 6, I agree with the conclusion of a study led by privacy expert and Oxford Professor, Ian Brown, which found the US system has 'much clearer rules on the authorization and limits on the collection, use, sharing, and oversight of data relating to foreign nationals than the equivalent laws

of almost all EU Member States'. A central question of this case is whether the US has 'adequate' safeguards around surveillance information; my review of the safeguards matches that of Professor Brown's – the US system generally has clearer and more extensive rules than the equivalent laws in EU Member States. In addition, the case study on the Foreign Intelligence Surveillance Court shows how thoroughly those rules are implemented in practice in the US. There is no similar evidence, to the best of my knowledge, of anything like that level of protection in practice in the Member States."

Then he proceeds to deal with some general comments in relation to the US. He says: *"It is a fundamental assessment of 'adequacy' or 'essential equivalence' goes to whether the nation protects rights and freedoms under the rule of law. The US Constitution created a time-tested system of checks and balances among the three branches of government, in continuous operation since 1790. The judiciary is a separate branch of the US government, staffed by independent judges who exercise the power of judicial review. The US Constitution enumerates fundamental rights, which serve as a systemic check against abuse because judges can and do strike down government action as unconstitutional where appropriate.* 11:20

[20] For protection against government access to personal data, the Fourth Amendment to the US Constitution – which prohibits unreasonable searches of people's 'person, houses, papers, and effects' – plays a particularly important role. Foreign intelligence searches on a US person, or on a non-US person who is in the US, remain subject to the Fourth Amendment, because such searches must meet the overall Fourth Amendment test that they be 'reasonable'. These constitutional protections apply to searches conducted in the US (including on data transferred to the US). As discussed below, the judiciary plays a key role in overseeing surveillance conducted in the US and holding it to constitution standards.

11:21

[21] In addition to constitutional checks, major safeguards in the US system of foreign intelligence law are codified in a number of statutes. The democratically-elected branches in the US have authorized surveillance to protect national security. They also have responded to evidence of excessive surveillance with laws setting limits on surveillance powers.

[22] Most notably, in 1978, the US Congress passed the Foreign Intelligence Surveillance Act (FISA). The

first major changes to FISA took place in the USA PATRIOT Act, following the attacks of September 11, 2001. Along with many others, I argued that those changes swept too broadly. There have been numerous pro-privacy reforms since 2001. For instance, following the Snowden disclosures, Congress in the USA FREEDOM Act of 2015 strengthened important aspects of FISA, and ended bulk collection under Section 215 of the PATRIOT Act.

[23] Under FISA and Supreme Court law, judges retain their power to oversee all electronic surveillance conducted within the United States. A search is either (a) conducted in the criminal context, in which case a judge must approve a warrant showing probable cause of a crime; or (b) conducted in the foreign intelligence context, in which case the Foreign Intelligence Surveillance Court must authorize the surveillance pursuant to FISA and subject to the reasonableness requirements of the Fourth Amendment. These are the 11:22
principal ways that an electronic communication search is carried out lawfully within the US.

[24] This section addresses three systemic statutory safeguards the US has placed over foreign intelligence: 11:22
(1) the Foreign Intelligence Surveillance Court; (2) metadata collection under Section 215; and (3) communications collection under Section 702.

[25] Since passage of FISA, the Foreign Intelligence Surveillance Court (FISC) has played a central role in regulating US foreign intelligence. FISA grants the FISC exclusive jurisdiction to issue orders for all foreign-intelligence surveillance carried out in the US. These include orders for individual surveillance, as well as oversight of larger intelligence programs.

[26] Within the FISC, independent and high-quality judges with lifetime appointments to the federal bench gain access to top-secret information, and exercise constitutional authority in enforcing legal limits on intelligence activities. FISC judges are selected for service by the Chief Justice of the US Supreme Court, and supported by a staff of security-cleared attorneys with expertise in national security law.

[27] Recently, the FISC and the Obama Administrative declassified numerous FISC pleadings, orders, and related materials. To determine how the FISC has applied in practice the safeguards identified in this Testimony, I devote Chapter 5 to a detailed review of the declassified materials. I find the materials support the following conclusions:

The FISC today provides independent and effective oversight over US government surveillance, backed by thorough review proceedings and constitutional judicial

authority. The FISC's standard procedures subject government surveillance applications to careful review, and FISC decisions show the court requiring the government to withstand rounds of briefing, meetings, questions, and hearings. In its evaluations of proposed surveillance, the FISC focuses on government compliance with existing or similar prior FISC orders. In recent years, the number of surveillance applications the FISC modified or rejected has grown substantially, and the FISC has exercised its constitutional power to halt surveillance it determines is unlawful.

The FISC monitors compliance with its orders, and has enforced with significant sanctions in cases of non-compliance." 11:24

He elaborates on that: "*In recent years - he continues in the next heading - the FISC on its own initiative as well as new legislation have greatly increased transparency."* 11:24

And he says in the next heading: "*The FISC now receives and will continue to benefit from adversarial briefing by non-government parties in important cases."* 11:24

Then he proceeds in section 2, Judge, and, just to remind you, this is a summary over 40 pages of the remaining parts of the report which I think is why

Mr. Collins said he would open it pretty well in full.

He says at paragraph 28: "*The most dramatic change in US surveillance statutes since 2013 concerns reforms of Section 215 of the USA PATRIOT Act, which provided the government with broad powers to obtain 'documents and other tangible things.' After the September 11 attacks, Section 215 was used as a basis for collecting metadata on large numbers of phone calls made in the US.*

[29] The USA FREEDOM Act abolished bulk collection under Section 215 and two other similar statutory authorities. These limits on collection apply to both US and non-US persons. A far narrower authority now exists, based on individualized selectors associated with terrorism and judicial review of each proposed selector."

MS. JUSTICE COSTELLO: May I just ask you to remind me what's the code section for Section 215, is it 18 something or other? 11:25

MR. MURRAY: I thought it was *5*, Judge, but I will have that checked.

MS. JUSTICE COSTELLO: I just want to write them in so I can make sure that I don't, have consistency across the documents. Thank you, sorry. 11:26

MR. MURRAY: Judge, I just see footnote 33, in relation to section two one -- the abolition of bulk collection Section 215 refers to a narrower authority based on

individualised selectors. And that references Title 50 1861, but we'll get the precise reference because I know Mr. Collins was using those last week.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: Over the page then: "*Section 702 of FISA applies to collections that take place within the US, and only authorises access to communications of <u>targeted</u> individuals, for listed foreign intelligence purposes.* 11:26

The independent Privacy and Civil Liberties Oversight Board, after receiving classified briefings on Section 702, came to this conclusion: Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

[31] Chapter 3 on systemic safeguards for foreign intelligence and Chapter 5 on the FISC provide detail about the PRISM and Upstream programs under Section 702. Misunderstanding about the PRISM program traces to the original and since-revised Washington Post story, which stated that '[t]he

National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies' to extract a range of information. This statement was incorrect. In practice, PRISM operates under a judicially-approved and judicially-supervised directive, pursuant to which the government sends a request to a US-based provider for collection of targeted 'selectors', such as an e-mail address.

[32] There have also been concerns about Upstream as a mass collection program. In fact, the US government receives communications under both Upstream and PRISM based on targeted selectors, with actions under each program subject to FISC review. Concerning scale, a declassified FISC opinion found that over 90% of the Internet communications obtained by the NSA in 2011 under Section 702 actually resulted from PRISM, with less than 10% coming from Upstream. The US intelligence community now releases an annual Statistical Transparency Report, with the statistics subject to oversight from Congress, Inspector Generals, the FISC, and the Privacy and Civil Liberties Oversight Board, and others. For 2015, there were 94,368 'targets' under the Section 702 programs, each of whom was targeted based on a finding of foreign intelligence purpose. That is a tiny fraction of US, European, or global Internet users. Rather than having mass or unrestrained surveillance, the

documented statistics show the low likelihood of communications being acquired for ordinary citizens.

[33] I have testified previously that Section 702, in my view, is a reasonable response to changing technology, set forth in a statute that was debated publicly prior to its enactment. The now-declassified FISC materials, along with reports on Section 702 by the Privacy and Civil Liberties Oversight Board and the Review Group, show a far more targeted and legally-constrained set of actions under Section 702 than press accounts had initially suggested.

[34] In addition to codifying systemic safeguards, the US has established multiple review and oversight mechanisms related to foreign intelligence. Following the Snowden disclosures, I was one of five members of the Review Group on Intelligence and Communications Technology that President Obama created to conduct a comprehensive review of US surveillance programs. We received top-secret briefings and presented our report of over 300 pages to the President in December 2013. In January 2014, the Obama Administration informed us that 70 percent of our 46 recommendations had been adopted in letter or spirit, and others have been adopted since that time.

[35] Going forward, multiple institutions, each with access to classified information, exercise

oversight responsibilities over foreign intelligence activities."

And he then identifies: "*Executive agency inspectors general, Congressional oversight committees, the Privacy and Civil Liberties Oversight Board and privacy offices in the executive agencies."* 11:30

He then addresses what he describes as transparency safeguards: "*[36] The US system of foreign intelligence surveillance law has long had important transparency requirements, such as statistical reports about the number of court orders issued. Since 2013, there have been numerous changes in the direction of transparency, while recognizing the harm to national security that can result from disclosure of classified information, such as about the sources and methods of intelligence activity. The transparency safeguards complement oversight by the FISC and the other oversight mechanisms just discussed – transparency is appropriate where possible consistent with national security, and additional oversight is performed by judges and others with top-secret clearances where transparency is not appropriate.* 11:30

[37] As discussed in greater detail in the following chapters, transparency safeguards in the US include: 1. Reports on legal interpretations."

And he discusses provision in the Freedom Act which

included a new rule addressing the risk of secret law with the FISC having to release opinions which have a 'significant construction or interpretation of the provision of law', government transparency reports, company transparency reports, additional government transparency actions. 11:31

And then in section E the Executive Safeguards:

"*In 2013 the US Executive Branch has instituted multiple safeguards to supplement the legislative protections outlined above. My experience in the Review Group and more generally leads to my conclusion, detailed in Section VI(A) of Chapter 3, that these Executive Branch safeguards matter a great deal in practice.* 11:31

[39] Foremost among the new executive-branch safeguards is Presidential Policy Directive 28 (PPD-28), which mandates that US surveillance agencies make privacy integral to signals intelligence planning. PPD-28 requires that agencies prioritize alternative sources of information – such as diplomatic sources – over signals intelligence. Where surveillance is used, it must be 'as tailored as feasible', proceeding via selectors such as e-mail addresses whenever practicable. Bulk collection cannot be used except to detect and counter serious threats, such as terrorism, espionage, or nuclear proliferation. Data about EU

citizens cannot be disseminated unless the same could be done with comparable data about US persons. Although PPD-28 does not use terms from EU law such as 'necessary' and 'proportionate', prioritizing alternatives to surveillance and requiring tailored collection and use limits are examples of US law implementing specific safeguards to address these concerns.

[40] Additionally, recent agreements between the EU and US bind the US executive branch to safeguard EU citizens' personal data. The EU-US Umbrella Agreement protects personal data transferred to US agencies for law-enforcement purposes, restricting transfers and permissible uses, and providing EU residents with access and correction rights. The Privacy Shield contains commitments from the US government to act promptly and effectively to address EU data protection concerns – and subjects Privacy Shield performance to an annual review process. These commitments and reviews provide the EU and its DPAs an ongoing mechanism to protect personal data transferred to the US, including data processed for national security purposes.

11:33

In addition to foreign intelligence - he says in the context of the systemic safeguards in law enforcement - the US has established a system of safeguards protecting individuals in the context of criminal

investigations. As mentioned above, government collection of electronic communications in the US takes place primarily either under law enforcement or foreign intelligence legal authorities. For collection in the US, any other authority such as Executive Order 12,333 does not apply. This part of my Testimony outlines the systemic safeguards in place for collection in the US of electronic communications in criminal investigations.

[42] Reacting to the US colonial experience with English monarchs, the US Constitution sets forth multiple fundamental rights to check government overreach in criminal cases. These rights have resulted in multiple areas where the US is stricter than other countries, including many EU countries, in providing criminal procedure safeguards:

1. Strict Judicial Oversight. Independent judicial officers oversee applications for warrants to conduct searches and collect evidence. 'Probable cause', the requirement for granting a warrant to search, is a relatively strict requirement for digital searches.

2. Stricter Oversight for Interceptions. Telephone wiretaps and other real-time interception have even stricter requirements, such as successive rounds of agency review, minimization safeguards for non-targets, and requirements to exhaust other sources of

information.

The so-called 'exclusionary rule' bars evidence obtained through an illegal search from being used at criminal trials, while the 'fruit of the poisonous tree' doctrine further bars additional evidence derived from the illegal search. Officers who conduct illegal searches are subject to civil damages lawsuits.

4. Orders Permit Legal Challenges. US law requires court orders to clearly indicate the legal basis for a warrant or information request, permitting the recipient to determine whether there is a basis to challenge the order.

5. No Mandatory Data Retention. US law does not require data retention for Internet communications, such as e-mail. For telephone communications, US law requires limited retention of records needed to resolve billing disputes.

6. Strong encryption.

[43] In significant measure, the creation of the United States itself derived from an insistence on protecting the rights of individuals in the criminal justice system. Although it is a complex task to assess precisely where the US and EU provide stricter safeguards in criminal investigations, the US has

significant, and often constitutional, safeguards that often are lacking in the EU. In my view, a fair comparison of the adequacy of the two systems should carefully consider such additional factors."

And he then says: "*[44] Intelligence agencies necessarily often act in secret, to detect intelligence efforts from other countries and for compelling national security reasons. The US has developed multiple ways to ensure oversight by persons with access to classified information for the necessarily secret activities, and to create transparency in ways that do not compromise national security. In my view, the US system provides effective checks against abuse of secret surveillance powers. I agree with the team led by Oxford Professor Ian Brown, who after comparing US safeguards to other countries, concluded that 'the US now serves as a baseline for foreign intelligence standards', and that the legal framework for foreign intelligence collection in the US 'contains much clearer rules on the authorisation and limits on the collection, use, sharing and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States'. In addition, as shown in the detailed study of the Foreign Intelligence Surveillance Court, those rigorous legal standards are effectively implemented in practice, under the supervision of independent judges with access to top-secret information."*

He then moves from that, Judge, to the individual remedies in US privacy law in paragraph 45. In the US, he says:

11:36

"*An EU resident or other individual has multiple remedies available for violations of privacy. These individual remedies work in tandem with the systemic safeguards just discussed. For many issues involving secret surveillance by agencies, I believe systemic safeguards are often particularly effective. In the US, oversight bodies such as the FISC, the PCLOB, agency Inspectors General, the Senate and House Intelligence Committees, and the President's Review Group that I served on gain access to classified information. That access allows these overseers to detect privacy problems and take action to correct them. By contrast, there are reasons to be cautious about disclosing national security secrets to individuals or in open court, where the act of disclosure itself can pose new security risks.*

[46] The US system bolsters those systemic safeguards with a multi-pronged approach to individual remedies. I have sometimes encountered the view in the EU and elsewhere that the US lacks remedies generally for privacy violations, or that remedies are only available to US persons. That is not correct. As the lead author of the textbook for the International

Association of Privacy Professionals (IAPP) US private-sector privacy law exam, I wrote an overview of US privacy laws that apply to the private sector, including enforcement mechanisms, that on its own took nearly 200 pages and eleven chapters. Annex 1 to Chapter 7 of my Testimony also charts this combination of systemic safeguards and individual remedies to provide an overview of the US legal privacy regime in total, as complement to the detailed explanations provided of each aspect of that regime in Chapters 3, 4, and 7.

[47] The large quantity of US privacy laws sometimes leads to a different critique from the EU, that US remedies are 'fragmented' and may for that reason may not be adequate under EU standards. I hope that this explanation of US privacy remedies can demonstrate how the different pieces of US law fit together. The complexity of US law arises in part from its pro-enforcement legal culture, with the result that multiple privacy enforcers each may have the legal ability to bring an action. This division of authority can be beneficial for privacy protection, as it allows subject matter experts to enforce in their areas of expertise, allows multiple agencies to leverage their resources to police categories of activity on behalf of data subjects, and also allows private rights of action for individuals.

[48] To explain the US privacy enforcement system, I outline here the paths an aggrieved person in the US or EU may take in response to concerns regarding US privacy violations, as explained more fully in Chapter 7: Individual Remedies in US Privacy Law. First, I discuss individual judicial remedies against the US government, including the recently-finalized Privacy Shield and Umbrella Agreement, as well as the recently passed Judicial Redress Act. Next, I examine the civil and criminal remedies available where individuals, including government employees, violate wiretap and other surveillance rules under laws such as the Stored Communications Act, the Wiretap Act, and the Foreign Intelligence Surveillance Act. After that, I highlight three paths of non-judicial remedies individuals can take: The PCLOB, Congressional committees, and recourse to the US free press and privacy-protective non-governmental organizations. Next, I talk about individual remedies against US companies that improperly disclose information to the US government about customers. These causes of action against US companies can be brought both by individuals (US and non-US) as well as by US federal administrative agencies. I also examine remedies available under state law in the US and private rights of action, including enforcement by state Attorneys General. I also provide in this part an answer to some of the concerns raised in the Irish Data Protection

Commissioner's Affidavit in this case. Specifically, I respond to the Affidavit's concerns regarding fragmented remedies in US law, possible limitations on the availability of remedies, and concerns regarding the doctrine of standing under US law. This part explains how the overall US legal system addresses these concerns, and how specific reforms such as the Ombudsman mechanism in the Privacy Shield Framework affect these concerns.

[50] Part 3 concludes with a caveat – individual remedies are sometimes difficult to provide in the intelligence setting, because of the risk of revealing classified information to hostile actors. The desirability of individual remedies, in intelligence systems, thus depends on the advantages of providing an individual remedy against the risks that come from disclosing classified information. Put in the language of Article 8 of the European Convention of Human Rights, the desirability of individual remedies, in intelligence systems, depends on how implementation of the right is judged with the necessity in a democratic society of protecting other interests including national security and public safety."

And he then proceeds to deal, first of all, with US civil judicial remedies, qualifying individuals, he says: "*[52] Qualifying individuals, including EU persons, may bring civil suits against the US*

government for violations of law that can result in monetary damages and injunctions against ongoing illegal government programs or activities. Remedies of this sort exist under: The Judicial Redress Act; the EU-US Privacy Shield; the Umbrella Agreement; the Stored Communications Act (SCA); the Wiretap Act; and the Foreign Intelligence Surveillance Act (FISA).

[53] Taken together, the EU-US Privacy Shield, the Judicial Redress Act, and the Umbrella Agreement provide important individual legal remedies for EU persons who believe they have suffered privacy harms. The EU-US Privacy Shield created new remedies against the US government available to EU persons. The Privacy Shield creates an Ombudsman within the US Department of State who can hear complaints from EU data subjects related to US government actions. This Ombudsman operates independently from US national security services, and the protections apply to data transfers under Standard Contractual Clauses: The Ombudsman has the authority to review 'requests relating to national security access to data transmitted from the EU to the US pursuant to the Privacy Shield, standard contractual clauses [and] binding corporate rules (BCRs)'. The Privacy Shield also allows individuals to invoke, free of charge, an independent alternative dispute resolution body to handle complaints against US companies participating in the shield.

[54] Under the Judicial Redress Act of 2016, the US expressly extended the right to a civil action against a US governmental agency to obtain remedies with respect to the willful or intentional disclosure of covered records in violation of the Privacy Act or when a designated US governmental agency or component declines to amend an individual's record in response to an individual request. The Judicial Redress Act directly addresses a concern that had previously been expressed by EU officials: That EU citizens were not afforded protections under the Privacy Act. Although EU Member States have not to date finalized their participation under the Judicial Redress Act, my understanding is that the EU and US plan to do so.

[55] The Privacy Act allows US and qualifying non-US persons to sue a US federal agency for the improper handling of covered records; to obtain injunctions or monetary damages; and to review, copy, and request amendments to their records. An individual may sue under the Act when the agency willfully or intentionally fails to comply with the Privacy Act in a way that has 'an adverse impact on [the] individual'. An individual also qualifies to sue if an agency determines not to amend the individual's record in response to a request, fails to provide appropriate review based on a request, or refuses to comply with a request. As discussed further in Chapter 7, there are exceptions to the applicability of the

Privacy Act.

[56] The Umbrella Agreement provides remedies for EU data subjects whose data is transferred to US law enforcement authorities. Individuals can access this personal information, subject to certain restrictions equivalent to what US citizens face, and EU data subjects may request correction or rectification. If a law enforcement agency denies an access or rectification request, it must explain its basis for denial 'without undue delay'. The EU data subject may, in accordance with the applicable US legal framework, seek administrative and judicial review of such denial, or seek judicial review of any alleged willful or intentional unlawful disclosures of the personal information. If appropriate, the court may require access or rectification, and, with respect to other violations, may award compensatory damages. These abilities are granted in part by the Judicial Redress Act, passage of which was due in part to a requirement of the Umbrella Agreement.

[57] The SCA provides a remedy for both US and EU citizens for unlawful access to or use of stored communications data by an unauthorized individual government actor or US agency. The rules for lawfully accessing stored data turn on the type of data. For the content of communications, such as e-mail, an independent judge applies the Fourth Amendment's

constitutional rule, requiring probable cause of a crime. Access to metadata requires the government to certify to a judge that the information likely to be obtained is relevant to an ongoing criminal investigation. A company can voluntarily disclose basic subscriber information (BSI), and the government can compel access to BSI through other judicial process such as a grand jury subpoena. A data subject whose data is unlawfully accessed can bring suit under the SCA against individual officers and US agencies if the violation was 'willful'. Successful suits against individual officers can result in money damages of at least $1,000 USD, equitable or declaratory relief, attorney's fees, legal fees, and/or punitive damages. Any government employee found to have willfully or intentionally violated the Act can also be subject to discipline. Suits against a US agency may result in actual damages or $10,000 USD, whichever is greater, plus litigation costs.

11:45

[58] The Wiretap Act provides a similar right of action for individuals against the US government. Under the Wiretap Act, the government must show both probable cause and a number of other standards, including a sufficiently serious crime and an explanation of why the information cannot be obtained by other means. Wiretaps are only authorized for a specific and limited time, must minimize the amount of non-relevant information intercepted, and any surveillance conducted

outside those bounds is considered unlawful. Applications under the Wiretap Act must also be approved at the highest levels of the DOJ before they can be submitted to a judge for review. Like the SCA, the Wiretap Act also allows aggrieved individuals, including EU persons, to file suit when their communications have been unlawfully intercepted by the US government. If an individual has 'intentionally' violated the Act, a data subject may obtain 'appropriate relief', including an injunction of any ongoing wiretaps, monetary damages, and punitive damages.

[59] FISA also provides individual remedies for data subjects against the unlawful acts of individual government officers. Any surveillance of a data subject performed without statutory or Presidential authorization, misuse of surveillance information, or unlawful disclosure of surveillance information by an individual officer makes that officer liable to suit in US court. Data subjects who successfully sue such officers can receive actual damages greater than or equal to $1,000 USD, statutory damages of $100 USD per day of unlawful surveillance, and potential additional punitive damages and attorney's fees if appropriate. An EU data subject may sue under FISA as long as he or she is not a foreign power or an agent of a foreign power."

Then, Judge, there are, there is consideration of US criminal judicial remedies and outlined there are a number of offences that can be prosecuted by the appropriate prosecuting authorities.

11:47

Over the page there's consideration of what are described as non-judicial individual remedies and these include reference to the PCLOB, the free press, non-government privacy organisations and I think Congressional committees.

11:47

Then if you turn the over the page to 124 he moves back to additional US privacy remedies under federal law and here he explains that there is:

11:47

"*Redress for privacy harms from private companies, such as service providers of web mail and social networks, that improperly disclose information to the US government. These service providers have strong incentives to follow the law and their own stated company policies, as violations can result in enforcement actions, costly lawsuits and significant reputational harm to the business. The SCA and Wiretap Act in particular allow for suits against private companies that unlawfully share customer data, which can result in costly damage awards. These risks shape what information companies are willing to share with the government and under what process.*"

He explains then, Judge, at paragraph 67 that there are various federal administrative agencies that are regulators and enforcers of this, including the Federal Trade Commission and the Federal Communications Commission. 11:48

He then refers, Judge, over the page, 125, to *"Enforcement Under State Law and Private Rights of Action"*. And he says that: 11:48

"*State law and state Attorneys General provide additional privacy protections for consumers both in and outside the US. As discussed by Professor Danielle Citron, these Attorneys General have emerged as key privacy enforcers in the US. Chapter 7 offers a detailed case study of California law and enforcement to illustrate this point. The prevalence of plaintiffs' lawyers and private rights of action, along with the significant damages assessed in these actions, have increased the incentive for companies to comply strictly with applicable law.*"

As he records that state attorneys are permitted to investigate petitions from individuals, including EU persons. 11:49

Then in Section 5 he addresses concerns in the Data Protection Commissioner's affidavit:

"The Irish Data Protection Commissioner has filed an affidavit in this case summarising findings regarding. US remedies. The following briefly cites relevant DPC Affidavit statements, then shows where the Court may find discussion of these issues in my Testimony.

[71] The DPC Affidavit states a finding that 'the remedies provided by US law are fragmented, and subject to limitations that impact on their effectiveness to a material extent'. Chapter 7 acknowledges that US remedies can appear fragmented, and explains how the numerous ways in which US law permits individuals to remedy privacy violations fit together. The complexity of US law can in part be traced to the fact that more than one source of enforcement can exist for any given privacy issue. This division of authority can be beneficial, as it permits private rights of action for individuals, while allowing multiple agencies to police categories of activity on behalf of data subjects.

[72] The DPC Affidavit states that US remedies 'arise only in particular factual circumstances', such as intentional violations, and are 'not sufficiently broad in scope to guarantee a remedy in every situation in which there has been an interference with personal data'. As discussed in Chapter 7, Sections I, III(A), some US remedies – as with criminal statutes generally – require intent to show a violation. The scope of

individual US remedies is discussed throughout Chapters 7 and 8.

[73] The DPC has suggested, as a positive development, that US remedies may be reassessed 'in the context of' the Privacy Shield Ombudsman mechanism. Chapter 7, Section I(A)(1) discusses how EU residents can now lodge complaints with an independent Ombudsman regarding US government collection of data – regardless of whether they have been informed that personal data has been collected, and without needing to show intent or actual harm. Chapter 7 also discusses redress avenues against companies that violate privacy rights, charting remedies available specifically to EU citizens.

[74] The DPC Affidavit states a finding that 'the 'standing' admissibility requirements of the US federal courts operate as a constraint on all forms of relief available'. Chapter 7, Section V provides details about US case developments since ***Clapper****, mentioned in the DPC's Draft Decision. Chapter 7 more generally discusses avenues US law offers individuals to remedy privacy violations, including: Judicial remedies; non-judicial remedies such as the PCLOB and the free press; administrative-agency remedies via agencies such as the Federal Trade Commission and Federal Communications Commission; the Privacy Shield Ombudsman. The doctrine*

of standing potentially affects judicial remedies, and Chapter 8 discusses the reasons courts in the US and the EU have been cautious about disclosing national security secrets in open court. Remedies such as the Ombudsman, the PCLOB, and the FTC are not subject to such standing limitations.

[75] The DPC's Affidavit also quotes a number of findings about US surveillance law set forth in EU Commission reports published on November 27, 2013. These Commission reports predate the Review Group's reform recommendations, as well as practically all of the post-Snowden reforms to US foreign-intelligence practice my Report discusses. I would generally refer the Court to Chapters 3 (Systemic Safeguards for Foreign Intelligence), 5 (the Foreign Intelligence Surveillance Court), 6 (the Oxford Assessment of Post-Snowden US Surveillance Law), and 7 (US Individual Remedies) for a picture of US foreign intelligence practice as it stands today." 11:52

And then he says: "*Conclusions on individual remedies, with a caveat.*

[76] Part 3 of this Summary of Testimony has set forth the multiple ways that individuals, including EU citizens, can achieve remedies in the US for privacy violations. Before turning to Part 4, I briefly discuss a caveat about individual remedies in the

intelligence setting. The desirability of individual remedies, in intelligence systems, must be weighed against the risks that come from disclosing classified information. In the terms used in Article 8 of the European Convention on Human Rights, the availability of the individual right to privacy is assessed against the necessity in a democratic society of the interests of national security and public safety.

[77] The field of cyber security provides an analogy for deciding what types of remedies individuals should have about processing of their information by surveillance agencies. Many of us today are at least somewhat familiar with three types of cyber security precautions: (1) do not click on links in emails, because they might be phishing attacks; (2) update your anti-virus software; and (3) have a good firewall. The idea I am suggesting is simple but I believe helpful – be cautious about creating a new vector of attack, such as individual remedies, into a protected system.

[78] A simple example illustrates the sort of harm to national security that could result from individuals' direct access to their data held by an intelligence agency. Suppose a hostile actor, such as a foreign intelligence service, wants to probe the NSA or a Member State intelligence agency. The hostile actor may have Alice use a text service, Bob an e-mail service, and Carlos a chat service. They then file

access requests, and only Bob has a file. If so, then the hostile actor has learned something valuable – the e-mail service is under surveillance, but the text and chat services appear not to be. In this example, the individual remedies become a form of cyber attack – the hostile actor can probe the agency's secrets, and learn its sources and methods.

[79] Chapter 8, on Hostile Actors and National Security Considerations, thus explains ways that a hostile intelligence agency or other advanced persistent threat could use individual remedies as a form of cyber attack. It also points out that attacks against intelligence agencies are not hypothetical – they occur every day by the most capable adversaries in the world. In short,
restricted access to an intelligence agency's secrets can be seen as a security feature, as well as being a privacy bug.

11:54

The chapter develops an important related point."

MS. JUSTICE COSTELLO: Sorry, what does he mean by a privacy bug there, the last word?

MR. MURRAY: (Short pause) hmmm.

MS. JUSTICE COSTELLO: Well, I suppose we can ask him in due course. 11:54

MR. MURRAY: I'm not entirely certain, Judge, but I think we'll have the pleasure of Prof. Swire next week, so I'll move that up the list of

cross-examination questions.

"*[80] The Chapter develops an important, related point – both European and US courts have already created doctrines to prevent this sort of attack. In the US, courts in certain instances recognize what is called the 'state secrets doctrine', so that judges (while maintaining overall supervision of a case) take care not to let individual litigation become a route of attack on national security secrets. Similar judicial decisions appear to be the norm in Europe, with judges protecting against disclosure or use in open proceedings of national security information. In other words, established law recognizes limits on individual remedies in the foreign intelligence area.*

[81] As a lawyer from the US, I do not attempt to state as an expert how these considerations about hostile actor attacks would be judged under EU law. I do offer some observations, however, based on my previous experience with EU law. As discussed in Chapter 2, I worked extensively in the 1990's on the EU right to access, including leading a US delegation to six EU countries to research how the right to access was interpreted in practice. Article 12 of Directive 95/46/EC states the right to access in broad terms, without specifying exceptions. Nonetheless, our research discovered literally dozens of exceptions in practice.

[82] This experience informs my views about the applicability of Article 8 of the European Convention on Human Rights, and Articles 7, 8, and 47 of the EU Charter of Fundamental Rights. As just discussed, Article 8 of the Convention evaluates the availability of an individual right to privacy against the necessity in a democratic society of the interests of national security and public safety. The EU and US decisions limiting disclosures of national security secrets, just discussed, reflect judicial assessment of how to protect both privacy and national security.

[83] In contrast to Article 8 of the Convention, the right to private and family life in Article 7 of the Charter and the right to data protection in Article 8 of the Charter do not state that the rights have derogations for national security, public safety, or other reasons. It would be surprising to me, however, if Articles 7 and 8 were understood to have no derogations, for consideration of national security and other compelling rights and interests. Similarly, Article 47 of the Charter states, without derogations, that '[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article'. It would appear logical to me that EU judges would consider the necessity of national security, public

safety, and other public interest factors in determining the scope of individual remedies under Article 47.

[84] In summary overall on individual remedies, Part 3 of this Chapter and Chapter 7 describe the numerous individual remedies available in the US for privacy violations, including for violations of the privacy of EU citizens. These individual remedies exist in addition to the much improved set of systemic safeguards that exist in the US due to reforms since 2001, and especially since 2013. In discussing individual remedies, I have added a caveat about the scope of individual remedies, in intelligence systems, due to the risks that come from disclosing classified information.

[85] I now turn to Part 4, on other considerations. The combination of systemic safeguards, individual remedies, and other considerations should inform any assessment of the adequacy of protections for data transfer from the EU to the US."

Then he proceeds to address in Part 4 what he describes as the potential breadth of the decision and assessing the adequacy of protections for transfers to the US. 11:58

"*Part 4 of this summary of testimony, he says, addresses five considerations:*

1. The broad effect under US law of a finding that protections against excessive surveillance are inadequate;

2. The broad effect for transborder transfers to other countries of such a finding, including for the BRIC countries; 11:58

3. The possible effect of an inadequacy finding concerning standard contractual clauses for other lawful mechanisms for transfer of data to countries outside the EU; 11:58

4. The potentially large negative effects on EU economic well-being from such a finding as stated by EU institutions and Member States, and required under international trade law; 11:58

5. The potentially large negative effects on EU national court and public safety from such a finding as stated by EU institutions, and contrary to NATO and the goal of protecting minimal security."

MS. JUSTICE COSTELLO: I think that's mutual. 11:59

MR. MURRAY: Sorry, excuse, mutual security. So he then addresses those. He starts off with the broad US definition of service provider affected by a ruling.

"*[87] This proceeding would be simpler in certain respects if the effects of an adequacy finding applied only to one or a relatively few companies. As discussed in Chapter 9, however, the relevant US law applies broadly. Any assertion that Section 702 would*

apply only to a narrow set of companies such as Facebook is inaccurate.

[88] Section 702 applies to data collection from 'electronic communications service providers', a term that is defined broadly under US law. US courts have interpreted the relevant definitions to include any company that provides its employees with corporate e-mail or similar ability to send and receive electronic communications. A finding of inadequate protection that applies to Section 702 would thus apply to almost any company with operations in both the EU and US. There is no exception or statutory interpretation that would narrow the potential applicability of a finding of inadequacy with respect to Section 702. To have that impression would not account for the breadth of such a decision.

[89] The EU legal regime, he says, as it applies to consent in the employee context means that the broad application of Section 702 may have a particularly strong effect on human resources activities such as internal corporate communications, managing employees, or payroll. EU data protection authorities have been skeptical that individual employees can provide voluntary consent to transfers of their personal data outside of the EU. Companies operating in the EU therefore may face significant challenges in obtaining effective consent from an EU employee to

transfer of their personal data to other countries, including the US. Thus, if there is a finding of inadequacy of protection in the US for Standard Contractual Clauses, individual consent in the employment context may not provide a practical alternative basis for transfers. 12:00

He continues then, Judge:

"*II. The US Has Stronger Systemic Safeguards than the BRIC Countries*

90. I next make some basic comparisons of the surveillance safeguards in the US compared to the important 'BRIC' countries – Brazil, Russia, India, and China. The comparison is relevant due to the nature of the inquiry about US adequacy – when personal data is transferred from the EU to the US, are there adequate safeguards against surveillance by the US government? My Testimony has provided details about the many systemic safeguards and individual remedies that are in place against excessive national security surveillance for data that is transferred to the US.

91. The basic point is simple – suppose that safeguards against surveillance in the BRIC countries are weaker than safeguards in the US. If the US is found inadequate, then logically it would appear that the safeguards in countries with weaker safeguards are also

inadequate. Put another way, if the US safeguards are found inadequate, then it would appear that transfers of personal data would have adequate protection only for countries that have stronger safeguards than the US."

He then, Judge - I think what he's just said there expresses the point - he details that from paragraphs 92 to 95. And I think at paragraph 96, having outlined the systems in those jurisdictions, his conclusion is this, he says: 12:02

"*The four BRIC countries are large and important nations and trading partners of the EU. All have extensive surveillance activities with less transparency and oversight, and fewer overall systemic safeguards and individual remedies, than the US.*

97. The relative lack of safeguards is noteworthy for at least two reasons. First, I have encountered the view that transfers from the EU to the US should be prohibited, due to US surveillance laws, while simultaneously expressing the view that transfers from the EU to other countries, such as China, would be permitted. This reference to China led me to examine the implications of the Chinese safeguards against surveillance, which are less extensive than safeguards in the US.

98. Second, my experience in global data protection law leads me to the conclusion that the relative lack of safeguards in the BRIC countries holds true for the preponderance of other countries outside of the EU. The role of the US as the 'benchmark' for surveillance safeguards, and the relative lack of safeguards in most non-EU countries, has important implications: If the US is held to lack adequate protections against surveillance, then logically there would be lack of adequacy in the BRIC countries and numerous other countries. Only countries whose safeguards are demonstrably stronger than those in the US would appear to have a lawful basis to receive personal data from the EU. The logical import of this conclusion apparently would remove the lawful basis for substantial portions of transborder data flows from the EU."

He then, in section III, explains his view that an inadequacy finding for SCCs may have implications for 12:03
other lawful bases for data transfers. And at paragraph 99 he says this:

"*The current proceeding specifically concerns whether Standard Contract Clauses (SCCs) provide adequate protection, with reference to US surveillance practices. The Draft Decision of the Data Protection Commissioner said that she considered herself 'bound by the judgment' in the 2015 Schrems case to engage in the*

current legal proceedings. I understand this statement as the Commissioner seeing a link between the legal treatment of one basis for legal transfer (the Safe Harbor) and another basis for legal transfer (SCCs). Should a Court agree with that link, then there is a possibility that a judgment in the instant proceeding will have implications for other bases for legal transfer."

He says then at paragraph 100: 12:04

"*There are multiple ways that a legal finding about one legal basis for transfer may or may not be relevant to a legal finding about a different legal basis. To begin, I understand the instant proceeding as an opportunity to develop a much more detailed factual record than was before the CJEU in the 2015 Schrems case. My Testimony sets forth numerous aspects of US law and practice that were not in the record in the 2015 case. As discussed throughout my Testimony, there are strong reasons to conclude that the system of safeguards in the US for foreign intelligence investigations is stricter and more effective in practice than those in EU countries. The detailed record before the Court in this proceeding thus illustrates how a judicial finding about adequacy under one lawful basis of transfer (Safe Harbor) can be consistent with a different judicial finding about another lawful basis of transfer (SCCs).*"

And he then explains at paragraph 101 how a finding of inadequacy could carry over to other mechanisms of transfer. And at paragraph 104 he expresses a conclusion that he makes no finding about whether inadequacy for SCCs would entail a finding of inadequacy for Privacy Shield or BCRs.

"*The discussion here does support the possibility that an inadequacy finding for SCCs may have implications for other lawful bases for data transfers. In the balance of this Testimony, I refer to that broader possibility as a 'categorical finding of inadequacy' – a finding of inadequacy that would apply not only to SCCs but also to Privacy Shield and BCRs. If an inadequacy finding applied only to SCCs, then the effects of the finding may be limited, especially if the opportunity exists to interpret or update Privacy Shield and BCRs for the specific use cases where SCCs have been most helpful to date. If a categorical finding of inadequacy were to occur, however, it would appear to have significant implications for the overall EU/US relationship, affecting the foreign relations, national security, economic, and other interests of the Member States and the EU itself.*" 12:05 12:06

Then he says he's going to turn to how this affects the economic well-being of the EU Member States. So he says at 105:

"*My view is that there would be large economic effects from a categorical finding that the US lacks adequacy due to its surveillance regime. The development of a detailed record in the current proceeding, in my view, provides an opportunity to set forth those economic effects, along with my extensive comments about the nature of the adequacy of the systemic surveillance safeguards themselves.*

106. I do not undertake a statistical analysis of the magnitude of the potential economic effects. Instead, my comments are based on my overall experiences in the field. In considering the economic effects, I briefly discuss EU statements about the importance of the trans-Atlantic economic relationship, before examining international trade considerations."

He then addresses European Union statements about the importance of the transatlantic economic relationship 12:07
and he quotes a number of those. Over the page, Judge, he addresses trade agreements, including the general agreement in trade and services. He says there's important provisions in international trade treaties that support privacy of protections. 12:07

"*In my opinion, a categorical finding of inadequacy of US surveillance safeguards, and blockage of data transfers to the US, would create a significant*

possibility of a treaty violation."

And he explains at paragraph 111:

"*As is widely understood, the general approach under the WTO and the GATT is to support free trade and suppress protectionist measures. For that reason, a legal rule that prevents data from leaving a jurisdiction can pose a free trade difficulty – what is the lawful basis for treating transfers to a different country such as the US differently than data sharing within a country?*

112. For privacy, the usual answer is that the General Agreement on Trade in Services (GATS) has a specific privacy exception. To provide more scope for nations to enact data protection laws, Article IV of the GATS states:

'Nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures ... (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'.

This language provides a significant legal defense against the claim that a data protection regime violates GATS or the free trade regime more generally.

113. The data protection exception is limited, however. Article XIV also states the exception is subject 'to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.'

114. There is a factual question as to what constitutes 'unjustifiable discrimination between countries where like conditions prevail.' In my view, however, this GATS language provides an additional reason to consider how the safeguards in the US compare to both the EU and to other nations, such as the BRIC countries. As discussed in Chapter 6, the Oxford team's finding that the US is the 'benchmark' for such safeguards raises a difficulty under the GATS when EU Member States have less thorough safeguards. In addition, the concern about 'unjustifiable discrimination' would appear to apply if transfers were allowed to the BRIC or other countries but not to the US.

115. A categorical finding of inadequacy of US surveillance safeguards thus raises the risk of significant economic effects because of the elimination

of lawful transfers, which according to EU institutions are vitally important, and also because of the sanctions that may result from treaty violation under the GATS."

12:10

He then continues, Judge, this, as he describes it, more detailed factual record than was before the CJEU in **Schrems** at paragraph 116:

"*As is true for economic well-being, European institutions have strongly supported the EU/US relationship in the areas of national security, law enforcement, and information sharing for intelligence purposes. The EU Commission has stated: 'The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.' 192 Data flows 'are an important and necessary element' of this alliance, not only for economic reasons, but also as 'a crucial component of EU-US co-operation in the law enforcement field.' Data flows are also critical to 'the cooperation between Member States and the US in the field of national security'.*"

And he then elaborates upon examples of that information sharing. And if you go over to paragraph 119, Judge, I think his conclusion is in that and the following paragraph:

"*Information sharing for national security and public safety reasons is important in countering terrorist attacks of the sort that have struck Brussels, Paris, and elsewhere in the recent past. Our Review Group report discussed in detail why information sharing about individuals is especially important to counter terrorist threats. Today, both ordinary citizens and terrorists use largely the same devices, software, and computer networks, so surveillance of terrorism suspects often takes place on networks used by ordinary citizens. By contrast, during the Cold War, the most important threats came from nation states such as the Soviet Union, with a far lower likelihood of monitoring the communications of ordinary citizens. This convergence of communication systems used by terrorist suspects and other persons is an important factor, in my view, of what is 'necessary in a democratic society'...*

120. In sum, this discussion shows that a categorical finding of inadequacy would create substantial risks for national security and public safety, be contrary to the clear policies of EU institutions, and also raise issues for Member State treaty obligations. In a period marked by highly visible terrorist attacks within the EU, disruption of information sharing also raises the risk that future terrorist attacks will not be prevented."

Then at paragraph 121 he summarises what he's said in the preceding 40 pages. He says:

"*This Summary of Testimony explains that the combination of systemic safeguards and individual remedies in the US, in my view, are clearly effective and 'adequate' in safeguarding the personal data of non-US persons. Moreover, the Court of Justice of the European Union (CJEU) has announced a legal standard of 'essential equivalence' for transfers of personal data to third countries such as the US. Based on my comprehensive review of US law and practice, and my years of experience in EU data protection law, my conclusion is that overall intelligence-related safeguards for personal data held in the US are greater than in the EU. Even more clearly, the US safeguards are at least 'essentially equivalent' to EU safeguards. I therefore do not see a basis in law or fact for a conclusion that the US lacks adequate protections, due to its intelligence activities, for personal data transferred to the US from the EU.*

122. This Summary of Testimony discusses the potential breadth of a decision in this proceeding, and makes observations relevant to assessing the adequacy of protections for data transfers to the US. I examine issues in this proceeding under Article 8 of the European Convention of Human Rights... Article 8

provides that '[e]veryone has the right to his private and family life.' It also states: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' I address similar considerations under the Charter's Article 7... Article 8... and Article 47...

123. In terms of Article 8 of the Convention, in my view based on two decades of experience in US and international privacy and surveillance laws and practices, the systemic safeguards and individual remedies in the US in combination result in necessary actions that are taken 'in accordance with law.' In light of those safeguards and individual remedies available to EU citizens in the US, I respectfully believe and assert that continued transfers of personal data under Standard Contract Clauses are 'necessary in a democratic society' to protect vital interests of the EU, including national security, public safety, and economic well-being."

Now, much of that report - and indeed some of the passages I've just opened to you come close to saying

this in terms - appear to be directed to a complaint which is a recurring complaint that Facebook make in their affidavits - and we'll see this later - that in **Schrems** the Court of Justice did not have an adequate factual record before it. Facebook, it should be said, were clearly aware of the **Schrems** case when it was before the courts here; they could've, but never applied to be joined as a party to it. But they do make the complaint vociferously and often that the record of evidence which was before the Court of Justice was inadequate and there are complaints made - and again we'll see this in some of the affidavits - that the Court of Justice proceeded on an inadequate evidential basis and, in some places it appears to be suggested, an incorrect one. 12:14

Much of this seems to be directed, and *properly* directed, towards the assessment that the Court of Justice will ultimately conduct if the court determines that it's appropriate to refer the matter. And actually, not all that much of it, in our respectful submission, addresses what *we* submit to be the core issue around the adequacy of the legal remedies. 12:15

But there is one chapter in the report which addresses the legal remedies, Judge - and Mr. Collins had, I think, agreed with Mr. Gallagher and indicated to you last week that he would open this, together with the introduction - and that's chapter seven. So, Judge, if 12:15

I can ask you to go forward a good deal in the report to the page that has 7-1 at the bottom.

MS. JUSTICE COSTELLO: Yes, I have that. Thankfully, I've got tabs.

MR. MURRAY: I see. Very good, okay. So I think it's fair to say that the first number of pages are a re-summary of the summary which we have already said and it outlines what he proposes to do in this chapter. And I'm going to ask you to go, that being the case, to page 7-4, where he considers the US civil judicial remedies. 12:15 12:16

He explains in paragraph 13 that civil suits are possible in certain circumstances, remedies exist. In paragraph 14 then he moves on to the specifics. He starts by saying: 12:16

"*The Judicial Redress Act, the EU-US Privacy Shield, and the Data Protection and Privacy Agreement (i.e., the Umbrella Agreement) combine to provide new individual legal remedies for EU persons who believe they have suffered privacy harms, in addition to those specified by the Standard Contractual Clauses (SCCs) themselves.*

15. Under the Judicial Redress Act, the US expressly extended the right to a civil action against a US governmental agency to obtain remedies with respect to the willful or intentional disclosure of covered

records in violation of the Privacy Act to qualified individuals. The Judicial Redress Act also extends the right to a civil action against a designated US governmental agency or component when that agency or component declines to amend the record in response to a qualifying individual's request. A qualifying individual is one who has been subject to improper response to a request from a US agency. The Act allows US and qualifying non-US persons to sue a US federal agency for the improper handling of their data; to obtain injunctions or monetary damages; and to review, copy, and request amendments to their data. In contrast to some of the statutes discussed below, these suits are brought against the agency itself rather than against an individual actor within the agency.

16. Prior to the passage of the Judicial Redress Act in 2016, an action under the Privacy Act could be brought only by 'US persons', who are US citizens or non-citizen permanent residents. Under the Judicial Redress Act, non-US persons may bring a cause of action listed under the Privacy Act if the US Attorney General, in consultation with the Secretaries of State, Treasury, and Homeland Security, designates that the non-US person's country of citizenship 'has entered into an agreement with the United States that provides for appropriate privacy protections' and that the country permits the transfer of personal data for commercial purposes to the US. Although EU member

states have not to date been individually identified as required under the Judicial Redress Act, my understanding is that the EU and US plan to finalise that process."

And you'll have heard that has been advanced since the report, Judge.

"*17. Under the EU/US Privacy Shield, the US has created new remedies against the US government available to EU persons. For complaints concerning US government actions, EU data subjects can lodge a complaint with an Ombudsman within the Department of State. The Ombudsman will respond to individuals who file complaints related to the Privacy Shield and inform them whether or not the laws relevant to their situation have been violated. Importantly, this Ombudsman is independent from US national security services. The Ombudsman can be used to process 'requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs) [and] binding corporate rules (BCRs).' Indeed, the US and the EU Commission have made clear that the Ombudsman mechanism 'is not Privacy Shield specific' and 'covers all complaints relating to all personal data and all types of commercial transfers from the EU to companies in the US.' Any written commitments from the Ombudsman in response to individual inquiries will*

also be published in the US Federal Register...

18. Individuals in the EU have multiple methods for redress against companies, rather than the US government, for privacy complaints. First, individuals can invoke, free of charge, an independent alternative dispute resolution (ADR) body to handle any complaints against US Privacy Shield companies. Information on and a link to the ADR must be provided on the company's website, and the ADR must be able to 'impose effective remedies and sanctions' in response to valid complaints. Second, individuals can file a complaint with an EU Data Protection Authority (DPA), which have their existing enforcement powers today under national law and will gain additional enforcement powers when the General Data Protection Regulation goes into effect... The Privacy Shield also allows US companies to opt for using an EU DPA as its independent recourse mechanism, and DPA oversight is mandatory when a company handles personnel data transfers from the EU to the US. Individual complaints to the DPA can result in advice delivered to the company and made public to the extent possible. Third, if the company fails to comply with the DPA's advice within 25 days, the DPA may refer the issue to the Federal Trade Commission (FTC) for enforcement. Under Section 5 of the FTC Act, the Commission can bring an enforcement action for a 'deceptive' practice if the company promises to comply with Privacy Shield but fails to do so. Fourth, if the

company fails to comply with the DPA's advice within 25 days, the DPA may also refer the matter to the Department of Commerce to determine if the company's non-compliance should result in removal from the Privacy Shield List.

19. The Umbrella Agreement provides remedies for EU citizens whose data is transferred to US law enforcement authorities. Any individual will be entitled to access their personal information – subject to certain conditions, given the law enforcement context – and request corrections if it is inaccurate. Similarly, individuals are entitled to seek correction or rectification of personal information that they assert is either inaccurate or improperly processed. If the petition for access, correction, or rectification is denied or restricted, the authority must provide an explanation of the basis for its denial 'without undue delay.' The Agreement provides that, if the US authority denies a request, the EU citizen may seek judicial review... An EU citizen may also petition for judicial review of alleged willful or intentional unlawful disclosure of his or her information, for which the court may award compensatory damages where appropriate. The US passed the Judicial Redress Act in part to fulfil this requirement of the Umbrella Agreement.

20. Standard Contractual Clauses, when implemented by a

US company, also offer individual privacy remedies. Under Commission Decision C(2004)5721, '[e]ach party shall be liable to the other parties for damages it causes by any breach of these clauses' and to 'data subjects for damages it causes by any breach of third party rights' under the SCCs. Data subjects are also specifically empowered to enforce the SCCs as a third party beneficiary against the data importer or the data exporter with regards to that individual's personal data. The importer and exporter both agree to allow such suit to be adjudicated in the data exporter's country of establishment.

21. Where a data subject alleges that the data importer has breached the SCCs, the subject is required to request that the data exporter enforce the data subject's rights against the importer. If the data exporter does not take such action within a reasonable period (typically one month) then the data subject may proceed to enforce his or her rights against the data importer directly. The data subject may also file suit against the data exporter in this case for failure 'to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations'..."

Then he deals with the Electronic Communications Privacy Act and the SCA. And he says that it:

"... *creates an individual right of action for*

individual data subjects, including EU citizens. The Stored Communications Act (SCA) governs access to stored communications data. It provides individual remedies for data subjects whose stored communications data that has been unlawfully accessed or used by either an individual government actor or US agency as a private third party actor which accesses a network without authorization. The protections for access to an individual's stored data are not limited by citizenship and all remedies available under the Act are likewise available to EU citizens...

23. Under ECPA, different standards apply for judicial orders for US government access, depending on the type of data requested. The strictest of the applicable standards applies the Fourth Amendment's constitutional rule of probable cause... determined by an independent judge. That probable cause standard now applies to the stored content of electronic communications, including e-mail. Easier access is permitted to what historically has been called 'pen register' and 'trap and trace' information, the metadata about the communication. To access this dialling, routing, addressing, and signaling information, the government must certify to the judge that that the information likely to be obtained is relevant to an ongoing criminal investigation. Fourth, basic subscriber information... can be voluntarily disclosed to the government upon request, or can be obtained through

other judicial process...

24. For violations of these rules, the data subject may bring a civil suit against the agency and/or the individual, even if the data subject is not a US citizen. Suits against both individual officers and US agencies must demonstrate that the violation of ECPA was 'willful.' If a suit against an individual officer succeeds, the data subject may receive money damages of at least US$1,000, equitable or declaratory relief, reasonable attorney's fees, reimbursement of legal fees, and/or punitive damages. The government employee found to have willfully or intentionally violated ECPA may also be subject to discipline... Suits against a US agency may result in actual damages or $10,000, whichever is greater, plus litigation costs."

He then deals with the Wire Tap Act. It:

"... *Act creates an individual right of action against unlawful government action. The rules for getting a wiretap – a real-time interception of a data subject's communications – are even stricter than the usual probable cause standard. To get a wiretap, in addition to probable cause, the government must meet a number of other standards, including seriousness of the crime and an explanation of why the communications sought could not feasibly be obtained by other means. Authorisations for wiretaps must be for a specific and*

limited time and must include minimization of non-relevant information to protect the privacy of interceptees. Continued surveillance outside that timeframe without separate judicial authorization is considered unlawful.

26. Additionally, an application under the Wiretap Act must be approved at the highest levels of the US Department of Justice (DOJ) before it is authorized for submission to a judge. The Wiretap Act requires federal investigative agencies to submit requests for the use of certain types of electronic surveillance... to the DOJ for review and approval before those requests may be submitted for judicial review. The US Attorney General is tasked with reviewing and approving these requests, but is also allowed to delegate that authority to a limited number of high-level DOJ officials... These officials review and approve or deny requests for wiretaps and to install and monitor electronic bugs...

27. As is the case with the SCA, the Wiretap Act provides remedies to data subjects whose communications have been unlawfully intercepted by the US government. Remedies under the Wiretap Act are, as with the SCA, available to EU data subjects. Where an individual has 'intentionally' violated the Act, a data subject may be entitled to 'appropriate relief.' Relief can include an injunction of the action if ongoing, monetary

damages, and additional punitive damages where appropriate."

Then finally in that context, he deals with FISA and explains that it: 12:26

"*... provides individual remedies for data subjects against unlawful acts of individual government officers. If an individual officer conducts surveillance of a data subject without first obtaining statutory or Presidential authorisation, misuses surveillance information, or unlawfully discloses surveillance information, that individual officer can be sued by the data subject in US court. Authorising statutes, such as Section 702... provide additional restrictions and safeguards... A data subject who succeeds in suing an individual for conducting unauthorised surveillance may receive actual damages of not less than $1,000, statutory damages of $100 per day of unlawful surveillance, and the award of additional punitive damages and attorney's fees where appropriate... the Foreign Intelligence Surveillance Court (FISC) has been diligent in policing agencies that attempt to circumvent its judicial orders, and conducts ongoing review of surveillance programs. Along with the existence of the individual statutory remedies, the FISC has made clear that failure to comply with its orders can result in the revocation of authorisation*[s]."

He deals then, Judge, in the following pages with the criminal remedies. He had a summary of those, as you'll recall, in his opening chapter. And he then proceeds at page 7-12 to deal with various non-judicial remedies - and I'm just going to move through these very quickly; the PCLOB - we've heard of this before - the Congressional committees, and then over the page, individual remedies through the US press and various advocacy groups. And he elaborates upon those over the following pages. And if you go to 7-16, paragraph 41, he explains why he believes that these are relevant: 12:27 12:27

"*Lawyers sometimes assume that legal action is the most effective way to remedy a problem and effect change. In the discussion here, I highlight the crucial ways that remedies occur in the US through a free press, advocacy to the companies about their practices, and the efforts of nongovernmental organisations. The role of the press and non-governmental organisations is often substantial in the US for surveillance and privacy issues. In my view, a fair assessment of the checks and balances that exist against surveillance abuse should include consideration of the role of the free press and public advocacy.*"

Then in section III he deals with individual remedies against US companies, such as service providers of webmail, social networks, should they improperly

disclose information. And he then addresses privacy enforcement by some of the Federal agencies. He explains at paragraph 43 that individual remedies are available such as service providers on webmail and social networks should they engage in activities that violate state or Federal privacy laws or their own public privacy policies. He explains that: 12:28

"*Using its law enforcement and foreign intelligence authorities, the US government can seek to compel the production of personal data from a US company, or compel the aid of a company in conducting wiretaps or surveillance. These service providers have strong incentives to follow the law and their stated company policies. Violations can result in lawsuits against the service provider, as well as business harms.*"

He elaborates upon that, Judge, and then over the page refers to the private causes of action arising against private companies under the Stored Communications Act. He explains that that cause of action exists and what its parameters are at paragraph 45. And similarly, he engages in the same exercise at paragraph 47 in relation to the cause of action against non-state agencies under the Wire Tap Act. 12:29 12:29

He identifies, starting at 7-18, various Federal administrative agencies which have a role, which he explains, Judge, at the top of page 7-19, just above

paragraph 50. He explains that These administrative agencies do not themselves bring actions against intelligence agencies. However, he thinks they're important, because they *can* bring actions against companies that fail to comply with the applicable law or company privacy policies, such as when the companies improperly provide electronic communications to the government. And he explains in that regard the jurisdiction of the Federal Trade Commission tasked with regulating and enforcing actions in US commerce for the protection of consumers and the public welfare. 12:30 12:30

He gives a short history of the FTC and, at paragraph 53, explains the types of claims or actions that can be brought by the FTC for unfair or deceptive behaviour and he explains that this functions as a de facto common law of privacy norms and best practices. And he cites a textbook which describes these as default standards for privacy and that the FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States. And then examples are given of consent decrees obtained by the FTC in enforcement actions it brought against a number of private companies. 12:30 12:31 12:31

Then he says at paragraph 54:

"*Notably, as part of the US's participation in the Privacy Shield Framework, the FTC has committed to*

assistance in four areas: '(1) referral prioritisation and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation with EU DPAs.' This assistance includes information sharing and investigative assistance, including sharing information obtained in connection with an FTC investigation, issuing compulsory process on behalf of an EU DPA, conducting its own investigation, and seeking oral testimony from witnesses or defendant in connection with an EU DPA's enforcement proceeding. To assist in these commitments, the FTC will create a standardised referral process and provide guidance to EU Member States on the type of information that would best assist the FTC in its inquiry... The FTC has also committed to exchanging information on referrals with referring enforcement authorities..."

He addresses then, in a similar vein, the functions of the Federal Communications Commission, which is responsible for regulating and enforcing rules on interstate and international communications by radio, television, wire, satellite and cable. And then the type of enforcement privacy -- or, sorry, privacy enforcement actions it has taken against private companies are identified in the following paragraphs. 12:32 12:32

At page 7-24 he addresses the Consumer Financial

Protection Bureau and, at page 7-25, the SCC, which again has brought enforcement actions for failing to protect private information of customers, the Department of Health and Social -- sorry, the Department of Health and Human Services in section V, and again he instances actions taken, enforcement actions taken by it.

He moves, Judge, at 7-30, paragraph 70 to the power of enforcement under state law, including enforcement by the State Attorney Generals. And in paragraph 70 he explains that: 12:33 12:33

"*Section IV introduces privacy enforcement under state law and federal or state private rights of action. Each state has an Attorney General tasked with protecting consumers. As documented by Professor Citron, these AGs have emerged as important privacy enforcers. This Section then examines the numerous private rights of action that exist under both federal and state law, using the state of California as one example. The prevalence of plaintiffs' lawyers and private rights of action in the US means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law.*"

He then explains the role, which he summarises at paragraph 71, of the State Attorney Generals. He says

that:

"*I next describe an important but sometimes overlooked set of actors in privacy enforcement in the US, the State Attorney Generals.*" 12:34

He explains that they're the chief law enforcement officers, they've a wide range of powers and responsibility and he gives the example of California and enforcement action taken by the Californian state 12:34 through the Attorney General and other agencies.

He deals at paragraph 78 with the private rights of action. He says that:

"*It is something of a cliché (and often a true observation) that the US favors plaintiffs more than most other countries. During negotiation of the Safe Harbor in 1999-2000, I heard US Ambassador David Aaron, the lead US negotiator, say more than once to EU negotiators: 'We'll take your privacy laws if you take our plaintiffs' lawyers.' The prevalence of plaintiffs' lawyers and private rights of action means that defendants (including companies and often government agencies) have increased incentive to comply strictly with applicable law. In the US, the written law is usually not aspirational – it is the basis for enforcement and litigation.*"

Then he identifies features of the US legal system which favour plaintiffs and plaintiffs' lawyers: The attorney's fees, contingency fees, jury trial and broad discovery. And he identifies then, again going back to California, the individual statutes in the State of California which these plaintiffs' lawyers might be tempted to seek to have recourse to. 12:35

He then, at page 7-37, paragraph 84 deals with another reason that he feels US law favours plaintiffs, which is the availability and use of class actions. He explains what these are and identifies very large settlements that have emerged from the use of the class action procedure. 12:35

12:36

Now, he then moves, Judge, and considers, in a very short section of his report, standing to sue. And you'll find this at paragraph 87 on page 7-38. And what he explains here is that:

"*The Irish Data Protection Commissioner (DPC) has filed an Affidavit which states that 'the "standing" admissibility requirements of the US federal courts operate as a constraint on all forms of relief available' in the US. This statement appears to refer to the discussion of the US Supreme Court case Clapper -v- Amnesty International... In Clapper, Amnesty International and other plaintiffs brought a constitutional challenge to Section 702 of FISA on the*

day after it entered into force in 2008. The Supreme Court dismissed the challenge because it found the plaintiffs did not show an injury that granted them standing to sue."

And you'll recall the facts of this were outlined by Ms. Gorski in her evidence on Friday, as well as by Mr. Collins in the course of last week. But he says this:

"*88. It would be a mistake to read more into Clapper than it actually holds. In one sense, I agree with the quotation from the DPC, in the sense that a plaintiff does have to establish standing to sue in order to get relief from a US court. The case should not, however, be read to create a per se ban on cases involving US foreign intelligence or counterterrorism programs*" - I don't *believe* we have made that case - "*Two lower courts, for instance, have found that individuals had standing in the foreign intelligence realm, to challenge the Section 215 telephone metadata program.*" 12:37

And you'll see there again reference to **ACLU -v- Clapper** to which reference was made last week and another case, **Klayman -v- Obama**, which you'll see in Mr. Richards' report. And just on that, Judge, to answer the question that you asked me earlier about Section 215, that's 50 USC, Section 1861. 12:38

MS. JUSTICE COSTELLO: 1861?

MR. MURRAY: Yeah. And Section 702 is 50 USC, Section 1881a

MS. JUSTICE COSTELLO: I saw that in a footnote.

MR. MURRAY: Just to go back then, after footnote 292, he says: 12:38

"*Another court found, in a counter-terrorism setting, that an individual had standing to challenge suspected placement on the terrorist watch list.*" 12:38

And refers there to **Shearson -v- Holder**.

"*The facts and law of the individual case will determine whether an individual has standing...*

89. One concern the Supreme Court identified in Clapper is that when US surveillance is challenged in court, affirming or denying an individual's standing to bring the challenge permits him – or an adversary watching the case – 'to determine whether he is currently under US surveillance simply by filing a lawsuit.' This statement in Clapper is consistent with my discussion in Chapter 8, on how hostile actors can seek to use individual remedies to probe an intelligence agency and to learn its national security secrets. Chapter 8 explains in detail how an adversary intelligence agency could deploy an individual remedy to conduct such probes. It also documents how courts in both the EU and US have a clear history of caution about disclosing

national security secrets in open court."

You'll recall, Judge, this was the subject of some debate on Friday and the position was suggested by the witness that, inter alia, these problems could be addressed either by relaxing the standing regime, or alternatively, by having mandatory notification after there was no longer any prejudice. 12:39

"*90. Nor has Clapper turned out to prevent individuals from bringing lawsuits against companies that commit privacy violations, even in the absence of out-of-pocket damages. Since Clapper was decided in 2013, US courts have accepted major class-action litigation against companies such as Adobe Systems and Sony following data breaches. In a number of these cases, courts have affirmed individuals' standing on allegations that data was obtained by unauthorised third parties, without requiring individuals to show any financial or other loss.* 12:40

91. In addition, the doctrine of standing addressed in Clapper pertains only to the US federal courts, and thus at most impacts judicial remedies. This Chapter has identified multiple ways that individuals can seek to address privacy violations in the US, including: Judicial remedies; nonjudicial remedies...; administrative agency remedies...; state Attorneys General; and new remedies provided by the Ombudsman and

the Umbrella Agreement. Only federal judicial remedies are affected by even the broadest reading of Clapper.

92. All of the above gives reason for caution in interpreting the implications of Clapper. Moreover, the DPC has suggested that her findings on the effects of standing may need to be reassessed in light of the Ombudsman and the Umbrella Agreement. Through the Ombudsman mechanism, EU individuals can now lodge complaints regarding US government collection of data. Ombudsman complaints can be brought regardless of whether individuals can show that personal data has been collected, and without needing to show that harm or other adverse consequences were suffered. Similarly, individuals can exercise access rights under the Umbrella Agreement...

VI. Conclusion

93. This Chapter has sought to present in an organised and understandable way the US system for individual remedies for privacy violations. Section I described judicial remedies against the US government. Section II described non-judicial remedies... Section III described how suits against non-governmental entities operate... Section IV filled out the enforcement landscape...

94. As stated in the introduction... these individual remedies complement the systemic safeguards in the US

system..."

Now, Judge, if I could respectfully say one perhaps ends that analysis not necessarily seeing a *huge* difference in the legal explanation or the explanation that has been proffered by the Commissioner's expert witnesses of what the requirements for standing are, of the difficulties that they present or indeed of the other limitations arising under the Judicial Redress Act, which of course merely makes available the remedies under the Privacy Act, which in turn is subject to, as you will have heard, a wide range of exceptions, a context in which a number of agencies and in particular the NSA and, I think, the CIA are not covered by the Judicial Redress Act insofar as those remedies are concerned, insofar as Mr. Collins explained last week, damages provisions which, under **Cooper**, require proof of what we would call actual damage and provisions which have requirements of willful -- proof of willfulness or intention before those remedies will be available. 12:42 12:42 12:42 12:43

I'd also note, it's perhaps just of relevance when we look at Prof. Vladeck's report, that the Administrative Procedure Act I don't think features in Prof. Swire's analysis *at all*. He may make short reference to it, but it certainly doesn't feature prominently in his analysis. 12:43

Sorry, excuse me, Judge, I had intended --
Mr. Gallagher has helpfully just reminded me that there is, at the end of chapter seven --
MS. JUSTICE COSTELLO: I saw this chart, yes.
MR. MURRAY: Yeah, there's a chart which sets out US privacy remedies and safeguards and whether or not they are available to EU persons. 12:43

Just to note, now that I have it open, if you go to 7-45 you will see that in the context of the constitutional remedy under the Fourth Amendment, the fourth item down, "*Civil suit against law enforcement officials that perform an unlawful search under the Fourth Amendment*", certainly Prof. Swire appears to be of the view that that remedy is only available if they are in the US at the time of the search. And that goes back to the **Urquidez** case which Mr. Collins referred you to last week. 12:44 12:44

The other expert report, Judge, which Facebook have tendered is Prof. Vladeck's. And you'll find that at tab two. 12:44
MS. JUSTICE COSTELLO: In which trial book?
MR. MURRAY: I'm sorry, the same book, Judge. Prof. Vladeck, Judge, is a professor at the University of Texas Law School. He's published widely in relation to national security law and counter terrorism. And at paragraph two of his report he outlines the basis for his expertise - he relates it especially to cases 12:45

arising out of the war on terrorism. He's the co-author of national security law and counter terrorism case books, he explains they're the leading US law textbooks in their respective fields and that he's published in an array of legal publications, including the Harvard Law Review and the Yale Law Journal and that these articles have been cited by US courts and academic commentators. He's been called to testify before Congress over a dozen times, including at a rare public hearing held by the House Permanent Select Committee on intelligence in the aftermath of the Snowden disclosures. And he refers then to other consultation he's provided and to a number of awards which you'll see outlined, Judge, over the following page. And he gives his educational qualifications at paragraph five. 12:45 12:46 12:46

Now, I hope it's fair to say, Judge, that in the first number of paragraphs, six to nine, he just summarises what the Commissioner has said. And if I can pick up at paragraph ten. He says this: 12:46

"*As I explain in the Report that follows, it is my expert opinion that the DPC Draft Decision's analysis is incomplete in several key respects, each of which contributes to an inaccurate picture of the protections (and remedies) available under current US law to EU citizens whose data is held by US companies. As noted below, some of these inaccuracies are compounded by*

similar shortcomings in the Morrison & Foerster Memo and the O'Dwyer Affidavit, and not adequately addressed in the Gorski Report.

11. Thus, this Report endeavours to provide an outline of current US data collection authorities relevant to data of EU citizens held by US companies, the most significant internal and external checks on such data-gathering, and the current scope of judicial and non-judicial remedies for individuals whose data are unlawfully collected, used, or retained.

12. As this Report explains, thanks to a series of reforms-including... PPD 28... the USA FREEDOM Act... and... the Judicial Redress Act... there is a more robust legal regime today to protect data of EU citizens held by US firms from unlawful seizure by the US government as compared to what was true under US law as recently as two years ago. While this Report takes no position on whether these safeguards are sufficient as a matter of EU law, it cannot be gainsaid that they have markedly improved privacy protections for EU citizens as a matter of US law and practice.

13. Moreover, although standing doctrine has been an obstacle to some *efforts to obtain judicial redress in cases in which such data is unlawfully seized, it is not nearly as comprehensive a constraint as the DPC Draft Decision suggests and the same issues raised in*

cases in which standing has been rejected have been litigated on the merits elsewhere. Indeed, with one important but equivocal exception" -

And that's the exception that the Fourth Amendment can't be used as a cause of action by anyone other than US citizens or non-citizens lawfully present. And he then observes that that's an equivocal exception, because US courts have been hostile, in any event, to the **Bivens** claims in a national security context. But to go back to the text after footnote two. He says: 12:48 12:48

"*The upshot of these reforms has been to place EU citizens on materially equal footing as their American counterparts, at least with respect to their ability to seek redress in cases of allegedly unlawful data collection from US firms on US soil.*"

Judge, what Prof. Vladeck then does - and subject to the court and Mr. Gallagher, I propose to pass over it - is he goes through his own, quite properly, his own description of each of the legal mechanisms: The Executive Order, which you'll see starting at paragraph 15; FISA, paragraph 18; the extension of FISA to cover physical searches and pen registers; the Electronic Communications Privacy Act; the PATRIOT Act at paragraph 34; FISA amendments at paragraph 38; he addresses PRISM and the Privacy Shield. 12:49 12:49

And then at paragraph 54 he addresses the, I suppose, substance of his analysis, starting with constraints on US collection authorities. So I will, with your leave, unless Mr. Gallagher has an objection, move directly to paragraph 54, because the court has already obviously *some* familiarity with those legal provisions. So having outlined those, he says at paragraph 54: 12:50

"*By far, the most widely cited constraint on US data collection authorities is the Fourth Amendment.*" 12:50

And he quotes that. He says:

"*Contemporary Supreme Court doctrine has reduced the Fourth Amendment to two different requirements - the Warrant Clause...; and the Unreasonable Search and Seizure Clause.*

55. In the context of data of EU citizens held by US companies, however, the Fourth Amendment is less likely to play a role. Under the Supreme Court's 1990 ruling in United States -v- Verdugo-Urquidez, non-citizens lacking substantial voluntary connections to the United States are not protected by the Fourth Amendment... Although the Supreme Court has never addressed whether the Fourth Amendment might apply to searches of those individuals' data if the data is located within the United States, the prevailing assumption is that the answer is 'no'.

56. Even if the Fourth Amendment does apply... the collection authorities most relevant to data of EU citizens held by US companies have thus far been held to not violate the Fourth Amendment, either because of a 'foreign intelligence surveillance' exception to the Warrant Clause; the 'third-party doctrine; or some combination thereof. In this regard, EU citizens are no differently situated than their American counterparts; the principal and most significant constraints on the government's data collection and retention authorities... are statutory and administrative.

57. As noted above, each of the collection authorities relevant to EU citizen data held by US companies includes a series of built-in collection restrictions. Thus, Section 2703(d) orders and NSLs are quite limited in the specific kinds of information that companies can be" -- 12:52

MS. JUSTICE COSTELLO: Can you we mind me what NSLs are?

MR. MURRAY: Yes. These are letters that are sent, the national security letters requiring the recipient to provide information in accordance with 12:52 their terms. Now, the legal basis for those I think may be order 12333 --

MR. GALLAGHER: No, if you go back to 29 and 30.

MR. MURRAY: Sorry, Mr. Gallagher has

helpfully asked me to go back to 29 and 30, Judge, page nine.

MS. JUSTICE COSTELLO: I have that, yes.

MR. MURRAY: So he addresses them there:

"*29. At the same time as these authorities were evolving, Congress also began to create more specific (and secretive) authorities for third-party data requests - what came to be known as... (NSLs). Although NSLs have their origins in financial privacy... they became increasingly popular in the 1980s and 1990s in response to state privacy laws...*

30. Thus, the SCA also created the first true NSL authority" - that answers my question - "*authorising requests to 'wire or electronic communication services provider[s]', but only for 'subscriber information and toll billing records information'... and only if (1) the information was 'relevant to an authorised foreign counterintelligence investigation', and (2) there were 'specific and articulable facts giving reason to believe that the person or entity... is a foreign power'.*"

He explains they were less powerful than subpoenas, more than adequate in situations where state privacy legislation presented the only barrier to compliance and he says there's four NSL authorities other than section 2709, all of which relate to financial records, 12:53

consumer credit agencies. They're non-judicial, he says in 32, but Congress has also amended FISA to allow government to obtain orders from the FISC to third parties to produce documents in their possession concerning identified foreign power. 12:54

So, Judge, sorry, just to go back then, I was on paragraph 57.

MS. JUSTICE COSTELLO: Yes, thank you.

MR. MURRAY: He says: 12:54

"... *FISA warrants can sweep more broadly, but they require probable cause to believe that the target of the search is not just a foreign national, but an 'agent of a foreign power'; and section 702 only authorises programmatic surveillance consistent with the prescribed targeting and minimization requirements.*

58. Under the NSA's now-declassified minimisation requirements under section 702, the agency may retain communications to, from, or about an American if they contain foreign intelligence information (an expansively defined concept that includes information relating to US foreign affairs), evidence of a crime, certain cybersecurity-related information, or information 'pertaining to a threat of serious harm to life or property'... Although the Wittes/Mirski analysis" - which he quotes there, or references there - "*was pegged to the 2011 procedures, the 2015*

procedures do not appear to be materially different... The government has also declassified the FBI's 2014 and the CIA's 2015 minimisation procedures under section 702...

59. US persons communications that do not meet those criteria are generally to be 'destroyed upon recognition', but the NSA is otherwise permitted to retain these communications for up to six years from the start of surveillance. And the NSA may share 'unminimised communications' with the FBI and CIA, subject to those agencies' minimisation procedures.

60. Communications acquired under section 702, whether of US persons or non-US persons, are stored in databases with strict access controls. They may be reviewed only by intelligence personnel who have been trained in the relevant (and privacy protecting) minimisation procedures, and who have been specifically approved for that access in order to carry out their authorized functions."

And he refers to the Litt letter.

"*61. In light of these measures, in its 2014 Report on section 702, the PCLOB concluded that 'the protections contained in the Section 702 minimisation procedures are reasonably designed and implemented to ward against the exploitation of information acquired under the* 12:56

program for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits.'

62. And although the targeting and minimisation requirements under section 702 are designed to minimise the collection of US person information, one of the central reforms of PPD-28 is to expand application of these principles to collection of non-US person data, as well. Under... PPD-28, section 2, signals intelligence collected in bulk can only be used for six specific purposes: Detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to US or allied armed forces; and combating transnational criminal threats, including sanctions evasion.

63. Further to that end, section 4 of PPD-28 requires that each U.S. intelligence agency have express limits on the retention and dissemination of personal information about non-US persons collected by signals intelligence, comparable to the limits for US persons. To qualify for retention or dissemination as foreign intelligence, personal information must relate to one of the authorised intelligence requirements described above; be reasonably believed to be evidence of a crime; or meet one of the other standards for retention

of US person information...

64. Information for which no such determination has been made may not be retained for more than five years, unless the Director of National Intelligence expressly determines that continued retention is in the national security interests of the United States. Thus, US agencies must generally delete non-germane non-US person information collected through signals intelligence five years after collection. Section 4(a)(1) of PPD-28 further bars US agencies from disseminating personal information solely because the individual in question is a non-US person.

65. In addition to the targeting and minimisation restrictions, one of the most significant constraints on the government's ability to use data within its possession is the Privacy Act of 1974, which restricts the records that a federal agency may keep, requiring that they be 'relevant and necessary to accomplish a [required] purpose of the agency.' When an agency 'establish[es] or revis[es]' the 'existence or character' of a database, it must publish a notice in the Federal Register... The SORN describes the records being kept in the database and their permissible uses. The Act also obligates agencies to give individuals a mechanism to see and challenge the accuracy of their information... and it restricts agencies' maintenance of information about First Amendment-protected

activity...

66. Although the Privacy Act as written only applies to US persons, the Judicial Redress Act... extends its protections to citizens of covered countries (or 'regional economic integration organisations'). A country (or regional economic integration organization) can be designated as 'covered' under the JRA by the Attorney General if (i) it has an agreement with the United States regarding privacy protections for data shared in the course of joint investigations, or has 'effectively shared' such information with US authorities and adequately protects privacy; (ii) it allows US companies to transfer its citizens' data between its territory and the United States; and (iii) the data-transfer agreement does not 'materially impede the national security interests of the United States'... The U.S. government has not yet made the 'covered country' determinations...

67. To be sure, even if the EU is so designated, the JRA would not necessarily put EU citizens on the same footing as US persons, given the limits on the kinds of causes of action that can be brought under the JRA...; and the specific definition of a 'covered record' to focus on materials transferred from overseas to 'a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.'

68. These distinctions may pale, however, in comparison to larger constraints built in to the Privacy Act itself, including the authority of agencies to exempt their records from the Privacy Act in their entirety in certain circumstances, including when the records are classified in the interest of national security."

And this is the point I just referred to when I finished Prof. Swire's report. 13:00

"The NSA has taken advantage of this provision... *'All systems of records maintained by the NSA/ CSS and its components shall be exempt... to the extent that the system contains any information properly classified under Executive Order 12958 and that is required by Executive Order to be kept secret in the interest of national defense or foreign policy.'). Lest it seem like this maneuver is controversial, though, 'It is hard to see how it could be otherwise'*" - and he's 13:00 quoting here from a text, Mr. Edgar - "*'It is hard to see how it could be otherwise... [I]f the NSA obtains data belonging to a terrorist who is in Paris and may be planning an attack, it should not have to provide the target with access to his files and the ability to* 13:00 *correct them', the core purpose of the Privacy Act*".

MS. JUSTICE COSTELLO: We might take a break at that point. I'm sure you need it.

MR. MURRAY: Thank you.

(LUNCHEON ADJOURNMENT)

THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS FOLLOWS

REGISTRAR: Data Protection Commissioner -v- Facebook Ireland.

MS. JUSTICE COSTELLO: I spoke to the registrar Mr. O'Neill, so I can sit on Monday in this case.

MR. MURRAY: Oh, very good. Thank you, Judge.

MS. JUSTICE COSTELLO: We'll take it at eleven o'clock.

MR. GALLAGHER: Thank you. 14:02

MR. MURRAY: Thank you. Judge, so we're dealing with Prof. Vladeck's report and I was just at page 20 paragraph 69, the report is at Tab 2.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: And Prof. Vladeck having referred to Mr. Edgar's blog, he continues on: 14:03

"*69. On top of these varying built-in collection, use, and retention restrictions, U.S. government data collection is subject to a series of oversight and accountability mechanisms. The NSA – one of 17 U.S. intelligence agencies – has over 300 employees dedicated to compliance, and other agencies also have their own oversight offices. The Department of Justice provides extensive oversight of intelligence activities.*

70. Each U.S. intelligence agency has its own Office of the Inspector General, internal departments with

responsibility for oversight of foreign intelligence activities, among other matters. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions. And although Inspector General recommendations are usually non-binding, their reports are often made public, and are in any event are provided to congress. Congress is thus kept abreast of any non-compliance.

71. In addition, the Office of the Director of National Intelligence's Civil Liberties and Privacy Office (CLPO) is tasked with responsibility for ensuring that the U.S. intelligence community operates in a manner that advances national security while protecting civil liberties and privacy rights. Other U.S. intelligence agencies have their own privacy officers.

72. Moreover, as noted above, the PCLOB has been charged by Congress with the responsibility for analyzing and reviewing counterterrorism programs and policies, including the use of signals intelligence, to ensure that they adequately protect privacy and civil liberties. Among its public reports on intelligence activities is a comprehensive report on collection under section 702.

73. Finally, Congress, through the House and Senate Intelligence and Judiciary Committees, exercises significant oversight responsibilities with respect to U.S. foreign intelligence activities. For collection under section 702, specifically, Congress exercises oversight through statutorily required reports to the Intelligence and Judiciary Committees, and periodic briefings and hearings. These include a semiannual report by the Attorney General documenting the use of section 702 and any compliance incidents; a separate semiannual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures designed to ensure that collection is for a valid foreign intelligence purpose; and an annual report by heads of intelligence elements which includes a certification that collection under section 702 continues to produce foreign intelligence information. Taken together, this array of oversight authorities led one commentator to describe FISA surveillance as 'the most oversight-laden foreign intelligence activity in the history of the planet'.

74. In addition to these oversight mechanisms, each of the collection authorities described above is subject to judicial review. NSLs and section 2708(d) orders can be attacked by their recipients in regular federal district courts. FISA warrant applications are carefully scrutinized by the FISC (and can be

collaterally attacked in civil and criminal litigation, as discussed below), and collection under section 702 is also subject to review by the FISC (and, in some cases, collateral review in civil and criminal litigation, as discussed below). Indeed, section 702 expressly authorizes the recipient of the 'directives' to challenge such directives before the FISC – and to appeal adverse decisions to the FISC and, if necessary, the Supreme Court."

14:05

And he gives an example of that, entertaining an appeal from Yahoo.

"*75. The FISC not only provides review of section 702 collection when it authorizes the initial program (and recertifies it thereafter), but it exercises an ongoing review of these authorities through the government's obligation to report compliance incidents."*

And he references then a provision: "*Mandating written submissions to the judge who approved particular applications whenever the government discovers 'that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law'). Indeed, one of the most troubling reported abuses of section 702 came to light only because of a declassified October 2011 opinion identifying the abuse (in response to a reported compliance incident) and*

14:06

sanctioning the government."

And he refers then to the Bates opinion.

"*Although there are reasons to question whether the judicial review provided by the FISC is as rigorous as it could be, there is little doubt, as the October 2011 episode demonstrates, that it has served as a significant check upon the government's execution of its collection authorities.*

76. To help bolster the FISC's role as an accountability mechanism, Congress in the USA FREEDOM Act of 2015 formalized a procedure for the participation of an amicus curiae tasked with providing the court with 'legal arguments that advance the protection of individual privacy and civil liberties,' 'information related to intelligence collection or communications technology,' or 'legal arguments or information regarding any other area relevant to the issue presented to the court,' in cases 'present[ing] a novel or significant interpretation of the law.'

Although, he says, as I have written elsewhere, I believe Congress could – and should – have gone further in the creation of such a 'special advocate' position, the amicus provision already appears to have had a salutary impact on the quality of the FISC's decision making, as evidenced by amica curiae Amy

Jeffress's well-documented role in an important November 2015 ruling by the FISC.

77. In addition, as noted below, the government's execution of its collection authorities is also subject to accountability through ordinary civil and criminal litigation – including motions to suppress evidence derived from these collection programs in criminal cases and civil suits seeking declaratory or injunctive relief or damages arising out of alleged abuses of these authorities. The remedial scheme is by no means perfect, but there is little question that the existence of these additional accountability mechanisms exerts pressure on the government to hew to the permissible scope of its collection authorities.

78. Thus, the collection authorities described above are subject to a series of significant constraints."

And he then lists those legal constraints on collection: 14:08

"*Including built-in limits and those required by the Fourth Amendment, EO 12333 and PPD-28;*

b. Legal constraints on the use and retention of collected information, including built-in limits and those required by the Fourth Amendment, Executive Order 12,333, PPD-28, and federal statutes such as the Privacy Act; 14:08

c. Robust internal constraints on access to the collected data;
d. Internal oversight;
e. External oversight by the PCLOB;
f. External oversight by the House and Senate intelligence and Judiciary Committees; and
g. Ex ante and ongoing judicial supervision."

Then he moves to remedies.

14:08

"79. In addition to the substantial oversight and accountability mechanisms described above, US law 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 applied in U.S. federal courts 'operate as a constraint on all forms of relief available.' This conclusion was apparently predicated on the discussion of Article III standing in the Morrison & Foerster Memo. On closer inspection, although there certainly are defects in the existing remedial scheme, the DPC Draft Decision (like the Morrison & Foerster Memo) fails entirely to account for several of its key features while misinterpreting several others—and, as a result, paints a rather incomplete picture of contemporary law.

80. First, the DPC Draft Decision, like the Morrison &

Foerster Memo, nowhere mentions 50 U.S.C. 1809, which makes it a federal felony for an individual to intentionally 'engage in electronic surveillance under color of law' without statutory authorization, or to 'disclose or use information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized' by statute. Thus, if any government official intentionally conducts unauthorized surveillance or discloses or uses the fruits thereof, they face serious criminal penalties under U.S. law.

81. Second, as in the Morrison & Foerster Memo, the DPC Draft Decision's survey of available remedies to challenge unlawful electronic surveillance is incomplete. Of most significance, neither the DPC Draft Decision nor the Morrison & Foerster Memo anywhere addresses the Administrative Procedure Act (APA), section 702 of which provides that 'A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review including declaratory and injunctive relief'. Critically for present purposes, section 702 does not distinguish between plaintiffs who are US persons and those who are not."

And he refers then to a case call **Bangura -v- Hamsen**.

*"82. Indeed, it was the APA, and not any of the causes of action discussed in the DPC Draft Decision, that provided the basis for the Second Circuit's invalidation of the bulk phone records program in **ACLU -v- Clapper**, only after the court painstakingly explained why none of the more specific remedies referred to in the DPC Draft Decision or the Morrison & Foerster Memo preempted or otherwise precluded the more general remedy provided by the APA.*

83. The existence of a private civil remedy to challenge allegedly unlawful surveillance under the SPA is significant because it overcomes many of the shortcomings the DPC Draft Decision and Morrison & Foerster Memo identified in the other discussed civil remedies; if the government is collecting the data of an EU citizen in violation of the FAA or some other statutory constraint (or, indeed, in violation of the U.S. Constitution), the APA appears to provide a remedy for declaratory and/or injunctive relief available to U.S. citizens and non-citizens alike.

84. Third, with regard to damages, the DPC Draft Decision, like the Morrison & Foerster Memo, is skeptical of the remedy provided by 50 U.S.C. 1810 because, as it correctly notes, 'this provision does not operate as a waiver of sovereign immunity, which means that the US cannot be held liable under this section'."

And he then quotes a case of **Al-Haramain Islamic Foundation -v- Obama**.

"*But the DPC Draft Decision proceeds to suggest that 'the utility of pursuing individual officers may is [sic] questionable,' without providing any substantiation. Indeed, 'officer suits' have always been the most common mechanism for obtaining damages under U.S. law when suing government officials within their official capacity – entirely because of sovereign immunity concerns.*

85. Thus, there is nothing untoward about the specter of suing an individual officer – for example, the Director of National Intelligence – for unlawful surveillance. If the DPC Draft Decision's skepticism of section 1810 is instead attributable to the (surely correct) view that an individual officer is not likely to be in a position to satisfy a significant damages judgment, it is worth emphasizing that, in virtually every case in which section 1810 could apply, the federal government would almost certainly indemnify the officer defendant.

86. Fourth, the DPC Draft Decision is skeptical of the utility of the suppression remedy provided by section 1806 – which allows defendants in criminal cases to seek to exclude any evidence derived from FISA on the ground that it was unlawfully obtained. Commissioner

Dixon is certainly correct that the section 1806 suppression remedy 'is not a free-standing mechanism that can be invoked, but rather is more akin to a defensive protection correct the individual in administrative and judicial proceedings.' But this analysis neglects the very distinct possibility that a motion to suppress may result in litigation of a substantive legal issue of transcendent importance – including the legality of particular collection methods and programs under section 702.

87. Indeed, the most significant constitutional challenges to section 702 to date have all arisen in the context of motions to suppress evidence in criminal cases."

And then gives examples of that: *"If any of those cases lead to a judicial determination that evidence should be (or should have been) suppressed because particular aspects of 702 collection are illegal and/or unconstitutional, that will necessarily have consequences far beyond that individual defendant's case.*

88. Fifth, the DPC Draft Decision also suggests that existing remedies would provide no basis for challenging collection of data under non-statutory authorities such as Executive Order 12,333. Thus, it concludes, 'it is simply not possible 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 authorities in question simply do not apply to EU citizen data held by U.S. companies within the United States. Thus, while I share the DPC Draft Decision's concern about the dearth of legal remedies for abuses of these authorities, I fail to see how they are germane to the scope of this particular inquiry."

And that again, Judge, is an issue that was debated last Friday with the witness.

"89. Sixth, the DPC Draft Decision, providing analysis similar to that offered in Morrison & Foerster memo rightly raises concerns about Article III standing – the requirement that a plaintiff demonstrate an injury-in-fact that has been caused by the defendant and that can be redressed by a favorable decision." 14:14

And he refers then to the O'Dwyer affidavit:

"*As the DPC Draft Decision noted the Supreme Court's decision in **Clapper** rejected the standing of a number of private plaintiffs to challenge the constitutionality of Section 702 on the ground that they could not demonstrate that collection of their communications were 'certainly impending', or that,* 14:14

even if they could, they could not demonstrate that such a collection was 'fairly traceable' to Section 702 as opposed to some other government surveillance authority."

14:15

And then in footnote 23 he explains that: "*The plaintiffs in **Clapper** were 'attorneys and human rights, labour, legal, and media organisations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad'. 'They communicate by telephone and e-mail with people the Government 'believes or believed to be associated with terrorist organizations', 'people located in geographic areas that are a special focus of the Government's counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government'."*

And as has been explained to you, Judge, notwithstanding that position, and the occupation of the plaintiffs, it was held there was no standing. And Prof. Vladeck indeed says at paragraph 90:

14:15

"*I have been sharply critical of the **Clapper** ruling before, and have also suggested that it might well have come out differently had it been decided after the Snowden disclosures."*

And he cites his own article there:

"*But the DPC Draft Decision errs, in my view, in concluding that U.S. law thereby requires a claimant 'to demonstrate that harm has in fact been suffered as a result of the interference alleged.' Even after the* ***Clapper*** *decision, it is still sufficient, under U.S. law, for a claimant to demonstrate nothing more than 'the collection, and maintenance in a government database, of records relating to them.' As the citation suggests, this was the basis upon which the ACLU and other privacy and civil liberties organizations were successfully able to challenge the bulk phone records program under section 215.*

91. To similar effect, the federal appeals court in Philadelphia recently reversed the district court's dismissal of an attorney's challenge to the constitutionality of section 702 – the same claim as in ***Clapper*** *– on the ground that, at least based on the facts as alleged by the plaintiff (which, at that preliminary stage of the litigation, had to be taken as true)."*

MS. JUSTICE COSTELLO: Was that a facial challenge as it is called? 14:17

MR. MURRAY: Yes. And he explains that, Judge, because he says:

"*He very well might have standing to bring the precise*

*claim that the plaintiffs in **Clapper** were barred from pursuing."*

And he refers to that case **Schuchardt**: *"To be sure, the Third Circuit was skeptical that, based upon public reports concerning section 702, the plaintiff would be able to adduce evidence in support of his factual allegations to withstand a motion for summary judgment. But the larger point for present purposes is how narrowly numerous courts have read the Supreme Court's **Clapper** decision – even in substantially similar contexts."*

Then he comes back to, I think, the cases which have been referred to before, the **Obama -v- Klayman** case. 14:17
You saw that referenced by Prof. Swire. He said:

"*The only court of appeals that has rejected a plaintiffs standing to challenge a secret surveillance program since **Clapper** was the D.C. Circuit in **Obama -v- Klayman**. But in rejecting standing, the court in Klayman pegged its analysis to the higher burden a plaintiff must overcome when pursuing a preliminary injunction, holding only that the plaintiff could not show a 'substantial likelihood of success' on the standing question. Although I have criticized the court for applying the higher injunction standard to the standing."*

MS. JUSTICE COSTELLO: Sorry, I have lost you, what

paragraph are you on?

MR. MURRAY: Sorry, it's footnote 25, Judge.

MS. JUSTICE COSTELLO: Oh, I beg your pardon.

MR. MURRAY: No, no, I'm sorry, that's my fault. So it's: *"The only Court of Appeals that rejected the plaintiff's standing."* 14:18

MS. JUSTICE COSTELLO: Yes, I see that, yes. Thank you, yes.

MR. MURRAY: And he continued: *"But in rejecting standing, the court in **Klayman** pegged its analysis to the higher burden a plaintiff must overcome when pursuing a preliminary injunction, holding only that the plaintiff could not show a 'substantial likelihood of success' on the standing question. Although I have criticized the court for applying the higher injunction standard to the standing question."*

He gives the citation for that: *"Klayman's focus on the unique posture of that case will likely vitiate its precedential value in other contexts – including on remand in the same case, in which the district court still concluded that one of the plaintiffs had standing."* 14:18

So to go back up to the text at paragraph 92: 14:19

"*Further, evidence of the avenues for establishing standing after **Clapper** can be found in District Court decisions in non-surveillance case, in which a number*

*of courts have read the Supreme Court's ruling so as not to preclude standing simply because the direct injury has not yet publically manifested. Thus, the court in **Natural Resources -v- Illinois Power** found standing on the part of environmental groups to challenge a power plant's compliance with emissions standards based on future harm, even though the plaintiffs stipulated that the emissions were not causing them any health harms. As the district court explained, **Clapper** left intact the Supreme Court's earlier ruling in **Friends of the Earth Inc. -v- Laidlaw**, which did not require proof of direct, personal harm so long as the plaintiffs could demonstrate a likelihood of harm to their recreational or aesthetic interests.* 14:19

*93. Likewise, the district court in **In re Sony Gaming Networks** explained that **Clapper** did not foreclose standing when plaintiffs 'alleged a 'credible threat' of impending harm based on the disclosure of their Personal Information following [a cyber] intrusion,' even though none of the plaintiffs alleged that the intrusion actually led to a third party gaining access to their data. As the Supreme Court itself clarified one year after **Clapper**, '[an allegation of future injury may suffice if the threatened injury is 'certainly impending, or there is a 'substantial risk' that the harm will occur.' Given how much more is publicly known today about U.S. government surveillance*

*authorities – especially section 702 of FISA – it seems far more likely that an EU citizen could demonstrate a 'substantial risk' that his communications will be unlawfully collected by the U.S. government today than it would have would have appeared to the Supreme Court in **Clapper**."*

And then he says over the page: "*Of course there have also been district court decisions since **Clapper** that have rejected standing to challenge secret government surveillance programs; including **Jewel**, discussed below, and the Section 702 specific analysis in **Wikimedia -v- NSA**. As these cases illustrate, there is significant uncertainty in the lower courts over exactly when **Clapper** does and does not foreclose standing, and I do not mean to suggest otherwise. The critical point for present purposes is that this uncertainty is not merely as categorically hostile to standing as suggested in the DPC Draft Decision, instead is more reflective of the case-specific vagaries of individual lawsuits.*

*95. Thus, based on the cases surveyed above, it is my view that, where EU citizens can marshal plausible grounds from which it is reasonable to believe that the U.S. government has collected, will collect, and/or is maintaining, records relating to them in a government database, they will likely have standing to sue even in light of the Supreme Court's **Clapper** decision.*

*96. Seventh, the DPC Draft Decision, perhaps motivated by similar discussion in the Morrison & Foerster Memo, also expresses concern about Rule 11 and its requirement that 'the factual contentions [made in a pleading] have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.' Together with **Clapper**, the DPC Draft Decision concludes, Rule 11 'would appear to preclude the bringing of precisely the kind of complaint now before me.' This conclusion rests on a significant misunderstanding - he says - of Rule 11, which is designed to authorize the imposition of sanctions upon attorneys who abuse the judicial process – and not to disincentivize claims against the government that may fail to materialize after discovery. As the Reporter's Notes accompanying Rule 11 state: 'If evidentiary support is not obtained after a reasonable opportunity for further investigation or discovery, the party has a duty under the rule not to persist with that contention. Subdivision (b) does not require a formal amendment to pleadings for which evidentiary support is not obtained, but rather calls upon a litigant not thereafter to advocate such claims or defenses'.*

In other words, the purpose of Rule 11(b) is not to prevent parties from bringing lawsuits in the first

place, but rather to prevent them from continuing to press claims once (and for which) it has become clear that there is no evidentiary support. Especially where the relevant evidence is secret, it is difficult to imagine that the government would ever seek to invoke Rule 11(b), or that a court would grant a motion thereunder, at the outset of a suit.

97. Eighth, with regard to the DPC Draft Decision's discussion of the Judicial Redress Act, it is true, as the Report suggests, that 'the US Supreme Court has held that a claimant seeking to recover statutory damages under the Privacy Act must prove, not just that 'actual damages' have been incurred, but that he or she has incurred pecuniary loss or damage'." 14:23

And he refers to **Cooper**.

"*But the DPC Draft Decision, like the Morrison & Foerster Memo, views this requirement as one of 'standing,' and, suggests that an inability to demonstrate pecuniary loss will foreclose all of the remedies provided by the JRA. This is not correct. At most, a plaintiffs inability to demonstrate pecuniary loss in this context will prevent him from obtaining damages. He will still be entitled to pursue a claim for any other appropriate relief under the JRA and Privacy Act, including declaratory and/or injunctive relief.*

98. In summary, then, although there are shortcomings in the existing U.S. legal regime with regard to redress of unlawful government data collection, I do not believe that they are nearly as comprehensive – or that standing is as categorical an obstacle – as the DPC Draft Decision or the Morrison & Foerster Memo suggest. Indeed, although I have been critical, in numerous writings, of the gaps and defects in contemporary U.S. doctrine when it comes to judicial review of U.S. counterterrorism policies (and the means by which they are carried out). It is worth emphasizing that challenges to government surveillance and data collection are among the most well-protected remedies in this sphere, second only to the constitutionally required remedy of habeas corpus for those unlawfully detained." 14:24

If you look then, Judge, at footnote 29 he explains that: "*After the Supreme Court's **Clapper** decision, I suggested that '[a]bsent a radical sea change from the courts, or more likely intervention from Congress, the coffin is slamming shut on the ability of private citizens and civil liberties groups to challenge government counterterrorism policies'.* 14:24 14:25

I continue to believe, as noted above, that U.S. courts have made it too difficult for such plaintiffs to challenge post-September 11 counterterrorism and national security policies. But, perhaps because of

*Edward Snowden's subsequent disclosures, U.S. courts have been much more willing to recognize standing to challenge secret surveillance programs in recent years than I would have expected after **Clapper**, including in the cases noted above."* 14:25

So, Judge, to go back to paragraph 99:

"*Separate from the DPC Draft Decision, concerns about the scope of remedies for EU citizens under US law have* 14:25
also been raised in the Expert Report of Ms. Ashley Gorski, a lawyer with the National Security Project of the ACLU. Like the DPC Draft Decision, Ms. Gorski's Expert Report emphasises concerns over whether EU citizens will have standing to challenge the unlawful 14:25
collection, retention or use of their data under existing US law."

And he continues then at paragraph 100: "*Unlike the DPC Draft Decision, Ms. Gorski's Expert Report also* 14:26
invokes the 'state secrets privilege' as a separate obstacle preventing US federal courts from entertaining challenges to secret surveillance programs. In fact, the 'state secrets privilege' is actually two separate doctrines under U.S. law – '[o]ne completely bars adjudication of claims premised on state secrets (the 'Totten bar, the other is an evidentiary privilege ('the Reynolds privilege') that excludes privileged evidence from the case and may result in dismissal of

the claims.' In the context of the surveillance authorities discussed above, it would be difficult to fathom an appropriate case for invocation of the Totten bar, since the authorities themselves are not secret – and, thanks to what has become public after and, in light of the Snowden disclosures, the key programs under those authorities are no longer secret.

101. Thus, the state secrets privilege would pose its own obstacle to civil remedies in this context if and only if it requires the exclusion of a sufficient quantum of evidence such that it 'become[s] apparent that the case cannot proceed without privileged evidence, or that litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets.'

But whereas the state secrets privilege has posed significant obstacles, he says, to a number of other efforts to obtain redress for post-September 11 counterterrorism abuses, it has been singularly ineffective in the context of challenges to surveillance programs, at least in part because courts have held that FISA itself – by expressly authorizing civil remedies for violations of the statute (which, of necessity, would implicate state secrets) – necessarily abrogates the privilege as applied to FISA-based claims."

And he refers there to the **Jewel** case and quotes from that.

"*In other words, the state secrets privilege will be unavailable for claims that particular collection programs are inconsistent with any provision of FISA - including Section 702.* 14:27

102. Notwithstanding these holdings, Ms. Gorski suggests in her Expert Report that the state secrets privilege has been invoked by the U.S. government in 'challenges to Section 702 surveillance.' This statement is certainly correct so far as it goes, but it skirts over the nature of the substantive claim in the cited case – whether surveillance of the plaintiffs under section 702 violated the Fourth Amendment (a claim not within the purview of FISA itself, and so not covered by FISA's preemption of the state secrets privilege). As described above, an EU citizen challenging U.S. data collection under section 702 would almost certainly base such a claim on a violation of FISA – and not the Fourth Amendment. In such a context, the state secrets privilege should not apply, and I do not read Ms. Gorski's Expert Report as suggesting to the contrary. 14:27

*103. Thus, while it is beyond my purview to take a position on whether the objections raised by the CJEU in its **Schrems** judgment are still present, it is my*

expert opinion that the DPC Draft Decision's assessment of current U.S. remedies for unlawful collection of EU citizens' data from U.S. companies is significantly incomplete, that its analysis of the obstacles posed by 'standing' doctrine is substantially overstated, and that Ms. Gorski's invocation of the state secrets privilege as an additional obstacle is almost certainly inapplicable to the kinds of claims EU citizens might bring in U.S. courts to challenge the unlawful collection of their data." 14:28

Now, I think, Judge, I can move through the remaining affidavits a little bit more rapidly and if you turn to Book 4 there are three other - sorry, four other expert reports that Facebook have tendered. If I can ask you 14:29 to start off by going to Tab 14.

Mr. DeLong, Judge, is a former director of compliance at the National Security Agency and the purpose of his report is to address the value of signals intelligence 14:29 activities to the United States and to other countries. I'm just going to open the summary of his conclusions which you'll find at page 4 paragraph 15. And he explains there:

14:30

"*My report, he says, covers both the purpose and value of signals intelligence activities to the United States and the European Union and its Member States. While noting the 'content of the applicable rules in [the*

United States] resulting from its domestic law or international commitments,' this report is specifically focused on 'the practice designed to ensure compliance with those rules.'

16. Over the past three years the signals intelligence activities of the United States have received intense scrutiny. This report is designed to help better explain and provide context around how NSA conducts signals intelligence activities, what oversight and compliance processes and procedures are in place, and how those processes and procedures work and interact in practice.

17. As further developed in the sections that follow, I make the following major points:

A. Understanding how the scope and effect of safeguards in United States law, policy, and procedures apply to information collected for foreign intelligence purposes requires a detailed analysis of the design, resourcing, and actual implementation of signals intelligence compliance and oversight structures. The U.S. government employs an extensive and layered oversight and compliance structure that includes both programmatic and granular oversight within NSA, within the Executive Branch, and involves all three branches of government. This oversight and compliance structure is rigorous, substantive and contains both directly

embedded roles and those with substantial independence.

B. There is significant benefit from United States signals intelligence activities to the safety, security, and liberty of both the United States and the European Union. There is a strong, and mutual, alignment of interests and demonstrated value. Interlocked with the value, there is a substantial set of overlapping safeguards, based on generally accepted oversight and compliance principles, to protect fundamental rights, including the privacy of digital correspondence. Paraphrasing Jane Harman, a former United States Congresswoman and former member of the House Permanent Select Committee on Intelligence, 'if our intelligence community were to stand down, or if the oversight community were to step aside, we all know the results would be disastrous.'

C. With respect to the transfer of digital information from within the European Union to the United States, ultimately under the control of various private sector companies, the safeguards that govern the United States' signals intelligence activities – and the purposes behind such activities – are numerous in both places and there are mechanisms in place to evolve them over time in light of changes, such as changes in technology. When such information is in the United States, there are additional safeguards for such information when held by corporations. These

safeguards have been underemphasized to date and are more fully noted in this report.

D. Although at first impression various safeguards appear to only apply to United States persons and persons in the United States, in practice those safeguards offer protection to persons regardless of location or citizenship. In addition, in 2014, President Obama issued a new directive, Presidential Policy Directive 28 (PPD-28), which formalized many existing protections, added important additional protections, and provided more transparency to individuals and their governments around the world. Many of the policies specified in PPD-28 have, as a practical matter, been functioning in practice for decades. Their formalization and enhancement in PPD-28 helps to institutionalize those practices for the future, alongside important new protections also formalized in PPD-28.

D. A significant amount of material about signals intelligence activities (in particularly about the '702 Program,' and its parts colloquially known as 'PRISM' and 'Upstream') assumed as fact in the case documents, especially early ones, is simply incorrect. Much of the confusion across the period from 2013 to 2016 derives from the conflation of allegation (such as imagined unilateral 'direct access' by the government to internal computers of companies) and actual findings

of fact (such as interaction between the companies and the government occurring at arms-length through specific legal process). Since then, the U.S. government has declassified hundreds of pages of documents that provide outside observers greater clarity. To the extent possible, this report seeks to correct the record regarding the scope of safeguards and the nature, scope and practice of the signals intelligence activities."

14:34

Then, Judge, if you go forward to paragraph 124, he again summarises and presents by way of conclusion what he has said earlier in the course of his affidavit. He says that:

14:34

"124. Although the specifics and details are critically important, it is equally important to look broadly at the scope and diversity of the safeguards and the critical value of signals intelligence to the safety and security of the United States and the European Union. Even assuming that the United States should be held to higher standard, given its role and size, the full range of safeguards – including law, policy, compliance, oversight, resourcing, and effectiveness of design – are substantial and overlapping taking into consideration the value and benefit from signals intelligence activities.

125. The blanket protection limiting the range of

permitted company interaction with the United States Government, coupled with a limit on the scope of and pathways through which the United States Government can compel companies to provide specific information, coupled with the existing protections from the term 'foreign intelligence,' and even the framework of 702 specifically in involving, in detail, all three branches of the US government in the gathering of foreign intelligence from persons outside the United States is indeed, in many respects, 'extraordinary,' in the best sense of the word.

126. Furthermore, while there have been numerous important changes over the past years, a part of what appears as change over the past years is actually at its core a very important codification of existing practices, such as certain de facto protections that were codified into Presidential Policy Directive 28 in 2014. While at first impression it might be more satisfying to think that major change occurred everywhere, upon farther reflection such consistency with prior practices should give more confidence and comfort to those questioning whether the 'reforms will persist'.

127. Indeed, these reforms were in part implemented to reduce the possibility of fixture risks materializing. As a compliance professional, the additional emphasis was important and is very welcome, but re-emphasis of

existing practice is a stronger pathway to consistency with fundamental safeguards than sudden emphasis on all new safeguards, which would have required a much more significant change in practice.

128. And to close by re-emphasizing a few of the points made in this report, the United States signals intelligence activities provide substantial benefit to both the United States and its allies, in particular the people in the European Union, while going to great lengths (both out of necessity and law) to focus on information that is relevant and necessary to provide safety and security – and avoid information that is not at each step of the signals intelligence process.

129. Signals intelligence is at its core a complicated space – no more or less complicated than - the communications environment it seeks to carefully interact with – and the level of safeguards is designed, implemented, and resourced to directly account for that complexity with very real and positive protection for the fundamental liberties and security at the core of this matter."

Judge, at Tab 17 there's a report of Max-Peter Ratzel. 14:37
He is a former police officer and he worked with the German federal criminal police. He was at a senior management level in that force, he was a policy advisor and senior consultant to the German Federal Ministry of

the Interior. He became a director of Europol and he has worked on behalf of the German government on cooperation projects related to the awareness of law enforcement authorities of complying with European standards with regard to collection and exchanging of personal data.

He has also provided a management summary of his report which is at 10 of 37. Yes. Well in fairness Mr. Gallagher just asks me to draw your attention to the fact that he explains he is a native German speaker and that he has drafted the document in English. He speaks, reads and writes English as well, but I think perhaps some of the phraseology should be viewed in the light of that. 14:37 14:38 14:38

So, Judge, there is a management summary at section 4.

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

MR. MURRAY: That's 10 of 37 so I should open that and he describes these as his major findings and conclusions. 14:38

"*(a) the benefits and necessity of conducting electronic surveillance for the purpose of securing national security and the safety of persons.* 14:38

From my point of view the necessity to conduct electronic surveillance is evident. The three real case examples as rendered below in section 5.2(a) do

indicate the appropriate way forward. Only international connected investigators can successfully counteract international connected criminals, may it be in cases of Serious and Organized Crime or criminal activities by International Terrorists.

** Due to judicial preconditions and meeting legal provisions, the exchange of information must be proportionate at the same time.*

** To protect the citizens, the result of these intrusive measures must also be shared internationally between competent authorities (law enforcement agencies and intelligence services), inside the European Union and abroad, including the US. It goes without saying that this information transfer must be based on legal provisions. As a matter of fact it must be executed by highly qualified staff within the competent authorities, meeting highest standards of information sharing and respecting relevant rules and laws on privacy, data security, confidentiality and integrity. The responsible staff must be well trained, adequately equipped and carefully supervised while exchanging information.*

** The benefits, deriving from that coercive power, are essential for successful police work to prevent crimes to happen or to clarify cases which nevertheless had happened. In addition, the respective perpetrators can be trialed and convicted at the same time - which is an effective special prevention. Altogether, the benefits*

are obvious.

b) the ways (if any) in which restrictions on the transfer of data from the European Union to the US and other countries around the world might affect national security or the safely of persons or properly in the European Union:

** Based on my own practical experiences and exploiting most current open source information, it is clear to me that only the perpetual exchange of relevant data and information is the key to success for law enforcement and intelligence services in the EU MS and in the US likewise. By nature, this exchange must be based on common understanding and mutual trust. These two basic elements for any cooperation and information exchange must exist between the agencies and individual officers likewise, and it shall be supported by according legislation. In so far, judiciary and monitoring authorities shall be involved as well. Solid, relevant and reliable information, in combination with qualified crime analysis, is the strongest weapon of law enforcement and judiciary against criminals. To successfully counteract internationally connected criminal networks, law enforcement agencies and intelligence services must be internationally interconnected as well.*

** All of them must constitute a kind of well connected 'security grid'. Their network of information exchange*

and crime analysis must be widened and intensified at the same time. The archaic principle according to which information is only shared between those who 'need to know' is outmoded. One must share information trustfully and sufficiently early with everyone who is possibly concerned. Only then, you can detect and prevent crime or attacks to happen. The outdated 'need to know' principle must be replaced by the up-to-date 'need to share' principle.

** As the world is nowadays a 'global village', this approach shall not be limited to the EU and the US in future; the exchange of data shall be possible on a global scale. In doing so, one must ensure - e.g. by training and supervision - that the exchange partners' standards in privacy, data protection, confidentiality, integrity and in general policing are adequate to ours, of course.*

** This subtle and fine-spun network of personal relationship, institutional cooperation and trustful information exchange is the backbone of current security and risk assessments.*

** There will be a serious impact on our national security situations if this cooperation and information exchange does not work anymore in future and if the necessary exchange of data between the EU and the US or other countries around the globe will be limited or restricted by stricter laws or any further narrow-minded provisions, not considering the real security challenges. The individual danger and risk*

will increase, not only for countries, but also for regions. This will affect individual citizens' life and property as well."

Then he comments on two documents: Report of the Bulk Powers Review and Operational Case for Bulk Powers, Independent Review, UK government and records his agreement with those. 14:42

There is then, Judge, at Tab 19 an expert report from Joshua Meltzer. He, Judge, is a senior fellow at the Global Economy and Development program at the Brookings Institute and teaches international trade law at the John Hopkins School for Advanced International Studies. He addresses the role of the global movement of data in the context of economic growth and international trade. And his key conclusions are, I think, expressed shortly at paragraph 3 on page 2 of his report where he says: 14:42 14:43

"*The following are my key expert opinions on the economic and trade implications of restricting transfers of personal data from the EU.* 14:43

1. That restrictions on the flow of personal data out of the EU will negatively affect EU economic growth. 14:43

2. That restrictions on the flow of personal data out of the EU will negatively affect EU imports and exports.

3. That restrictions on the flow of personal data out

of the EU will negatively affect foreign direct investment into the EU.

The interrelated way that restrictions on personal data leaving the EU will affect economic growth, trade and investment means the following testimony provides support, he explains, for all these opinions."

Now, Judge, Facebook has filed three affidavits from its own staff. I'll just open one of them at tab, is at this book, I will perhaps open them slightly out of order, but, because it's in this book, if you go to Tab 23. And this is an affidavit of Andrea, I am sure I am getting the pronunciation wrong of Scheley and she is the associate general counsel for Facebook. She addresses a number of propositions which are summarised in her conclusion on page 9 paragraph 40, but just perhaps to identify the headings. 14:44 14:44 14:45

If you turn to page 2, Judge, she explains that Facebook does not participate in any government programme of 'mass' or 'undifferentiated' surveillance, and she elaborates upon that. At paragraph (b) she explains that national security requests reflect a tiny fraction of Facebook accounts and she references at paragraph 12 to bi-annual *"Global Governments Request Report"* which contains a detailed country-by-country breakdown of the number of government requests seeking Facebook user data: 14:45 14:45

"*The Global·Governments Requests Report is free to access.*"

And she refers to extracts from that. And at paragraph 14, she says: 14:46

"*The Global Governments Request Report shows the tiny percentage of Facebook accounts that are actually the subject of U.S. national security requests. For example, reporting for the first six months of 2015 - the latest period for which full figures have been published - shows that less than .0010% of Facebook accounts were the subject of a US national security request for data during this time period. It is stated differently during a representative six month time period, US national security requests sought information relating to less than one account in* a *hundred thousand. To be clear, the figures from the first six months of 2015 are not an outlier. As the reporting shows, Facebook has consistently received a very small number of US national security requests.*"

And she then proceeds to --

MS. JUSTICE COSTELLO: I might just ask you to make a note of something I will ask you to clarify later on. 14:47 I am just wondering how this idea that there are relatively few accounts targeted or captured ties in with the standing arguments where, was it Prof. Vladeck, was saying that post Snowden he thought

that the **Clapper** restrictions mightn't be so tight. Just I will need a little help through that in due course.

MR. MURRAY: Certainly, Judge. And when I come back to --

MS. JUSTICE COSTELLO: Just while it came into my head.

MR. MURRAY: -- the submissions. Absolutely, I will bear that in mind: "*These numbers should also be seen in light of the number of requests received by Facebook from EU member states. In the first six months of 2015, only 16,855 Facebook user accounts were the subject of requests from EU law enforcement. This is greater than the number of user accounts that were the subject of US national security requests over the same period.*" 14:47

And she says that: "*Facebook has consistently sought to correct the erroneous rumour it shares information relating to a large number of its users with the US government. Indeed, far from trying to conceal the number of accounts that have been the subject of national security requests, Facebook has, on more than one occasion, appeared before US federal courts to argue in favour of its right to disclose more information about the number of national security requests it receives from the US Government.*" 14:48

She explains that Facebook joined others in industry in petitioning the FISA court, which has oversight of the

operation of the Foreign Intelligence Surveillance Act, to require the U.S. Government to permit companies to disclose more information about the volume and types of national security rated orders they receive."

14:48

And she then refers to Facebook participating as an amicus curiae in the same context.

She says at (c) Facebook carefully scrutinises law enforcement requests for user data, and she goes through the practices that the company follows in support of that proposition. 14:48

She then, Judge, in the conclusion she says:

14:48

"*Facebook Inc.'s response to government requests by Facebook Ireland user data is addressed by what she describes as the DTPA. "*

You will see that defined at paragraph 3. It is the intra-group agreement between Facebook and Facebook Inc. titled the Data Transfer and Processing Agreement of 20th November 2015: 14:49

"*Facebook Inc has never acceded to any request from any government - including any arm of the US government - for direct, widespread, indiscriminate, or unmediated access to any of its data, including Facebook Ireland User Data. To the extent that the judgment in*

Schrems *suggests the contrary, it is incorrect.*

"The correct facts, she says, were not placed before the court in that case.

A tiny fraction of Facebook's accounts (one account in 100,000 over a six month period) has ever been the subject of a national security request."

14:49

And she refers then to the comprehensive and robust framework Facebook has in place for dealing with these matters.

14:49

I think the principal Facebook affidavit, Judge, is in Book 5 Tab 27 and that's an affidavit of Ms. Cunnane. You'll find that, Judge, as I said, at Tab 27 Book 5.

14:50

So, Judge, I will open this affidavit in full. If you go to, she explains she is the Head of Data Protection and Privacy for Facebook. She is also a solicitor. At paragraph 3 she explains that she makes the affidavit to explain Facebook's use of the SCCs and to detail the relationship between the relevant parties, how the SCCs restrict Facebook's disclosure of the user data to government authorities, the security obligations imposed on Facebook by the SCCs and the remedy and oversight provisions.

14:51

14:51

She says Facebook is a US corporation, established

under the state of Delaware, principal place of business in California. Facebook Inc is a publicly traded corporation. She explains what Facebook Ireland is. And then at paragraph 11 she says this:

14:51

"*11. Facebook Ireland's role as the provider of the Facebook Service outside the US and Canada, and its role as the data controller in respect of Facebook Ireland User Data, is a matter of public record and is documented in Facebook's publicly available terms of service and Data Policy.*"

And she exhibits that:

14:52

"*Facebook Ireland uses a number of service providers to assist it in supplying the Facebook Service. Facebook Inc is one of these service providers. Facebook Inc provides a wide range of services to Facebook Ireland, including technical, engineering, product, research, sales, marketing and human resource services. So as to enable Facebook Inc to provide some of these services, Facebook Ireland needs to transfer Facebook Ireland User Data to Facebook Inc in the US. For example, Facebook Ireland uses certain technical infrastructure services provided by Facebook Inc to provide the Facebook Service.*

13. This transfer is subject to an intra-group agreement between Facebook Ireland and Facebook."

That's the DTPA to which I have just referred:

"*14. The DTPA is based upon the SCCs for the transfer of personal data to processors established in third countries approved by the European Commission. In the DTPA, Facebook Ireland is referred to as the 'data exporter', and Facebook Inc is referred to as the 'data importer'.*

14. The DTPA is based upon the SCCs for the transfer of personal data to processors established in third countries approved by the European Commission in Decision 2010/87. In the DTPA, Facebook Ireland is referred to as the 'data exporter', and Facebook Inc is referred to as the 'data importer'.

15. Under the DTPA, Facebook Inc and Facebook Ireland assume a range of precise obligations which govern the transfer of data between the parties. These obligations protect Facebook Ireland User Data which is transferred to Facebook Inc. Clauses 4(a) to (, judge,) of the DTPA sets out the obligations of the data exporter (here, Facebook Ireland), while Clauses 5(a) to (, judge,) sets out the obligations of the data importer (here, Facebook Inc). These obligations include an agreement and warranty from Facebook Ireland that Facebook Ireland User Data is processed in accordance with Irish data protection law and that

Facebook Ireland has and will instruct Facebook Inc to only process Facebook Ireland User Data in accordance with Irish law. Facebook Inc reciprocally agrees and warrants that it will only process Facebook Ireland User Data in accordance with the instructions it receives.

16. The DTPA imposes additional obligations on Facebook Ireland and Facebook Inc, which are detailed below. Most importantly for the present proceedings, the DTPA addresses Facebook Inc's response to government requests for Facebook Ireland User Data and sets out the security safeguards that Facebook Inc must deploy to keep Facebook Ireland User Data secure. I describe these requirements, and the manner in which Facebook Inc complies with them, from paragraph 26 below.

17. In line with the SCC Decision, the DTPA also contains a robust set of remedy and oversight provisions. These provisions allow individuals, such as Mr. Schrems, to seek redress in the event of a breath of the SCCs and enables the Plaintiff, the Data Protection Commissioner to review and control the ways in which Facebook Inc processes Facebook Ireland User Data. These aspects of the SOCs are outlined from paragraph 40 below.

18. To the best of my knowledge and belief, Facebook

Ireland does not transfer any Facebook Ireland User Data to Facebook Inc in reliance on the SCCs approved by the European Commission in the earlier decisions."

Then she refers then again to the DTPA and quotes at paragraph 21 from Appendix 1, she says: "*It describes the ways in which Facebook Ireland has authorised Facebook Inc to use Facebook Ireland User Data. These include: 'Promoting safety and security (such as using information to verify accounts, investigate suspicious activities or possible violations of terms or policies, or responding to law enforcement, civil law and other legal requests' (Emphasis added). In accordance with this authorisation, Facebook Inc evaluates and responds to US government requests seeking access to Facebook Ireland User Data.*

14:54

22. SCC Decision 2010/87 contains an in-built limitation on the effect of national legislation applicable to data importers, such as Facebook Inc. The SCCs acknowledge that data importers may need to comply with local laws applicable in the jurisdiction In which they operate – so called 'mandatory requirements'. However, this derogation does not extend to all local laws, only those that do not go beyond what is necessary in democratic society."

And she quotes footnote 1 Clause 5 and I think that's been opened to you, Judge, by Mr. Collins:

"*Under the DTPA, only national provisions which 'do not go beyond what is necessary in a democratic society' are to be regarded as true mandatory requirements of national law which can justify a departure from the safeguards.*

24. Further, under Clause 5(b) the DTPA, Facebook Inc agrees and warrants that: 'It has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation, which is likely to have a substantial adverse effect on the warranties and obligations provided by the clauses, it will promptly notify the change to the data exporter."

She then refers to Ms. Scheley's affidavit. She explains at (c) that: "*The DTPA obliges Facebook Inc to deploy an comprehensive security programme.*" And she quotes the relevant provisions. 14:56

Then over the page, Judge, at heading (d) she explains that the DTPA restricts the ways in which Facebook can provide user data to third party subprocessors. She says: 14:56

"*Facebook Inc. is restricted by the DTPA with regard to*

its subprocessing arrangements. These restrictions are a core aspect of the security provided by the DTPA and ensures that Facebook Ireland User Data continues to enjoy equivalent protections to those contained in the DTPA when it is passed to a service provider for subprocessing."

Quotes Clause 11 of the DTPA. And over the page, Judge, at paragraph 35 says this:

"*35. As a result of the DTPA, Facebook Inc can only engage third party subprocessors to process Facebook Ireland User Data in circumstances where those third parties are engaged pursuant to a contract which imposes the same obligations on the subprocessors as are imposed on Facebook Inc under the DTPA. The DTPA, and by extension SCC Decision 2010/87, ensure that Facebook Ireland User Data continues to enjoy protection even in cases where a third party may have access to that data in the course of providing a service to Facebook."*

She refers then to the sample sub-processing agreement and refers to relevant provisions from it.

14:57

At paragraph 37: "*Facebook Inc. imposes stringent requirements on subprocessors. In particular, Clause 2(d) of Exhibit C of the subprocessing agreement requires that the subprocessor will 'promptly notify*

the data importer about:
i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited under criminal law to preserve the confidentiality of a law enforcement investigation;
ii) any accidental or unauthorised access; and
iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so'.

38. Furthermore, Clause 3 of Exhibit C of the subprocessing agreement provides that any data subject who has suffered damage as a result of any breach of the obligations in Clause 1 or Clause 8 by any party or subprocessor is entitled to receive compensation from the data exporter (i.e. Facebook Ireland) for the damage suffered. Pursuant to Clause 4 of Exhibit C, the data subject is entitled to refer an action for damages to the courts of Ireland, or to refer the dispute to mediation by an independent person, or where applicable, the supervisory authority (i.e. the Commissioner).

39. Through subprocessing agreements of this sort, which are required by SCC Decision 2010/87, Facebook Inc takes steps to ensure that Facebook Ireland User Data continues to enjoy proper protection, even in cases where such data is provided to third party service providers for subprocessing."

She then says: "*40. The DTPA incorporates remedies that can be pursued by individual data subjects in the event that they believe their data protection rights, as guaranteed by the DTPA, have been breached.*"

She then says: "*In the first instance the DTPA, in line with the requirements of SCC decision 2010/87 contains a third party beneficiary clause. Clause 3(1) provides that certain provisions of the DTPA, including those relevant to law enforcement access and data security, may be enforced by the data subject against the data exporter (i.e. Facebook Ireland). To facilitate the data subject in asserting such third party rights, Clause 3(4) of the DTPA provides that the parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes.*"

Clause 6 addresses damages. It provides: "*Any data subject who has suffered damage as a result of a breach of the obligations of Clause 3 or 11 by a party or subprocessor is entitled to recover compensation. Facebook Ireland may be liable to its users in damages should Facebook Inc. fail to deploy or comply with the safeguards required by the DTPA. And, if Facebook Ireland ceased to exist, data subjects could seek damages from Inc.* 14:59 14:59

43. Pursuant to Clause 7, the data subject is entitled to pursue his or her action to enforce third party beneficiary rights and/or a claim in damages in the courts of Ireland, as Ireland is the jurisdiction in which Facebook Ireland, the data exporter, is established.

44. In addition to a right to pursue an action to enforce third party rights and/or a claim in damages, the DTPA also provides the data subject with the option of referring a dispute to mediation."

Then refers to the powers that are given to the Commissioner to investigate and control the manner in which the data is processed. 15:00

Then, Judge, the last affidavit is at tab 25 in the same book.

MS. JUSTICE COSTELLO: Do we not have two? Is there a Chris Bream as well as Michael Clarke? 15:00

MR. MURRAY: Yes, that's tab 25, Judge.

MR. GALLAGHER: And there's Clarke as well.

MS. JUSTICE COSTELLO: Oh, Prof. Clarke, that's a different one, is it? Okay.

MR. MURRAY: Mr. Gallagher has reminded me, 15:00 I'd forgotten there's another expert, Prof. Clarke, who's a defence expert. I'll open Mr. Bream's affidavit and come back to Prof. Clarke's, Judge - they're in the same book.

Mr. Bream is Facebook's Security Director, Judge, and he details the steps that are taken by the company to prevent unauthorised access to Facebook users' information by third parties, including government authorities, and he addresses the steps taken to protect what he describes as state sponsored attacks and hacking.

15:01

I'll just perhaps identify, if you turn to paragraph six, he records that:

15:01

"*Facebook is not aware of any unauthorised US government searches of its servers or information in the United States. In addition, Facebook does not provide the US government with access to its servers or information in the United States. However, the US government has a right to request information from Facebook, pursuant to the legal processes described in the affidavit of Andrea Scheley, which I have reviewed...*

7. We are aware of numerous attempts by agents of other countries (so called 'state sponsored actors") to compromise our systems. As a result, we have deployed a particularly sophisticated, and constantly evolving, security programme which is specifically designed to deal with security threats posed by sovereign states and their proxies."

Then over the following paragraphs, Judge, he outlines the security measures that are taken and they're there. He concludes at paragraph 75 with a short summary of what they are -- or, sorry, a short summary of what he has explained in the preceding paragraphs. He reiterates he's not aware of any unauthorised US Government searches of its information, pursuant to the DPA, he refers to the extensive and detailed security safeguards and that it has an extensive and comprehensive security programme, the details of which are outlined in that affidavit. 15:02 15:03

Then, Judge...

MR. GALLAGHER: There is the supplemental affidavit. 15:03

MR. MURRAY: There is the supplemental affidavit of that same --

MR. GALLAGHER: It was handed in, but you probably won't have it convenient, Judge. 15:03

MS. JUSTICE COSTELLO: I don't have it in the right place, no (Same Handed).

MR. GALLAGHER: Yeah, exactly.

MR. MURRAY: He just explains, Judge, there, if you go to paragraph four, that in paragraphs 29 and 30 he uses the term "network traffic" in the context of Facebook's use of the HTTPS security programme and he explains that the use of that term refers exclusively to data in transit between the user and Facebook or 15:03

vice versa, the point where it's first received by Facebook and not stored data or data in transit between the Facebook sites. And then he explains --

MS. JUSTICE COSTELLO: Can you just assist me again; remind me what HTTPS stands for again? 15:03

MR. MURRAY: Well, Judge, if you go to paragraph 29 of the affidavit, the principal affidavit at tab 25.

MS. JUSTICE COSTELLO: Yes.

MR. MURRAY: At paragraph 29 he explains that 15:04
Since July 2013, Facebook has encrypted network traffic between users and Facebook's service by using what it describes as this protocol, the HTTPS protocol...

MS. JUSTICE COSTELLO: Mm hmm.

MR. MURRAY: ... by default in order to 15:04
defeat attempts by governments or hackers to eavesdrop or tamper with its traffic. So, Judge, just to go back to the supplemental affidavit.

MS. JUSTICE COSTELLO: Yes. Thank you.

MR. MURRAY: "*Similarly*", he says, "*at* 15:04
paragraph 30 I use the terms 'Facebook data networks' the same with 'fibre optic cables over which user communications transit' and the term 'data which users send to Facebook in the same sense'. Paragraphs 29 to 32 must be read in that light." 15:04

Then:

"*Finally, I refer to 'data transmitted from users to*

Facebook'. Again for the avoidance of doubt, I clarify I that here too the explanation set out above applies equally in this context. Therefore, when I discuss Facebook's use of PFS in paragraphs 33 to 36, I mean that even if the TLS keys were compromised, they could not be used to decrypt any traffic that had not previously been captured while in transit."

And as is obvious from there, Judge, those terms similarly refer to the encryption. 15:05

Michael Clarke, Judge, at tab 32. He's a Professor of Defence Studies at Kings College, London. And he addresses also the need for electronic surveillance. And there is -- at the conclusion of his report on page 20, paragraph 49, he says that it's his belief, with such a range of activities being conducted online, it would be impossible for the security and intelligence agencies or law enforcement authorities to try to counter their operations offline. 15:05 15:06

"*It is also my belief that intercepting the communications of criminals, terrorists and espionage groups through electronic means is, in principle, necessary insofar as this is a modern day equivalent of traditional policing techniques such as legitimately tapping a telephone or trailing a suspect to ascertain with whom they communicate. As patterns of electronic communication activities have evolved for all in the*

digital society, so, it is my belief, it is necessary that security and policing agencies should be able to operate in the same space.

50. Throughout EU member states data collection, interception and processing by the SIAs/LEAs must be conducted on the basis that such activities are deemed lawful, necessary and proportionate. As the foregoing has shown, however, the implied intrusion of the SIAs/LEAs both into the depth and width of the electronic fabric of a digital society as they go about their work is necessarily great. It is my belief that of the three pre-conditions, the advent of digital society across the EU makes the judgement of what is proportionate *in any given operation significantly more difficult to determine.*

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

He then says:

"*52. Notwithstanding any potential threats to privacy and civil liberties in Europe, it is my belief that the material outlined in the foregoing analysis indicates that significant restrictions on the transfer of material between EU member states and other countries would be highly damaging to the common pursuit of western societies to combat serious transnational crime and international terrorism. This is evident in two particular ways.*

Collection of material through transnational operations

53. It is evident from the foregoing analysis that transnational intelligence operations are inherently involved in accessing a great deal of communications and content data, and are particularly fundamental to the acquisition of bulk data and interception. It is difficult to see how existing interception powers could be effectively maintained if they could only be applied within a single jurisdiction. The current regime to manage different jurisdictions in this respect is through the Mutual Legal Assistance Treaties (MLATs). But they are widely regarded as unsatisfactory and too slow in practical operational terms when the agility of the criminal and terrorist threats is evident. A lack of more standardised processes, training and common guidance between the parties to MLATs - in particular

between some EU states and the US, all wait to be addressed by more cooperative international action.

54. As reactions to the Snowden revelations demonstrated, criminal and terrorist groups are alert and agile to all the technical and legal restrictions under which SIAs and LEAs in democratic and open societies operate. Both Al Qaeda and ISIS were reported to have changed their communication methods and other operational procedures in light of their reading of the Snowden material. This characteristic agility is expected to increase as the internet evolves further. Of the 40% of the global population that currently has access to the internet, Europe and North America now account for less than half of the total and this trend will grow as internet usage expands quickly in India, China, Africa and Latin America.

55. It is my belief that continuing cooperation, on a case by case basis, between SIAs/LEAs in individual countries and as wide a range of internet companies as possible, both large and small, is the only way forward in present circumstances for western societies to stay abreast of the transnational challenges they face from criminal and terrorist activities. Any significant restrictions on the current ability of SIAs and LEAs to cooperate with each other and with internet companies would, at the very least, make intelligence cooperation less agile in the face of highly agile adversaries, and

to that extent threaten the security and wellbeing of European, and other, societies.

Sharing of material and cooperation between the EU and other countries

56. The sharing of material that has been separately obtained by individual national security and intelligence agencies is equally critical to the current campaigns against criminality and terrorism among the democracies. The important variable is that which is shared. The SIAs and LEAs across the EU have different levels of surveillance capability and all operate in differing political environments. Nevertheless the relationships between the agencies of the major EU players in these respects - France, Germany, the Netherlands, Spain, the UK - and those of the United States are very important. In particular, the US and the UK have a very close and cooperative intelligence-sharing relationship that is unique within the EU-US context. The 'FiveEyes' intelligence-sharing arrangement encompasses the intelligence agencies of the US, Canada, the UK, Australia and New Zealand. It is a unique international arrangement, based on long operational experience and cumulative trust between the participants and is reportedly a mechanism for the transfer of the most sensitive intelligence 'raw material' in the world.

57. The EU and the US have created better information-sharing arrangements since 2010 covering, in particular, terrorist financing, foreign fighters, container security and irregular migration. Extradition procedures have been simplified. Information is now shared primarily through the Secure Information Exchange Network Application (SIENA), a platform for law enforcement cooperation between EUROPOL, EU member states and third parties that have agreements with EUROPOL, including the US. The US is EUROPOL's largest partner in the number of joint cases conducted, and the Federal Bureau of Investigation contributes the highest volume of information to the EU. Following the terrorist attacks on the continent in 2014 and early 2015, other deals were concluded. In February 2015, the US signed two new agreements with EUROPOL related to irregular migration and 'foreign fighters'; providing a platform for member states to share information on facilitators of foreign fighter travel and recruitment, as well as their sources of financing. Individual programmes between the EU and the US have clearly been useful to both sides of the Atlantic. The Terrorist Finance Tracking Programme, for example, is said to have provided over 16,700 intelligence leads since it was launched in 2010.

58. Nevertheless, 'sharing information' can cover many different levels of practical cooperation. Partners may offer assessments, summaries or even specific

terror alerts or practical leads in casework. There is no substitute for 'raw material' however, of the sort that communications interception provides. This is partly because every intelligence agency works to its own protocols and will treat and assess raw material a little differently, and partly because countries all have their own distinctive intelligence priorities. They ideally need the ability to draw their own most relevant conclusions from raw material rather than assessments pre-digested by another agency that will exist in a different policy environment.

59. In the event of restrictions on the existing levels of transfer of communications, content or bulk data between EU countries and the US, such sharing arrangements outlined above would undoubtedly continue and might even be enhanced. But in my opinion restrictions on the transfer of raw data between the EU and the US, and particularly between the UK and the US, would be seriously damaging to the quality of the transatlantic intelligence relationship. The agencies of EU countries would lose more access to raw data than would US (and Canadian) agencies, since the US generates far more data than any of its European counterparts. In my judgement, this would inhibit the present work of the SIAs/LEAs inside the EU and reduce their effectiveness in defending the national security and safety of people and property inside the EU."

Judge, we have then two final expert reports which are prepared for the Plaintiff, and both of them appear in book two. The first is at tab three and it's Mr. Serwin's supplemental memorandum. I think when Mr. Collins was opening the case, he opened the first --

MS. JUSTICE COSTELLO: Sorry, just a moment, I need to check this. Book two. I've got, tab one is the affidavit and then the -- the first report is at tab two and then tab three you say is the second report? 15:14

MR. MURRAY: Yes, that's right.

MS. JUSTICE COSTELLO: The thing is, I've just -- oh, I've just got a swearing page.

MR. MURRAY: Yeah, there's an exhibit sheet.

MS. JUSTICE COSTELLO: And it's behind the swearing page, yes. 15:14

MR. MURRAY: So I think Mr. Collins explained when he opened the first report of Mr. Serwin that there was a supplemental memorandum which he'd come back to at the conclusion of his opening of the other affidavits. 15:14

So he explains, Judge, that this memorandum, in the introduction, serves as a supplement to Morrison and Forester's May 24th memorandum and he says that the May 24th memo and this supplement provide a non-exclusive overview of private remedies available to EU citizens under federal law in the US against certain entities and individuals for alleged violation of data privacy 15:14

arising from the gathering of personal information in the context of national security.

He says that the memorandum doesn't opine on the effectiveness of the remedies for the purposes of Article 47, or on whether causes of action will be appropriate in a particular circumstance. 15:15

He then looks at the **Schuchardt** case, which was referred to in, I think, Prof. Vladeck's advice. He says: 15:15

"*After the May 24, 2016 Memo was completed, a federal circuit court issued an opinion in* [that case] *involving a constitutional challenge to an electronic surveillance program operated by the National Security Agency ('NSA'). The case analyses Article III standing in the context of a plaintiff who alleged that the United States Government was 'intercepting, monitoring and storing the content of* all or substantially all *of the e-mails sent by American citizens', including presumably the plaintiff's. The allegations made by the plaintiff were based in no small part upon the allegations made by Edward Snowden, which built upon prior public disclosures regarding alleged government monitoring. In the context of a motion to dismiss, the United States Government argued that the plaintiff's allegation was insufficient to establish a claim.*

For the purposes of a motion to dismiss, the court held that the plaintiff had adequately pleaded standing, but stated that its holding was narrow and the court explicitly stated that this did not mean that the plaintiff actually had *standing to sue. The court also noted that rulings on this question in other circuits varied depending on several factors, including the procedural posture of the case. In other words, as noted in the cases cited in footnote 7 of this memorandum, the burden imposed upon the plaintiff to establish Article III standing varies depending on when in the case, and how, the defendant challenges standing, which is why the court noted that its holding was narrow. Thus, although this case may appear, at first blush, to indicate a lower threshold for pleading Article III standing in this circuit, it does not change the fact-intensive and circuit-specific nature of these determinations, and this does not alter the conclusion that a plaintiff must still meet his or her burden to show sufficient harm under Article III.*

The plaintiff... also suggested that he was entitled to jurisdictional discovery, which is used to uncover jurisdictional facts. The court, however, cautioned that '[j]urisdictional discovery is not a license for the parties to engage in a 'fishing expedition', and that fact is particularly true in a case like this one, which involves potential issues of national security'.

Notably, the plaintiff in Schuchardt based his claims on excerpts of classified materials that were the focus of public reports, some of the reports themselves, and affidavits filed in other cases. These reports appeared to be important to the court analysis, and without such public disclosures regarding alleged surveillance, it could be more difficult for a plaintiff to bring suit.

The discussion of [the case] *illustrates a broader point regarding Professor Vladeck's views of Article III and my views in the May 24, 2016 Memo. Professor Vladeck and I broadly agree on Article III, and to the extent there are differences in our views, they are differences that largely result from a difference in emphasis in which cases one relies upon, and what the procedural posture is of those cases (given the sliding scale of the burden on plaintiffs noted above). In discussing Article III standing, Professor Vladeck acknowledges Clapper... in which the US Supreme Court found that the plaintiffs lacked standing to challenge the constitutionality of FISA. He also expresses his personal concerns regarding this decision.*

Both the May 24, 2016 Memo and this supplemental memorandum analyse Clapper and Article III standing in light of the recent Supreme Court decision in Spokeo -v- Robin, a case finding that a plaintiff in a case alleging a statutory violation of the Fair Credit

Reporting Act could not establish standing, which is consistent with a narrower reading of Clapper. It will remain to be seen what bearing Spokeo, which is not a national security case, has in the national security context on the Article III analysis.

In addition to the standing requirement, a plaintiff would have to consider the obligation to satisfy [Rule 11]. *Professor Vladeck's affidavit at page 29, footnote 28, asserts that the May 24, 2016 Memo conflates two distinct ideas - that Rule 11 'requires a good faith basis for the claims alleged in a proceeding', and that the fact of an EU citizen's surveillance 'would likely be classified and difficult to prove'. I respectfully submit that Professor Vladeck has misinterpreted the argument. The May 24, 2016 Memo simply notes that, particularly in a case where there has been no public disclosure regarding the alleged surveillance, it could be difficult for a plaintiff to argue that a good faith basis existed for their claim. The memo concludes: 'It remains to be seen how the Rule 11 requirements in conjunction with the Judicial Redress Act will be implemented...', and this remains all the more true in light of Spokeo.*

The district court in Schuchardt essentially noted this issue when it assessed Article III standing: 'On the other hand, courts have refused to find standing based on naked averments that an individual's communications

must have been seized because the government operates a data collection program and the individual utilized the service of a large telecommunications company.' Simply put, if a case is simply based upon 'naked averments', particularly where there is no public disclosure of a future data collection programme the pre-filing Rule 11 burdens must at least be considered before the case is filed.

Professor Vladeck asserts in his affidavit that the May 24, 2016 Memo should have addressed a claim under Section 702 of the Administrative Procedure Act. The APA has been used in certain cases, notably ACLU -v- Clapper, and that case is important to consider as an illustration of the APA Section 702 claim.

It is first important to note that remedies under APA Section 702 exist only for '[a]gency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court...' The APA was not 'designed to expand the jurisdictional foundations of the federal courts. Rather, [it] merely provide[s] additional remedies and procedures where jurisdiction has already been conferred by statute.' Where other statutes provide adequate remedies, the APA is unavailable. The alternate remedy 'need not provide relief identical to relief under the APA, so long as it offers relief of the "same genre".'

While the APA Section 702 claim has been used in cases where individuals directly seek relief, it is a claim that has faced some mixed results for plaintiffs in the national security context. As discussed below, courts have found that they are precluded from reviewing at least some claims involving intelligence gathering practices by the United States Government. Furthermore, circuit courts have had mixed views on whether a plaintiff in the national security context can establish that monitoring is 'final agency action' under the APA, which in one case precluded relief against the United States government for allegedly intercepting oversees communications.

The case cited by Professor Vladeck, ACLU -v- Clapper, presented a unique fact pattern in which the ACLU and other non-profit civil rights organizations challenged a telephone metadata program that was being conducted pursuant to... Section 1861. Section 1861 'allows the Director of the FBI or his designee to "make an application for an order requiring the production of any tangible things... for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities".' The plaintiffs only became aware of the government order in this case when a newspaper published a leaked government order directing the production of appellant's call records.

The court considered whether the plaintiffs were precluded from bringing suit to challenge the telephone metadata program via the APA. Although the APA establishes a right of judicial review of administrative action, it does not apply where statutes preclude judicial review. The court noted that... Section 2712, the first cause of action I examine in the May 24, 2016 Memo, explicitly withdrew the right to sue under the APA for certain government actions involving surveillance. Because the specific cause of action alleged by the plaintiffs in Clapper was not mentioned in Section 2712, and because the legislative history did not explicitly withdraw the right to sue the United States Government under this section, the court found that the plaintiffs had a right of action under the APA. Highlighting the unique circumstances of this case, the court further stated that in enacting Section 1861, 'Congress assumed, in light of the expectation of secrecy, that persons whose information was targeted by a Section 215 order would rarely ever know of such orders, and therefore that judicial review at the behest of such persons was a non-issue'. Nonetheless, under the circumstances of this case where the Section 1861 order was leaked to the public, judicial review came into question. The court vacated the lower court's judgment dismissing the complaint, but declined to conclude that a preliminary injunction was required.

In contrast, at least one other court considering this same issue found that it lacked jurisdiction to hear plaintiffs' APA claim challenging the Section 1861 order. The court there concluded that Congress did *intend to preclude APA claims in these circumstances. In holding that judicial review was precluded, the court stated that Congress had 'created a closed system of judicial review of the government's domestic foreign intelligence gathering' under the FISA provisions in question, and that this system 'include[d] no role for third parties'*."

And he's referring there to the **Klayman -v- Obama** case.

15:24

"*As demonstrated*", he says on page six, "*by the varying opinions issued by United States courts, the APA Section 702 claim faces several challenges beyond the Article III challenges that resulted in the dismissal of the complaint in Clapper... Moreover, it is important to note that the cases permitting APA claims under Section 702 in these circumstances* predated *the Judicial Redress Act ('JRA'). As noted in the May 24, 2016 Memo, the JRA extends certain remedies under the Privacy Act to EU citizens, and these remedies were not available for EU citizens at the time of Clapper, and the other published APA Section 702 cases, including the ability to bring suit in federal district court for certain Privacy Act violations by the US federal*

government relating to the sharing of law enforcement information. It is beyond the scope of this supplemental memorandum to assess the adequacy of remedies, but a US court certainly could consider whether the enactment of the JRA provides sufficient relief 'of the same genre' to make relief under APA Section 702 inappropriate.

In conclusion, the APA Section 702 claim has had a mixed history in the national security context. It will remain to be seen whether, or what kind of, role it has going forward given the existing remedies, the extension of certain of the Privacy Act remedies to EU citizens under the JRA, as well as the new redress available under Privacy Shield, which is discussed below."

And he then addresses the Privacy Shield:

"After the May 24, 2016 Memo was prepared, the United States and the European Union entered into the *EU-US Privacy Shield. Since other experts have covered Privacy Shield in some detail, I will focus my comments on the creation of an Ombudsperson. I would also note that Privacy Shield is not directly within the scope of my opinions, since they are, as noted above and in the May 24, 2016 Memo, confined to 'non-exclusive overview of private remedies available to EU citizens, under federal law in the United States'. Privacy Shield was*

significant enough, however, that I felt that it should be covered in some manner.

Professor Swire correctly observes that '[t]he EU-US Privacy Shield created new remedies against the US government available to EU persons. The Privacy Shield creates an Ombudsman within the US Department of State who can hear complaints from EU data subjects related to US government actions'. Professor Swire is also correct when he observes that the Ombudsperson is intended to be independent of the US national security services and, notably, that the Ombudsman has authority not just under Privacy Shield regarding these matters, but also under BCRs, as well as SCCs.

As noted in Annex A: EU-US Privacy Shield Ombudsperson Mechanism, the Ombudsperson is intended to undertake a number of functions, including:

** Effective Coordination - the Privacy Shield Ombudsperson will be able to effectively use and coordinate with the oversight bodies, described below, in order to ensure that the Ombudsperson's response to requests from the submitting EU individual complaint handing body is based on the necessary information. When the request relates to the compatibility of surveillance with US law, the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers.*

** Receive complaints from the EU individual complaint handling body and then conduct an initial review, track the status of requests and provide appropriate updates, as well as provide a timely and appropriate response to the submitting EU individual complaint handling body, as more fully discussed in Exhibit A.*

There is also a process that permits requests for further action where a request alleges a violation of law or other misconduct.

The scheme establishes new avenues by which a complainant can seek redress. It will remain to be seen how these new remedies will operate once implemented, particularly since Privacy Shield offers redress that appears to be in some ways different than the more traditional judicial remedies."

Then, Judge, the last report/affidavit is that of Mr. Richards, which you'll find at tab six. Now, he is a Professor of Law at Washington University School of Law, a graduate of the University of Virginia Law School. He's a particular interest in privacy information law. He's published widely on the topic, and you'll see his CV and indeed his list of publications at tab seven. He's published a book on intellectual privacy published by the Oxford University Press and a widely cited article dealing with the

15:25

15:28

decision of the Supreme Court in **Clapper**, which was published in the Harvard Law Review.

Judge, if you turn to paragraph five on page two, he summarises his opinion as follows. He says: 15:28

"*It is my opinion that there is substantial evidence to support the conclusions of the DPC Draft Decision and the Serwin Memorandum that EU citizens lack meaningful avenues of legal relief to remedy violations of their data protection and privacy rights in the US. Moreover, I believe these conclusions are correct interpretations of the state of US law at present. US privacy remedies are indeed fragmentary and suffer from individual deficiencies; they also have to surmount the general obstacle of standing doctrine, which appears to be becoming more stringent, especially in privacy cases. In addition, having reviewed the Privacy Shield framework, particularly the new Privacy Ombudsperson mechanism, I do not find that this program provides a legal remedy that changes my conclusion. All I can say at the present time is that it is distinct from a judicial redress scheme, and beyond that it is not possible to say what, precisely, it will deliver.*"

Then, Judge, if you'd go forward to paragraph 33 - in the intervening paragraphs he's summarised the DPC decision and explained the context. And on page 11 -- sorry, perhaps if I ask you to go back to paragraph 32

on page ten. He's dealing with his finding and expert reasons, "Data Protection Remedies Available to US Citizens Under US Law". He says:

"*The DPC Draft Decision noted that while EU citizens had some remedies under US law, '[f]rom a specific perspective, the remedies are fragmented, and subject to limitations.*"

And that passage, I think, has been already opened to you. He then says: 15:30

"*In this section of my report, I canvas what I believe to be the most important and most relevant judicial remedies, and discuss their contexts, elements, and limitations. In particular, insofar as the DPC Draft Decision reflects or takes account of the Serwin Memorandum, I have reviewed that Memorandum and its conclusions for accuracy and completeness.*"

Then he says:

"*As the DPC noted, unlike the EU and virtually all other industrialized Western democracies, the US does not have a comprehensive data protection statute... As Professors Solove and Schwartz put it in their leading casebook and treatise on privacy law, 'Numerous statutes are directly and potentially applicable to the collection, use, and transfer of personal information*

by commercial entities. Congress's approach is best described as "sectoral", as each statute is narrowly tailored to particular types of businesses and services. The opposite of sectoral in this context is omnibus, and the United States lacks such a comprehensive statute regulating the private sector's collection and use of personal information. Such omnibus statutes are standard in much of the rest of the world. All member nations of the European Union have enacted omnibus information privacy laws'."

He continues:

"Data protection law in the United States is thus a complex web of, among other things, constitutional law rules binding the government, incomplete sector-specific federal statutes, state law statutes and common-law rules. In my opinion, these facts support the DPC's conclusion that US privacy law remedies are 'fragmented' rather than general. Indeed, in my own scholarship I have argued that 'American law governing surveillance is piecemeal, spanning constitutional protections such as the Fourth Amendment, statutes like the Electronic Communications Privacy Act of 1986 (ECPA), and private law rules such as the intrusion-into-seclusion tort. But the general principle under which American law operates is that surveillance is legal unless forbidden... Plaintiffs can only challenge secret government surveillance they

can prove, but the government isn't telling. Plaintiffs (and perhaps civil liberties) are out of luck'... This paragraph, taken from the introduction of an article I published two weeks before Edward Snowden's revelations about the US government's surveillance activities in June 2013, reaches essentially the same conclusion about remedies and standing under US law as the DPC Draft Decision of May, 2016. The review of the relevant US legal doctrines which follows explains this conclusion in greater detail."

He then says:

"*There are at least two rights recognized under the US Constitution that could provide avenues for relief for EU citizens whose personal data has been gathered in the context of national security by the US government: The Fourth Amendment and the constitutional right of information privacy. I note that my analysis on these points goes beyond that of the Serwin Memorandum, which was directed to federal statutory causes of action.*"

He then quotes the Fourth Amendment and he explains that it protects privacy of communications. And at 15:33
paragraph 38 -- sorry, he explains in the last sentence of paragraph 37:

"*In these areas, the Foreign Intelligence Surveillance*

Act is usually considered to serve as the regulation and remedy of first instance.

38. Another obstacle to Fourth Amendment relief is the so-called 'Third-Party Doctrine'. This is the highly-controversial idea that information loses its Fourth Amendment protection when it is shared with a third party such as a telephone company... or a bank... The doctrine remains a matter of substantial criticism and debate, and at least one Justice on the current Supreme Court has called for the Court to reexamine it...

39. With respect to the third party doctrine, the federal government has long maintained that stored e-mails, which are communications shared with a telecommunications company, are within the third-party doctrine, though this proposition was flatly rejected by a federal appeals court in 2010... The federal government did not seek to appeal that case to the Supreme Court, and as a result, the rule in Warshak is only binding in the handful of American states governed by the ruling of that regional court (Kentucky, Michigan, Ohio and Tennessee). Whilst I believe that the Supreme Court would likely ratify the result in Warshak were it to hear a case squarely presenting the issue, the constitutional protection of e-mails in the United States remains unclear at present. (I agree with the Vladeck Report at 27 in this respect).

40. When the Fourth Amendment has been violated by the government, the normal remedy is the exclusion of evidence obtained in violation of the Constitutional rule from a criminal trial. However, since Fourth Amendment violations can happen outside the context of the investigation of criminals, the Supreme Court has also held that there exists an implied private right of action to protect all Americans against deprivations of Fourth Amendment rights by the federal government...

41. It remains unclear, however, whether a Fourth Amendment Bivens action is available to foreign claimants who lack substantial connections to the United States... As Professor Vladeck points out, 'U.S. courts have been hostile to Bivens claims in the national security context - so that such remedies may be formally *available to individuals with Fourth Amendment rights, but have at least thus far proven almost categorically unavailable to them in practice'."*

And he quotes Prof. Vladeck there in an article of his and refers to another case, **Turkmen -v- Hasty**, recognising a **Bivens** claim arising out of the allegedly unlawful conditions of confinement of immigration detainees in a national security case. 15:36

"*As Professor Vladeck further notes, the Supreme Court's grant of certiorari in Turkmen -v- Hasty may*

resolve this important question. At present, however, a Bivens claim under the Fourth Amendment does not seem to be one which is broadly open to EU citizens to effectuate privacy and data protection rights under Articles 7 and 8 of the European Charter against the US government.

Moreover, the Supreme Court will also hear a case this Term regarding the extraterritorial application of the Fourth Amendment stemming from a police shooting that occurred across the US-Mexican border, Hernandez -v- Mesa... It is thus fair to say that US law is unclear at present regarding whether an EU citizen (who is not a permanent resident of the United States) can bring a constitutional action for an alleged violation of her Fourth Amendment rights.

42. Another potential remedy for EU citizens might lie in the federal constitutional right of information privacy, which is a controversial offshoot of the even more controversial constitutional right of privacy recognized by the Supreme Court in Griswold -v- Connecticut... and Roe -v- Wade... In the case of *Whalen -v- Roe... the Supreme Court seemed to recognize such a right in obiter dictum in the context of a state database of prescription records, and while some lower federal courts have recognized the right, its existence to this day is a matter of some scholarly and judicial debate. In its two subsequent cases raising the*

doctrine, the Supreme Court has assumed without deciding the existence of the right, but then found that the right was not violated under the facts of each particular case. Accordingly, it declined to recognize the right explicitly...

There are several federal statutes that could potentially provide avenues of relief for EU citizens challenging the collection, use, and disclosure of their data by the federal government for national security purposes."

And then he begins with the Privacy Act/the Judicial Redress Act:

"*44. Although as noted above, the United States does not have a general data protection statute, it does have a sectoral data protection statute governing information held by the federal government. The Privacy Act of 1974 applies broadly to 'records' about an 'individual' held in a 'system of records'... which are protected by (among other things) a rule of nondisclosure... Violations of the Privacy Act are enforced by a variety of civil remedies, including injunctive relief... and in the case of an 'intentional or willful' violation, actual damages with a minimum recovery of $1,000, costs, and reasonable attorney fees...*

45. The Serwin Memorandum explains the remedies available under the Privacy Act, as extended to non-US persons under the Judicial Redress Act. I have read and examined the analysis set out in the Memorandum and its conclusions. I am satisfied that its analysis is both complete and well founded, and I agree with its conclusions. I also concur with the views expressed in the Memorandum to the effect that the remedies to be accessed under the Judicial Redress Act, in particular, are subject to limitations (both actual and potential) that are material in their nature and extent. I offer the following additional observations on those remedies.

46. One point in which I would like to amplify the Serwin Memorandum's discussion is its reference on page 5 to the Supreme Court's cutting back on the damages remedy under the Privacy Act in recent years. In Doe -v- Chao... the Supreme Court held in a case involving a Privacy Act claim that 'actual damages' under the Privacy Act needed to be proven in order for a plaintiff to recover the statutory minimum damages of $1,000. In the more recent case of FAA -v- Cooper... however, the Court held that as a matter of statutory interpretation, the Privacy Act remedy for 'actual damages' could not include damages claims for mental and emotional harm, and that plaintiffs seeking Privacy Act damages must show 'pecuniary harm' in order to recover. This was the case, in the Court's view,

because the Privacy Act, by authorising damages actions against the sovereign, constitutes a waiver of sovereign immunity, which must be strictly construed in favor of the government and against private plaintiffs. The decision occasioned a passionate (and to my mind, legally correct) dissent by three Justices led by Justice Sotomayor, but after Cooper, it is clear that the Supreme Court does not appear inclined to expand damage claims under the Privacy Act. As I interpret the majority opinion in Cooper, I have further doubts whether that Court would recognize the deprivation of European fundamental rights of privacy as 'actual damages' under the Privacy Act, on the ground that they were dignitary rather than pecuniary."

He then just refers in footnote one that, in connection with **Cooper**, he agrees with Prof. Vladeck's observation that the strict limitation on the availability of damages doesn't disturb the availability of injunctive relief against the government. 15:40

"*However*", he says, "*in my opinion, this does not invalidate the DPC's specific conclusion in section 59(9) of her Draft Decision that these developments mean that 'a requirement to prove pecuniary loss or damage will also operate as a precondition to the availability of particular remedies under the JRA'... Many violations of the rights of privacy and data protection under both the European (as I understand*

them) and traditional American views are nonpecuniary, but Cooper seems to foreclose them almost entirely."

He then says:

"*The Privacy Act's general rule of nondisclosure is subject to twelve statutory exceptions... three of which I would like to highlight. First, the Act exempts 'routine uses' of data by an agency. This allows the disclosure of a record for any 'routine use' if disclosure is 'compatible' with the purpose for which the agency collected the information in the first place... This is a very broad exception that, in the minds of many distinguished scholarly and practical commentators on privacy law, has the potential to be the proverbial exception that swallows the rule. For example, Paul Schwartz has noted that 'Federal agencies have cited this exemption to justify virtually any disclosure of information without the individual's permission'.*"

Then he has a quotation to similar effect:

"*The Privacy Act limits use of personal data to those officers and employees of the agency maintaining the data who have a need for the data in the performance their duties. This vague standard is not a significant barrier to the sharing of personal information within agencies... No administrative process exists to*

control or limit internal agency uses. Suits have been brought by individuals who objected to specific uses, but most uses have been upheld... The legislation left most decisions about external uses to the agencies, and this created the biggest loophole in the law. An agency can establish a 'routine use' if it determines that a disclosure is compatible with the purpose for which the record was collected. This vague formula has not created much of a substantive barrier to external disclosure of personal information... Later legislation, political pressures, and bureaucratic convenience tended to overwhelm the law's weak limitations. Without any effective restriction on disclosure, the Privacy Act lost much of its vitality and became more procedural and more symbolic."

"48. A second statutory exception in the Privacy Act disclosure bar is that for law enforcement. The Act excludes disclosures 'to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains (the record specifying the particular portion desired and the law enforcement activity for which the record is sought'...

49. A third exception to the rule of nondisclosure in

the Privacy Act allows individual agencies to follow a procedure to exempt systems of records if those records are (a) kept by the Central Intelligence Agency or (b) 'maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws'. As the Serwin Memorandum details, the NSA has taken advantage of this procedure, and further exempted records classified under its collection powers authorized by Presidential executive orders... Quoting a blog post by former Bush White House Official Tim Edgar, the Vladeck Report explains that this provision makes sense in that it would be counter-productive to allow domestic or international criminals and terrorists the ability to access their own NSA files... I agree with this conclusion, with the caveat that there is a difference between keeping targeted surveillance secret, and keeping entire surveillance programmes secret. It is my opinion that, under the best traditions of American constitutionalism, a democratic citizenry should have the right to know and consent to the broad contours of government surveillance that are engaged in by the state in their name...

50. As it was originally enacted in 1974, the Privacy Act (and thus its remedies) only applied to US persons. The definition of 'individual' in the statute is 'a citizen of the United States or an alien lawfully

admitted'... By its terms, then, the Privacy Act does not apply to EU citizens who are resident in Europe.

51. The Judicial Redress Act, signed by President Obama... has the potential to expand the remedies available to US 'individuals' to EU citizens... The Serwin Memorandum explains the remedies available under the Judicial Redress Act and offers opinions on its limited utility. I am satisfied that the analysis in the Serwin Memorandum is both complete and well-founded... The Judicial Redress Act grants the US Secretary of State the functional power to designate foreign nationals as US 'individuals' within the meaning of the Privacy Act, and thus to open up its remedies to those foreign nationals, including, in some cases, damages. To my knowledge, neither the EU (nor any Member State) has to date been so designated. However, even were such a designation to be made in the future (which I believe is quite possible, at least in part), because the Privacy Act is a limited statute due to its many exceptions, and because many of the records potentially at interest in these Proceedings have been exempted... it is difficult for me to envision that the Judicial Redress Act would be a vehicle for the kinds of effective litigation contemplated by the CJEU and the DPC... at least as I understand the meaning of those terms in Schrems I.

52. In particular, the exemption of government

surveillance records from the Privacy Act discussed above makes the Privacy Act a very poor vehicle for EU citizens to vindicate their fundamental rights... As Mr. Edgar continues in the blog post quoted above, '[p]retending that providing Privacy Act rights to EU citizens responds to European concerns about redress for targets of PRISM and other intelligence programs is not going to fool anyone. It will take more fundamental - and much more difficult - changes to surveillance law to address the EU's concerns about redress'."

Then he looks at the ECPA and the SCA. He says:

"*The Fourth Amendment to the US Constitution... protects the privacy of communications and other areas of human activity against unreasonable searches and seizures... Although the Supreme Court initially held, for example, that telephone calls were not protected by the Fourth Amendment because wiretapping was a non-physical intrusion... the Supreme Court reversed this position four decades later, holding in Katz... that wiretaps required a warrant. The following year, Congress passed the federal Wiretap Act...*

54. A few years later, the Supreme Court decided the case of United States -v- United States District Court... In this case, involving a warrantless wiretap of alleged domestic terrorists, the Court held that the

Fourth Amendment applied to regulate investigation of domestic threats to national security, though it held out the possibility that Congress might be able to create different rules than Title III for intelligence-gathering cases that might nevertheless satisfy the Fourth Amendment.

55. The Electronic Communications Privacy Act ('ECPA') was passed in 1986 to update the old Wiretap Act... The Serwin Memorandum explains the remedies available... I am satisfied that its analysis is both complete and well-founded, and I agree with its conclusions."

And he offers further thoughts on it. 15:46

"*57. ECPA is a detailed and highly complex statute, but its relevant provisions can be summarized succinctly. Title I of ECPA provides for extensive protection of the 'contents' of wire, oral, and electronic communications against both government and private interceptions. Title I of ECPA requires the government to obtain a warrant to intercept the contents of communications, has minimisation procedures, and violations of Title I are enforceable by criminal prosecution and civil penalties including a private right of action for substantial damages. The ordinary private right of action is not available against the United States. Section 2520 (providing for a right of*

action for 'any person *whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation'). Title I also has a statutory exclusionary rule for illegally-intercepted wire or oral (but not electronic) communications...*

58. Title II of ECPA, the 'Stored Communications Act', provides for government access to stored communications and telecommunications company customer data under a variety of standards. Unlike Title I, however, Title II has a private right of action, which provides that '[a]ny person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title" - or of the sections that are identified there - "*may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119... the Court may assess as damages (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs...*

59. Title II of ECPA also allows the government the ability to obtain the contents of stored wire and electronic communications from a telecommunications

company without notice to the customer who is the subject of surveillance if it obtains a warrant... Delayed notice is also available under 18 USC Section 2705. In April 2016, Microsoft Corporation filed a lawsuit against the federal government challenging these provision for secret notice on First and Fourth Amendment grounds. It argued that it had received over 2,500 secret orders over the previous 18 months, and that 68 per cent of these orders called for indefinite secrecy of the search. The case is currently pending in federal district court in Seattle."

In fact I think a decision has been handed down in that case very recently, on 8th January, which granted the government -- sorry, dismissed the government's motion to dismiss in part; in other words, it maintained part of the case intact. 15:49

"*(In full disclosure, I should note that I signed an amicus brief on behalf of a group of law professors supporting Microsoft's claim that the Stored Communication Act provisions... are unconstitutional). Microsoft brought the lawsuit in this case in part on behalf of its customers, because government's orders obtained pursuant to the secrecy provisions of the Stored Communications Act purportedly prevent those customers from ever learning about the surveillance, much less seeking a remedy against it, except perhaps when they might be prosecuted for illegal activity*

discovered through the surveillance."

Then he refers to an article addressing that.

"*60. ECPA was a remarkably far-sighted statute passed by Congress to (in effect) regulate e-mail before most people had even heard of the technology. However, thirty years on, ECPA is showing its age, as many of the technological assumptions that undergirded the statute have changed. This can lead to some absurd results. The Microsoft litigation just discussed illustrates one such case. Another example is that the Stored Communications Act provides for lower protection for the contents of electronic communications stored for over 180 days... In an age of telephone answering machines, modems, and magnetic tape, this distinction might have made some sense, but in the age of cloud computing and storage and instantaneous networking, it is not only problematic, but also arguably inconsistent with the Fourth Amendment. It is my opinion that most American lawyers working in this field agree that ECPA needs to be reformed, but cannot agree on the standards that should regulate privacy and law enforcement access to electronic information. In any event, the overuse of secret orders makes it hard for people whose electronic data is accessed under ECPA to challenge it (especially the majority of people who are not charged with crimes), and the 'willfulness' requirement in its remedy against the government is a material obstacle to*

relief."

Then he explains the background to FISA, which the court has already had outlined to it. And if you turn to paragraph 63, he references the Serwin memorandum. He says it's complete and well-founded and he agrees with it. He then says: 15:51

"*64. There are several causes of action for the unlawful use or disclosure of information obtained by a FISA surveillance order, which are laid out in the Serwin Memorandum. To this description I would add only three additional comments. First, these causes of action do not cover unlawful collection (although ECPA does regulate unlawful collection of electronic information generally). Second, in order to be actionable, an unlawful use or disclosure (or for that matter, a collection) must be known, which can be a challenge when dealing with secret government electronic surveillance. This challenge is compounded by the fact that the Supreme Court has recognized in its standing doctrine cases... that separation of powers considerations have led to a stricter application of standing requirements in the foreign affairs context.*"

And he refers to **Clapper**.

"*Third, the causes of action only apply to unlawful*

uses or disclosures that are 'willful', which is still an uncertain standard, despite the fact that the statutes have been on the books for years.

65. The expert reports adduced by Facebook in this case explain at length the sources of authority for US government surveillance of personal data of Europeans and the legal and policy safeguards that exist in the United States concerning this data... In particular, they explain that while the scope and authority of NSA electronic surveillance is broad, there exist numerous limitations and safeguards under US law. For example, the Vladeck Report notes seven such constraints: 'Legal constraints on collection, including built-in limits and those required by the Fourth Amendment, Executive Order 12333, and PPD-28; Legal constraints on the use and retention of collected information, including built-in limits and those required by the Fourth Amendment, Executive Order 12333, PPD-28, and federal statutes such as the Privacy Act; Robust internal constraints on access to the collected data; Internal oversight through agency Inspector General and Privacy and Civil Liberties Offices; External oversight by the PCLOB; External oversight by the House and Senate Intelligence and Judiciary Committees; and Ex ante and ongoing judicial supervision through judicial review'...

The Swire Report also goes into great detail regarding

US privacy law... The Vladeck and Swire Reports thus provide substantial evidence to support their contention that US Government surveillance is not unconstrained, and exists within the rule of law. By contrast, the Gorski and Butler Reports acknowledge these legal structures but have a more pessimistic conclusion about the level of constraint they impose in practice...

66. Given the scope of the opinion I have been asked to give in these Proceedings, I do not wish to wade into this debate in this Report because, in my opinion, this issue is complex, nuanced, but critically, it is not directly responsive to the question of remedies that I have been asked to address. Article 47 of the Charter guarantees European citizens a 'right to an effective remedy before a tribunal'. In my mind, external and internal safeguards are a very important element of law in general and privacy law in particular, but (in US constitutional law at least) they are analytically distinct from fundamental rights.

67. There is one substantive observation, however, I would like to make about the safeguards which operate to constrain government surveillance in the United States. In their reports, Professors Vladeck and Swire articulate and explain, in great detail, the various legal and policy safeguards that constrain surveillance by the US government. However, it is important to note

that many of these safeguards are contingent on the discretion of the President of the United States or other officials in the Executive Branch. Thus, while I agree with Professors Vladeck and Swire that American surveillance law has become more privacy-protective since the Snowden Revelations of June 2013, many of these protections are merely administrative rules, and a significant portion of these are politically contingent and thus quite fragile. For example, the President must appoint and the Senate must confirm a new Chair of the Privacy and Civil Liberties Oversight Board who is committed to civil liberties (which was an unfilled position from 2007-13 and is currently once again empty after its first chair, David Medine, stepped down in July 2016). The current or a future President also has the ability to amend, expand, or repeal executive orders such as Executive Order 12333 and the Presidential Policy Directive 28. In the American system of government as (so I understand) in the European, fundamental rights are not fundamental if they are contingent on the discretion of elected officials. (See, in agreement, the Robertson Report at 2960). I am reminded of the conclusion of Chief Justice John Roberts in the Supreme Court's most recent digital privacy case, in which he agreed that privacy-protective agency procedures by law enforcement were '[p]robably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols'... In that case, the Supreme Court

went on to extend the protection of the Fourth Amendment - a true fundamental right - to the contents of mobile phones seized incident to arrest.

68. The Serwin Memorandum discussed several other potential federal causes of action, including the Freedom of Information Act...; the Computer Fraud and Abuse Act...; and the Right to Financial Privacy Act... I am satisfied that its analysis is both complete and well-founded, and I agree with its conclusions."

He then proceeds, Judge, to address the standing doctrine and refers to the Plaintiff's draft decision. And at paragraph 70 he says:

"*As I understand the DPC's 'general objection', it is that Article 47 of the Charter requires that an effective remedy before a tribunal exists. Further, I understand that the DPC's interpretation of European law is that because an individual remedy under US Law requires a plaintiff to satisfy the elements of standing doctrine, 'these requirements appear to be incompatible with EU law in circumstances where, as a matter of EU law, it is not necessary to demonstrate an adverse consequence as a result of an interference with Articles 7 and 8 of the Charter in order to secure redress of a violation of the said articles'...*

71. In the 2013 Harvard Law Review article (as noted

above, published shortly before the Snowden disclosures of June of that year) about the dangers that unregulated and under-regulated government surveillance poses to democracy, I argued at the outset that, from an American perspective '[a]lthough we have laws that protect us against government surveillance... secret government programs cannot be challenged until they are discovered. And even when they are, our law of surveillance provides only minimal protections. Courts frequently dismiss challenges to such programs for lack of standing, under the theory that mere surveillance creates no harms. The Supreme Court recently reversed the only major case to hold to the contrary, in Clapper... finding that the respondents' claim that their communications were likely being monitored was "too speculative."'"

He then explains, Judge, in paragraph 72 - and you've heard, I think, this before - the separation of powers in US constitutional law and the relationship between that and the standing doctrine. He quotes from Article III of the Federal Constitution and identifies, at paragraph 75, a number of allied doctrines that have also been related to those separations of powers considerations. 15:57

Then at paragraph 76 he says:

"*Standing doctrine is derived from the textual*

commitment in Article III Section of the judicial power to (and as interpreted only to) enumerated classes of 'Cases' and 'Controversies'. In order to ensure that a suit before the court presents a case and controversy and that the plaintiff has 'standing' to bring a claim before the court that the court is able to adjudicate, the doctrine requires that the plaintiff establish three elements. In the absence of any one of these elements, the court lacks jurisdiction to entertain the claim because (so the logic goes) it would not be deciding a 'case or controversy'. In his leading treatise on constitutional law, Dean Erwin Chemerinsky explains further:

'The [Supreme] Court has said that some of these requirements are constitutional; that is, they are derived from the Court's interpretation of Article III and as constitutional restrictions they cannot be overridden by statute. Specifically, the Supreme Court has identified three constitutional standing requirements. First, the plaintiff must allege that he or she has suffered or imminently will suffer an injury. Second, the plaintiff must allege that the injury is fairly traceable to the defendant's conduct. Third, the plaintiff must allege that a favourable federal court decision is likely to redress the injury'...

77. These three constitutional standing requirements -

injury in fact, causation, and redressability - are reflected in the DPC Draft Decision.

78. I must explain at the outset that beyond stating this three-part test identifying coherent principles that run through the American law of standing can be very difficult. The doctrine is frequently confusing and indeterminate and open to charges that the Justices (and lower court judges) are in practice if not in intent manipulating what is supposed to be a procedural doctrine in order to affect the substantive merits of legal disputes."

Then he goes back to the text he's been quoting from and he says: 15:59

"*Standing frequently has been identified by both justices and commentators as one of the most confused areas of the law. Professor Vining wrote that it is impossible to read the standing decisions 'without coming away with a sense of intellectual crisis. Judicial behavior is erratic, even bizarre. The opinions and justifications do not illuminate'. Thus, it is hardly surprising that standing has been the topic of extensive academic scholarship and that the doctrines are frequently attacked. Many factors account for the seeming incoherence of the law of standing. The requirements for standing have changed greatly in the past 40 years as the Court has*

formulated new standing requirements and reformulated old ones. The Court has not consistently articulated a test for standing; different opinions have announced varying formulations for the requirements..."

Then he continues at paragraph 79:

"*In making this observation... I am not attempting to suggest that standing doctrine is incoherent (though, to be fair, a substantial number of critics of the doctrine do believe this). My point is merely that, beyond the broad conceptual outlines of the doctrine, the standing cases in privacy law as elsewhere in American law can be difficult to predict or restate. This is as much a challenge for litigants presenting claims that push near the boundaries of the doctrines as it is for academics, practicing attorneys, and judges who seek to understand or apply it*".

MS. JUSTICE COSTELLO: I think you might want to break there. 16:00

MR. MURRAY: Very good, Judge.

MS. JUSTICE COSTELLO: And it's a cheery thought to think I've to decide as a matter of fact what that all means.

MR. MURRAY: Yes. Well, we'll explain it tomorrow, Judge. 16:00

MS. JUSTICE COSTELLO: Eleven o'clock.

MR. GALLAGHER: Thank you, Judge.

MR. MURRAY: Thank you, Judge.

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

2

3

4

5

B

C

D

F

G

H

I

J

K

L

M

N

O

P

T

U

V

W