## 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 THURSDAY, 9th FEBRUARY 2017 - DAY 3

3

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

| | |
|---|---|
| 1 | **THE HEARING RESUMED AS FOLLOWS ON THURSDAY, 9TH** |
| 2 | **FEBRUARY 2017** |
| 3 | |
| 4 | **MS. JUSTICE COSTELLO:**  Good morning. |
| 5 | **REGISTRAR:**  Matter at hearing, Data Protection |
| 6 | Commissioner -v- Facebook Ireland Ltd. and another. |
| 7 | **MR. MICHAEL COLLINS:**  May it please you, Judge.  Judge, |
| 8 | it occurred to me that there were two other decisions |
| 9 | I should have mentioned to you in the context of |
| 10 | standing and I just want to deal with those as briefly |
| 11 | as I can before moving on to the Privacy Shield. |
| 12 | |
| 13 | If I could ask you to look at Book 2 of the US law |
| 14 | materials, and at Tab 19 there's a case called, I'm not |
| 15 | sure if I have the pronunciation is right, **Schuchardt** |
| 16 | **-v- The President of the United States**. |
| 17 | |
| 18 | This is, if you look at the synopsis first, Judge, the |
| 19 | background: |
| 20 | |
| 21 | "*Attorney brought action alleging that* |
| 22 | *electronic surveillance program operated by National* |
| 23 | *Security Agency (NSA) under Foreign Intelligence* |
| 24 | *Surveillance Act (FISA) violated Fourth Amendment by* |
| 25 | *intercepting, accessing, monitoring, and storing all or* |
| 26 | *substantially all of his e-mails.  The United States* |
| 27 | *District Court for the Western District of Pennsylvania* |
| 28 | *granted government's motion to dismiss, and attorney* |
| 29 | *appealed.* |

10:43

10:43

10:44

10:44

1     *The Court of Appeals, Hardiman Circuit Judge held that*

2     *[1] the injuries allegedly sustained by attorney were*

3     *sufficiently personal to support his standing to bring*

4     *suit, and*

5     *[2] attorney's claim that program intercepted,*

6     *accessed, monitored, and stored all or substantially*

7     *all e-mails sent by American citizens was sufficiently*

8     *plausible to support his standing to bring action."*

9

10    If I bring you forward in the opinion of the court,          10:45

11    Judge, to page 14 in the left-hand column, under the

12    heading 3 or the number 3, the court says:

13

14    "*The Government raises three principal arguments*

15    *challenging the plausibility of Schuchardt's PRISM*          10:45

16    *allegations.  First, it argues that Clapper and its*

17    *application by the D.C. Circuit in Klayman require us*

18    *to find his allegations implausible.  We disagree.*

19    *Two aspects of Clapper distinguish it from this case.*

20    *First, because the Clapper plaintiffs raised a facial*

21    *constitutional challenge to Section 702 on the day the*

22    *statute was enacted, they pleaded only prospective*

23    *injury, i.e. 'potential future surveillance'.  And*

24    *because that 'potential' relied on a 'speculative chain*

25    *of possibilities', the Supreme Court concluded that*

26    *they had failed to satisfy the imminence and*

27    *traceability element of injury-in-fact under Article*

28    *III.  Here, in contrast, Schuchardt's alleged injury*

29    *has already occurred insofar as he claims the NSA*

6

seized his emails.  It is therefore not surprising that
the Government has been unable to formulate an
analogous 'speculative chain' that would
doom Schuchardt's constitutional standing.

Another critical distinction between this case and
Clapper is that the district court entered summary
judgment, a procedural posture that required the
plaintiffs to identify a triable issue of material fact
supported by an evidentiary record.  In contrast,
Schuchardt sought to avoid dismissal in a facial
jurisdictional challenge raised under Rule 12(b)(1),
which requires him only to state a plausible claim, a
significantly lighter burden."

I think that's the equivalent of our striking out for
disclosing no reasonable cause of action or something
similar.

"This distinction in the standard of review is also
reflected in cases concerning national security
surveillance from our sister courts.  Compare ACLU
(plaintiffs had standing on motion to dismiss);
Jewel, (same), with Klayman, plaintiffs lacked
standing to pursue preliminary injunction because there
was no 'substantial likelihood' that they could
establish injury-in-fact, observing that summary
judgment imposes a 'lighter burden" than the
'substantial likelihood of success' necessary to obtain

7

a preliminary injunction); _ACLU -v- NSA_, plaintiffs
failed to establish injury-in-fact on summary judgment
because they had 'no evidence' on various points of
causation).  Here, Schuchardt has gone beyond mere
allegations to survive a motion to dismiss by creating
a limited evidentiary record to support his
allegations.

The Government's reliance on _Klayman_ is also misplaced.
There, the D.C. Circuit vacated the district
court's preliminary injunction, holding that the
plaintiffs had failed to demonstrate a substantial
likelihood of success on the merits.  However, the
panel split on the issue of the plaintiffs' standing,
and also disagreed on whether to remand the case for
further proceedings or outright dismissal."

The plaintiffs according to opinion of Brown J had
satisfied:  "_The 'bare requirements of standing'; in
the opinion of Williams J, plaintiffs lacked standing
to seek preliminary injunction, remanding
for jurisdictional discovery and so on._

_Under these circumstances it seems clear to us that
Klayman's persuasive force is minimized by its
splintered reasoning, different procedural posture, and
the fact that the D.C. Circuit addressed itself to a
now defunct surveillance program authorized by a
separate provision of FISA.  Accordingly, neither_

8

1    *Clapper* nor *Klayman* supports the Government in this
2    case.
3
4    *Second, the Government contends that Schuchardt's*
5    *allegations 'say at most that the government may*
6    *have the capability to seize and store most electronic*
7    *communications,' but '[t]hey do not say that the*
8    *government is searching or seizing most, let alone all,*
9    *e-mail.'  We agree that Schuchardt's alleged*
10   *facts — even if proven — do not conclusively establish*
11   *that PRISM operates as a dragnet on the scale he has*
12   *alleged.*
13
14   *The language of the leaked materials Schuchardt relies*
15   *on is imprecise.  The use of the term 'direct' in the*
16   *NSA's presentation could mean, for example, that the*
17   *Government has complete discretion to search all*
18   *electronic information held by a company participating*
19   *in PRISM at will; this would certainly be consistent*
20   *with the 'real-time' interception capability that the*
21   *NSA allegedly possesses, and could qualify as an*
22   *unconstitutional 'seizure' of all information stored on*
23   *the company's servers.  On the other hand, 'direct'*
24   *could mean."*
25
26   And I think they are referring to material that was
27   used in the original Snowden disclosures, there were
28   various slides describing the operation of the PRISM
29   programme, for example.

9

1    *"On the other hand, 'direct' could mean that the*
2    *Government merely has the legal authority to compel*
3    *participating companies to turn over 'communications*
4    *that may be of foreign-intelligence value because they*
5    *are associated with the e-mail addresses that are*
6    *used by suspected foreign terrorists.'  In that*
7    *scenario, it is implausible that Schuchardt's*
8    *communications would be targeted by PRISM.*
9

10   *At this early stage of legislation, however, Schuchardt*
11   *is entitled to any inference in his favour that may be*
12   *reasonably drawn from his pleaded facts.  And as we*
13   *have explained, the inference that PRISM 'collects all*
14   *or substantially all of the e-mail sent by American*
15   *citizens,' is one supported by his pleaded 'factual*
16   *matter.'  Accordingly, in this procedural posture, we*
17   *cannot accept the Government's preferred inference.*
18

19   *Finally, the Government disputes the notion that PRISM*
20   *is a dragnet, i.e. that it is 'based on the*
21   *indiscriminate collection of information in bulk.'*
22   *According to the Government --"*
23

24   Sorry, the reference there is quoting the, I forget the
25   PCLOB, I forget what the acronym stands for, Privacy
26   Civil Liberty Oversight Board I think:
27

28   *"According to the Government, 'the program consists*
29   *entirely of targeting specific persons that may be of*

1    *foreign-intelligence value because they are, for*

2    *example, associated with the e-mail addresses that are*

3    *used by suspected foreign terrorists."*

4

5    And it gives, there is a debate then about the extent    10:50

6    of that.

7

8    If I move over the page, Judge, to page 16 the last

9    page I want to refer to:  "*The problem for the*

10   *Government at this stage is that the scope of materials*   10:50

11   *that a court may consider in evaluating a facial*

12   *jurisdictional challenge raised in a motion under*

13   *Rule 12(b)(1) is not unconstrained.  As with motions*

14   *under Rule 12(b)(6), the court is limited to the four*

15   *corners of the complaint."*    10:50

16

17   That's what we would call the Statement of Claim.

18   **MS. JUSTICE COSTELLO:**  what does it mean by *facial*

19   jurisdiction?

20   **MR. MICHAEL COLLINS:**  I think they mean *on its face,*    10:50

21   Judge; in other words, like taking a statement and

22   saying 'on its face does it amount to a cause of action

23   recognised in law' or whatever it may be.

24

25   "*The court is limited to the four corners of the*    10:50

26   *complaint, 'documents integral to or explicitly*

27   *relied upon in the complaint,' and 'any undisputedly*

28   *authentic document that a defendant attaches if the*

29   *plaintiff's claims are based on the document.'*

11

1     *Schuchardt's pleadings are in no way based on any*

2     *countervailing authorities that support the*

3     *Government's position, nor are those authorities*

4     *integral to or explicitly relied upon by his*

5     *complaint—accordingly, we must ignore their persuasive*

6     *value, whatever it may be, at this stage of the*

7     *litigation.  Likewise, insofar as the Government's*

8     *arguments present new information disagreeing with the*

9     *factual premises underlying Schuchardt's claims, we*

10     *cannot consider them in this facial jurisdictional*

11     *challenge, the sole purpose of which is to test the*

12     *legal sufficiency of the plaintiff's jurisdictional*

13     *averments.  Instead, disagreements concerning*

14     *jurisdictional facts should be presented in a*

15     *factual challenge, at which time the court, after*

16     *allowing the plaintiff 'to respond with evidence*

17     *supporting jurisdiction,' may fully adjudicate the*

18     *parties' dispute, including the resolution of any*

19     *questions of fact."*

20                                          10:51

21 In other words they were saying take the pleadings on

22 their face, if in fact he is alleging facts if they are

23 ultimately proved which amount to saying 'all his

24 e-mails have been seized', that would be a sufficient

25 allegation to justify the necessary standing.  And they  10:51

26 make that clear in the next paragraph, Judge, because

27 they go on to say:

28

29     *"Our decision today is narrow: we hold only that*

12

1     *Schuchardt's second amended complaint - that's the*
2     *pleading - pleaded his standing to sue for a violation*
3     *of his Fourth Amendment right to be free from*
4     *unreasonable searches and seizures.  This does not mean*
5     *that he has standing to sue, as the Government remains*
6     *free upon remand to make a factual jurisdictional*
7     *challenge to Schuchardt's pleading.  In anticipation of*
8     *such a challenge, we provide the following guidance to*
9     *the District Court on remand."*
10                                                              10:52

11    And they go on to deal with that which I don't need to
12    deal with.  So it's a very narrow decision obviously in
13    terms of the standing issue.
14
15    The other case I want to refer to, Judge, is at Tab 27   10:52
16    in that book, and I'm going to deal with this very
17    briefly.  It's **Wikimedia Foundation -v- NSA**.  It's a
18    decision of the United States District Court for the
19    District of Maryland, which I think is under appeal.
20                                                              10:52
21    The memorandum opinion says:  "*This is the latest in a*
22    *recent series of constitutional challenges to the*
23    *National Security Agency's data gathering efforts.  In*
24    *this case plaintiffs, nine organizations that.*
25    *Communicate over the Internet, allege that the NSA's*
26    *interception, collection, review, and storing*
27    *Of plaintiffs' Internet communications violates*
28    *plaintiffs' rights under the First and Fourth*
29    *Amendments and exceeds the NSA's authority under the*

13

1    *Foreign Intelligence Surveillance Act.  Typical of*
2    *these challenges to the NSA's surveillance programs is*
3    *defendants' threshold jurisdictional contention that*
4    *plaintiffs lack Article III standing to assert their*
5    *claims.  This memorandum opinion addresses the standing*
6    *issue."*

7

8    Then it sets out who the organisations are, various
9    public interest and journalistic operations, non-profit
10   organisations and so forth.  There is then a useful          10:53
11   summary, Judge, which I'm not going to read, although
12   you may wish to read it yourself, which sets out
13   perhaps the background to the FISA Act and the
14   legislation that we have been discussing and its
15   describes the PRISM and Upstream programmes and so           10:53
16   forth.

17

18   On page 8 it begins to discuss Article III and the
19   standing and jurisdictional issues.  On page 10 it
20   discusses **Clapper -v- Amnesty International**, another     10:53
21   one of the case involving Mr. **Clapper** who I think until
22   recently was the Director of National Security
23   Intelligence, although there is a new nominee but not
24   yet confirmed and there is acting director I think
25   operating in the interim.                                    10:54

26

27   On page 14, Judge, at A they set out the arguments as
28   to why they say **Clapper** doesn't control:

29

14

1    *"Plaintiffs first argue that __Clapper__ does not control*
2    *here on the ground that the legal standard in this case*
3    *is different from the legal standard applicable in*
4    *__Clapper__ because the standing challenge in the present*
5    *case arises on a motion to dismiss rather than, as in*
6    *__Clapper__, on a motion for summary judgment.  To the*
7    *extent this argument refers to the difference between*
8    *reliance on factual allegations and reliance on a*
9    *factual record, plaintiffs are undoubtedly correct.*
10
11   *The Supreme Court has made clear that, because the*
12   *elements of standing are 'an indispensable part of the*
13   *plaintiff's case, each element must be supported in the*
14   *same way as any other matter on which the plaintiff*
15   *bears the burden of proof, i.e. with the manner and*
16   *degree of evidence required at the successive stages in*
17   *litigation.'  At the summary judgment stage, a*
18   *plaintiff cannot rest simply on allegations, but must*
19   *'set forth' by affidavit or other evidence 'specific*
20   *facts'; at the motion to dismiss stage, however,*
21   *'allegations of injury resulting from defendant's*
22   *conduct may suffice'."*
23
24   In other words if you brought a motion to dismiss for
25   no cause of action, you look at the allegations, but on     10:55
26   summary judgment you look at the actual substance of
27   the facts as alleged.
28
29   *"But to say the evidentiary basis is different is not*

15

1    *to say that the standing requirements change at each*

2    *successive stage.  They do not.  The means by which a*

3    *plaintiff establishes a standing - by allegation or by*

4    *record evidence - change but the three elements of*

5    *standing - actual injury, causation and redressability*    10:55

6    *- remain constant."*

7

8    And he goes on to discuss the familiar authorities then

9    in relation to that.

10                                                                10:55

11   On page 16 he says:  "*The plaintiffs next argue that*

12   *__Clapper__ does not control this case because more is now*

13   *known about Section 702 surveillance, including*

14   *Upstream surveillance, than was known at the time of*

15   *__Clapper__."*                                              10:55

16

17   And they set out some of the allegations and so on that

18   are made in relation to the surveillance.

19

20   On 17 the court says:  "*The plaintiff's series of*         10:55

21   *allegations does not establish Article III standing*

22   *because those allegations depend on suppositions and*

23   *speculation, with no basis in fact, about how the NSA*

24   *implements Upstream surveillance."*

25                                                                10:56

26   And they then go on to discuss the detail of that and

27   I don't think I need to take time in relation to that.

28

29   On page 20 paragraph C says:  "*Plaintiffs further*

16

1    *allege that __Clapper__ does not control here because newly*

2    *disclosed information reveals that Upstream*

3    *surveillance is fundamentally different from the*

4    *surveillance at issue in __Clapper__. Specifically,*

5    *Upstream surveillance involves the use of 'about*

6    *surveillance', which the NSA allegedly uses to review*

7    *every portion of everyone's communications - a broader*

8    *mode of surveillance than the targeted surveillance of*

9    *particular individuals' communications that was at*

10   *issue in __Clapper__."*                                    10:56

11

12   As I understand it, Judge, about surveillance is that

13   if you are targeting, say, somebody who has a

14   particular name, you might, in a targeted sense, you

15   would look for the communications, the e-mails between    10:56

16   myself and Mr. Gallagher let's say. But an *about*

17   communication or about surveillance would encompass,

18   not e-mails necessarily from me to Mr. Gallagher or

19   vice versa, but e-mails from two other parties in which

20   either my name or Mr. Gallagher's name was referred to    10:57

21   in the body of the e-mail, that the e-mail would be

22   *about* that person and, if you take the *about* type of

23   surveillance, that's clearly a wider type of

24   surveillance.

25                                                              10:57

26   *"The Plaintiffs contend that 'about surveillance' is*

27   *the 'digital analogue of having a government agent open*

28   *every piece of mail that comes through the post to*

29   *determine whether it mentions a particular word or*

17

1  *phrase.  The analogy is inapt; contrary to plaintiffs'*
2  *contention the publicly disclosed documents on which*
3  *plaintiffs rely do not state facts that plausibly*
4  *support the proposition that 'about surveillance'*
5  *involves examining every portion of ever copied*                    10:57
6  *communication."*
7
8  And again they discuss that issue and decide that
9  doesn't give them standing.
10                                                                        10:57
11  At D on page 21:  "*Plaintiffs next argue that* **Clapper**
12  *does not control here because plaintiffs are different*
13  *from the* **Clapper** *plaintiffs in important respects*
14  *concerning their internet communications."*
15                                                                        10:57
16  And it goes on to deal with details of some of the
17  individual parties which again I'm not going to deal
18  with.
19
20  On page 28 under IV, it says:  "*Plaintiffs further*               10:57
21  *allege actual injury on the ground that Upstream*
22  *surveillance undermines plaintiffs ability to carry out*
23  *activities crucial to their missions (i) by forcing*
24  *them to take burdensome measures to minimize the chance*
25  *that the confidentiality of their sensitive information*   10:58
26  *will be compromised and (ii) by reducing the likelihood*
27  *that individuals will share sensitive information with*
28  *them."*
29

18

1     And it goes on to say, they were the same arguments in

2     *Clapper* and the Supreme Court had rejected those

3     arguments.  Then on page 29:

4

5     "*A final point raised in Clapper merits mention here:*

6     *whether the standing requirement as applied in Clapper*

7     *bids fair to immunize Section 702 and Upstream*

8     *surveillance from judicial scrutiny.  This concern is*

9     *misplaced.  To be sure, no government surveillance*

10    *program should be immunized from judicial scrutiny, and*

11    *indeed Section 702 and Upstream surveillance have no*

12    *such immunity.  As the Clapper majority noted, Section*

13    *702 surveillance is reviewed when: (i) the FISC reviews*

14    *targeting and minimization procedures of general*

15    *surveillance practices to ensure, inter alia, 'the*

16    *targeting and minimization procedures comport with the*

17    *Fourth Amendment', (ii) criminal defendants prosecuted*

18    *on the basis of Section 702 surveillance challenge the*

19    *validity of that surveillance, and (iii) electronic*

20    *communications service providers who are directed to*

21    *assist the government in surveillance challenge the*

22    *challenge the Directives before the FISC.*"

23

24    And you will recall those three areas from yesterday.

25                          

26    "*Moreover, the recently enacted USA FREEDOM Act*

27    *provides that amicus curiae may be appointed to*

28    *represent the public in certain FISC proceedings*

29    *involving NSA surveillance pursuant to Section 702.*

19

1    *These examples of course are not civil challenges to*
2    *Section 702, and establishing standing to challenge*
3    *Section 702 in a civil case is plainly difficult.  But*
4    *such difficulty comes with the territory.  It is not a*
5    *flaw of a classified program that standing to challenge*   10:59
6    *that program is not easily established; it is a*
7    *constitutional requirement essential to the separation*
8    *powers."*
9

10   There is one other case which I'm not going to open,   10:59
11   Judge, but I just mention to you where it is because
12   it's referred to and the most recent decision on
13   standing is a decision of the Foreign Intelligence
14   Surveillance Court itself and that's a decision of 25th
15   January 2017 and that was an application by the ACLU to   10:59
16   obtain certain records from the FISC court which they
17   said they were entitled to by virtue of their first
18   amendment rights and the court rejected that
19   application saying that they didn't have standing.
20                                                             11:00

21   It's another useful decision in the sense that it goes
22   through all the authorities and it's a useful source in
23   that and I suppose it's the most recent decision and
24   perhaps as a matter of curiosity it happens to be a
25   decision of the Foreign Intelligence Surveillance   11:00
26   Court.  It's in Book 3 at Tab 42 but I'm not going to
27   open it, Judge, in the interests of time.
28
29   What I thought might be useful, however, on standing,

20

| | |
|---|---|
| 1 | Judge, is to, first of all we might as well give you |
| 2 | the experts summary document which came out of their |
| 3 | meeting, and I think a very helpful meeting it was. |
| 4 | Sometimes these things are not productive, I think this |
| 5 | was a productive meeting, Judge, a significant amount |
| 6 | of agreement was reached between the parties. |
| 7 | **MS. JUSTICE COSTELLO:** So I can find it again, where |
| 8 | are you proposing that this should be entered in the |
| 9 | booklets? |
| 10 | **MR. MICHAEL COLLINS:** The agreed? |
| 11 | **MS. JUSTICE COSTELLO:** Yes. |
| 12 | **MR. MICHAEL COLLINS:** I didn't address my mind to that |
| 13 | logistical point, Judge. |
| 14 | **MS. JUSTICE COSTELLO:** I will stick it in with the |
| 15 | written submissions. |
| 16 | **MR. MICHAEL COLLINS:** That's probably a good idea |
| 17 | actually, Judge, that's probably the best place for it. |
| 18 | |
| 19 | Can I draw your attention first, Judge, to a decision, |
| 20 | a recent decision that they mention on standing first |
| 21 | of all that I haven't referred to. It's on page 3 of |
| 22 | the experts summary. |
| 23 | **MS. JUSTICE COSTELLO:** Yes. |
| 24 | **MR. MICHAEL COLLINS:** It's a case called <u>Valdez -v-</u> |
| 25 | <u>National Security Agency</u>, it's the decision from the |
| 26 | District Court in Utah on January 10th, 2017. It says: |
| 27 | *"In this lower court case"* -- I am sorry this is an |
| 28 | introductory section where the experts have jointly |
| 29 | agreed on some pieces of information that are useful. |

11:00
11:01
11:01
11:01
11:01

21

1     **MS. JUSTICE COSTELLO:**  I was given it in soft copy this
2     morning.  I started reading it.
3     **MR. MICHAEL COLLINS:**  Good.
4     **MS. JUSTICE COSTELLO:**  But I didn't get very far.
5     **MR. MICHAEL COLLINS:**  No, that's fine:                    11:02
6
7     *"In this lower-court case, the district court denied*
8     *the NSA's motion to dismiss (for lack of standing) a*
9     *lawsuit filed by six plaintiffs who claimed that the*
10    *NSA unlawfully intercepted, gathered, and monitored all*
11    *electronic communications in and around Salt Lake City*
12    *and all Olympic venues during the 2002 Winter Olympics.*
13    *Focusing on the procedural posture, the district court*
14    *explained that 'it is generally not the role of trial*
15    *courts at the motion to dismiss stage to pass on the*
16    *plausibility of otherwise well-pled factual allegations*
17    *in pleadings'."*
18
19    And quote:  *"'At the pre-discovery motion to dismiss*
20    *stage, this court must assume the truth of well-pleaded*
21    *factual allegations that are not simply legal*
22    *conclusions or bare assertions of the elements of a*
23    *claim —so long as the allegations do not defy reality*
24    *as we know it' – even if, in the court's own judgment,*
25    *those facts seem at the outset incredible,*
26    *unbelievable, or highly unlikely to be true. ').  The*
27    *court distinguished the Supreme Court's **Clapper***
28    *decision because (i) it arose in the context of summary*
29    *judgment, not a motion to dismiss."*

1    which obviously has a different level of scrutiny:

2

3    "2.    Unlike in **Clapper** the plaintiffs 'affirmatively

4    state that their communications were, in fact,

5    unlawfully intercepted'."                              11:03

6

7    See also:  "Though those allegations will undoubtedly

8    be tested as this case proceeds, court concludes at

9    this early stage that the Plaintiffs have in their

10   Amended Complaint plausibly alleged injury and

11   redressability as required for Article III standing,

12   and they overcome the NSA's challenge to jurisdiction'.

13   This case will now presumably proceed to the summary

14   judgment phase, where the plaintiffs will face a higher

15   burden to establish by a preponderance of the evidence

16   that they were in fact surveilled."

17

18   So it's quite similar to the **Wikimedia** decision.

19

20   And at paragraph 9 there on page 4, Judge, they refer    11:03

21   to this decision of the Foreign Intelligence

22   Surveillance Court that I mentioned a moment ago:

23

24   "On Jan 25, 2017 the presiding judge of the FISC held

25   that there was no First Amendment right of access to     11:03

26   FISC opinions and that the ACLU therefore did not have

27   standing to seek access to the opinions at issue."

28

29   Refers to the case:  "Because the court concluded that

23

1      *the ACLU lacked standing, it also refused to consider*

2      *the request for public release pursuant to the FISC's*

3      *rules of procedure or the court's inherent supervisory*

4      *powers over its own records."*

5

6      And as I say that's in the Book of Authorities as

7      I have mentioned.

8

9      The experts deal with standing, Judge, at page 33 of

10     this document and I might just open that to you because

11     I think it helpfully summarises the very large area of

12     agreement between the experts on this and where they

13     disagree:

14

15     *"With regard to Article III standing the experts agree*

16     *on the following statements:*

17

18     *1.   There are three elements of Article III standing,*

19     *(1) injury-in-fact; (2) causation; and (3)*

20     *redressability.  'To establish Article III standing, an*

21     *injury must be concrete, particularized, and actual or*

22     *imminent [injury-in-fact]; fairly traceable to the*

23     *challenged action [causation]; and redressable by a*

24     *favorable ruling [redressability].'"*

25

26     Citing **Clapper -v- Amnesty International**:

27

28     *"2.   The U.S. Supreme Court has noted that, especially*

29     *in lawsuits against the federal government, Article III*

1     *standing doctrine is an important component of the*

2     *separation of powers – and that, in protecting the*

3     *political branches from undue judicial interference,*

4     *the courts' inquiry should be 'especially rigorous when*

5     *reaching the merits of the dispute would force us to*

6     *decide whether an action taken by one of the other two*

7     *branches of the federal government was*

8     *unconstitutional.*

9

10     *3.  Although the Supreme Court in __Clapper__ observed that* 11:05

11     *'we have often found a lack of standing in cases in*

12     *which the Judiciary has been requested to review*

13     *actions of the political branches in the fields of*

14     *intelligence gathering and foreign affairs', the Court*

15     *did not state whether intelligence-gathering and*

16     *foreign-relations cases receive special standing*

17     *consideration materially different from the more*

18     *general approach followed in all constitutional*

19     *challenges to federal government action.*

20     11:05

21     *4.  With regard to the three elements of Article III*

22     *standing doctrine, although they must be satisfied in*

23     *all cases, how they are satisfied depends upon the*

24     *posture of the lawsuit at the moment."*

25     11:05

26     The posture I think meaning the stage at which

27     procedurally it is reached, whether it's a motion to

28     dismiss as disclosing no cause of action or whether

29     it's a summary judgment, for example:

25

1    *"Thus, to survive a motion to dismiss, plaintiffs need*
2    *only allege plausible facts that, if true, would*
3    *satisfy each of these three elements.  In contrast, to*
4    *survive a defendant's motion for summary judgment on*
5    *standing, plaintiffs must establish their standing by a*    11:05
6    *preponderance of the evidence.*

7

8    *5.  The 'injury-in-fact' element of Article III*
9    *standing doctrine treats prior and future injuries*
10   *slightly differently.  Thus, to survive a motion to*
11   *dismiss for lack of standing, a plaintiff must allege*
12   *that a prior injury has actually occurred, whereas they*
13   *would need to allege that a future injury not only*
14   *might occur, but that 'the threatened injury is*
15   *certainly impending, or there is a substantial risk*
16   *that the harm will occur'."*

17

18   Citing **Susan B. Anthony list -v- Driehaus**.

19

20   *6:  "The **Clapper** decision rejected the plaintiffs'*    11:06
21   *standing to bring a claim for a future injury at the*
22   *summary judgment state of litigation, at which point*
23   *the plaintiffs '[could] no longer rest on...  mere*
24   *allegations, but must [have] set forth by affidavit or*
25   *other evidence specific facts."*    11:06

26

27   *7:  "In **Spokeo -v- Robins** - and you will recall*
28   *I opened that yesterday, Judge - the Supreme Court held*
29   *that a trivial procedural violation of a federal*

*statute (the Fair Credit Reporting Act), without any*
*actual harm to the plaintiff beyond the trivial*
*procedural violation, would be insufficient to satisfy*
*the 'injury-in-fact' prong of Article III standing*
*doctrine.  The Court then remanded the case to the*          11:06
*Court of Appeals to determine if the plaintiff indeed*
*had suffered an injury in fact.*

*8.  Finally, and perhaps most importantly, Article III*
*standing doctrine is, to a large degree, indeterminate.*   11:07
*Although the elements are, as shown above, capable of*
*objective description, their application to specific*
*cases is often difficult to predict — and may turn on*
*case specific factual variations otherwise unaccounted*
*for in the doctrinal standard.  This phenomenon is*
*reflected in lower-court decisions in post-**Clapper**,*
*post-Snowden suits challenging U.S. foreign*
*intelligence surveillance programs, some of which have*
*found Article III standing, and others which have not."*
                                                              11:07

Then they set out, Judge, you probably, if you have
looked at it, you will be familiar with the format they
have adopted.
**MS. JUSTICE COSTELLO:**  Yes.
**MR. MICHAEL COLLINS:**  The issue first is the issue of     11:07
**Spokeo -v- Robins**:  The Controller's expert's position
is:

"***Spokeo*** *is another recent Article III case from the*

27

1    *Supreme Court, and it represents a stricter reading of*
2    *standing.  The __Spokeo__ Court held that a plaintiff must*
3    *allege more than a bare procedural violation, divorced*
4    *from any concrete harm, and satisfy the injury-in-fact*
5    *requirement of Article III."*                          11:07

6

7    The Facebook expert position is:  "__*Spokeo*__ *concerned the*
8    *burden a plaintiff must meet to bring suit under the*
9    *Fair Credit Reporting Act, a statute that appears to*
10   *allow standing in cases where incorrect information*
11   *about him is posted on the Internet, even if that*
12   *incorrect information causes no tangible harm.  All*
13   *__Spokeo__ held is, obviously, that a plaintiff must still*
14   *show an injury in fact to demonstrate Article III*
15   *standing.  That was true before __Clapper__, and __Spokeo__*
16   *does nothing to 'narrow' it."*

17

18   And so there's a disagreement perhaps between them on
19   the exact extent of whether __Spokeo__ has narrowed or not
20   the standing requirements:                             11:08

21

22   Secondly, on the issue of *"standing and notice"*,
23   firstly Ms. Gorski's position --
24   **MS. JUSTICE COSTELLO:**  Which page are we on?
25   **MR. MICHAEL COLLINS:**  Sorry, page 35.              11:08
26   **MS. JUSTICE COSTELLO:**  Oh, the next page.
27   **MR. MICHAEL COLLINS:**  Yes.  The first column is of
28   course --
29   **MS. JUSTICE COSTELLO:**  The issues.

28

1    **MR. MICHAEL COLLINS:** -- Mr. Schrems' expert,
2    Ms. Gorski, and it says:

3

4    "*In response to Vladeck - Prof. Vladeck obviously -*
5    *Gorski states that more context is necessary. Firstly,*   11:08
6    *the 'plausibility' threshold applies solely at the*
7    *outset of the case, when a court assesses the*
8    *plausibility of the pleadings. For a court to reach*
9    *the merits of the case against the U.S. government, a*
10   *plaintiff must show by a preponderance of the evidence*
11   *that there is a 'substantial likelihood' that the*
12   *government has, is, or will seize or search their*
13   *communications. Second, because virtually none of the*
14   *individuals subject to Section 702 or EO 12333*
15   *surveillance receive notice of that fact, it is*
16   *exceedingly difficult to establish standing.*"

17

18   We didn't intervene in that particular point. And the
19   Facebook witness Prof. Vladeck states that:
20                                                              11:09

21   "*The DPC Draft Decision 'rightly raises concerns about*
22   *Article III standing,' and concludes that 'where EU*
23   *citizens can marshal plausible grounds from which it is*
24   *reasonable to believe that the U.S. government has*
25   *collected, will collect, and/or is maintaining, records*
26   *relating to them in a government database, they will*
27   *likely have standing to sue even if light of the*
28   *Supreme Court's Clapper decision.*"

29

29

And the reconciliation position is: "*The experts agree*
*on the respective thresholds that a respective*
*thresholds that a plaintiff must satisfy at the 'motion*
*to dismiss' and 'summary judgment' stages. See above*
*discussion of standing standards.*                    11:09

*The experts also agree that the government's failure to*
*notify individuals subject to its secret surveillance*
*programs makes it more difficult for plaintiffs to*
*establish Article III standing.*"                      11:09

Then finally with regard to Article III standing, the
experts have the following disagreements:

"*1) We disagree over the implications of the* **_Spokeo_**   11:10
*decision. Mr. Serwin believes that it 'is consistent*
*with a narrower reading of* **_Clapper_**'. *Prof. Richards*
*states that '*Spokeo *certainly made standing doctrine*
*stricter in general, especially in privacy cases'.*
*(Referring to Spokeo's 'tightening' of standing*
*doctrine and the 'higher obstacle' it imposes).*
*Prof. Vladeck believes that* **_Spokeo_** *applied existing*
*Article III doctrine (especially the requirement of a*
*concrete injury) to reverse a lower court ruling that*
*appeared to allow a suit even without such an injury,*
*and that it therefore did not alter the contours of the*
*underlying doctrine in any appreciable way.*

*2) We disagree over the implications of the district*

30

1      court's decision in *Wikimedia -v- National Security*

2      *Agency*."

3

4      That's the case I just opened to you, Judge, and did so

5      to give this comment context:             11:10

6

7      *"Ms. Gorski views that ruling as 'illustrat[ing] the*

8      *difficulties that plaintiffs face in establishing*

9      *standing, even at the outset of a case, when a*

10     *plaintiffs allegations must merely be plausible'.*

11     *Prof. Vladeck believes we should not draw general*

12     *conclusions from non-precedential district court*

13     *rulings (especially those that may soon be reversed on*

14     *appeal), and that, if* **Wikimedia** *does support any larger*

15     *conclusion, it is that 'there is significant*

16     *uncertainty in the lower courts over exactly when*

17     **Clapper** *does and does not foreclose standing.'  The*

18     *critical point for present purposes is that this*

19     *uncertainty is not nearly as categorically hostile to*

20     *standing as suggested in the DPC Draft Decision, and*

21     *instead is more reflective of the case-specific*

22     *vagaries of individual lawsuits.*

23

24     *3.  Finally, and perhaps most significantly, we*

25     *disagree over the implications of our analysis for 'the*  11:11

26     *DPC's conclusions that standing doctrine represents a*

27     *general obstacle to data protection claims brought by*

28     *EU citizens'.  Richards determines that this conclusion*

29     *'seems eminently correct'."*

31

1

2        See also the Serwin memo:  "*Prof. Vladeck disagrees.*
3        *In his view, although Article III standing is a*
4        *prerequisite for all civil litigation in U.S.  federal*
5        *court, the DPC Draft Decision 'substantially*          11:11
6        *overstates' the degree to which it is an obstacle in*
7        *challenges to unlawful government surveillance.*
8        *Whereas the DPC Whereas the DPC Draft Decision reads*
9        *U.S. law as requiring plaintiffs 'to demonstrate that*
10       *harm has in fact been suffered as a result of the*
11       *interference alleged', such harm can also be future*
12       *harm, and, in either event, Vladeck believes that it*
13       *can be established at the motion-to-dismiss stage*
14       *simply through plausible factual allegations in the*
15       *plaintiff's complaint."*                              11:11

16

17       So that's the summary on the standing position and
18       hopefully that experts summary is helpful in that
19       regard.

20                                                              11:12

21       So I want to leave standing now, Judge, if I may, and
22       I want to move on to what's known as the Privacy
23       Shield.

24

25       Judge, the Safe Harbour Decision had been the basis    11:12
26       upon which data was being lawfully transferred from the
27       EU to the US.  Because it was a Commission decision and
28       therefore once you are in compliance and transferring
29       pursuant to a Commission decision, for so long as that

32

decision remains valid, it is lawful under EU law to

make the transfers.  But there were always concerns

about the Safe Harbour Decision decision because it was

self-certification and a variety of other concerns

about it and the EU and the US had been in discussions    11:13

about the possibility of coming up with some other

arrangement.


That obviously got much greater impetus after the

**Schrems** decision when the Safe Harbour Decision was      11:13

declared invalid.  Because there was then the

difficulty as to under what régime or how could you

lawfully transfer data from the EU to the US.

There were of course these other mechanisms such as

SCCs which were the ones that were adopted by a number    11:13

of companies, including Facebook, and there are also

some other mechanisms as well.  There are various

binding corporate rules, for example, is another system

under which transfers can be made.
                                                          11:13

The two governments then came to ultimately a set of

arrangements which were designed to in effect replace

the Safe Harbour Decisions.  One is what's known as the

umbrella agreement, I have referred to this before,

Judge.  This is an agreement between the EU and the US     11:14

signed in June of 2016 dealing primarily with the

transfer of data in the context of criminal

investigation and prosecution.  I'm not going to go

through the detail of that agreement, Judge, but it's

in your books it's in Book 5 at Tab 55.  I'm not asking
you to go to it at this stage.

In addition - and that's what's generally referred to
as the umbrella agreement - but as part of the general
package, if I can loosely call it that, there was the
undertaking by the United States to do something to
make the Privacy Act protections available to EU
citizens and that was done, at least in part, through
the Judicial Redress Act of 2016 and we have looked at
that yesterday.  And the third element of it is what is
referred to as the Privacy Shield.

Now you will recall that there is this Article 29
working group, Judge, which is set up specifically
under Article 29 of the Directive and they have been
looking at the issue of the Privacy Shield arrangements
which were proposed, which were and are in essence,
Judge, and we will come to the detail of them now,
again a type of self-certification arrangement whereby
there are a set of principles set out in various
letters and forms of undertakings from the US
government that say 'this is the way we will conduct
our foreign surveillance or surveillance of foreign
data and so forth in the future, these are the
principles that we are going to observe and here are
certain mechanisms by which people who have complaints
in relation to it can get resolution of those
complaints in one form or another'.  And from the

| | |
|---|---|
| 1 | viewpoint of EU citizens who wish to make a complaint |
| 2 | in relation to how an agency has acted in particular, |
| 3 | apart from the companies themselves, there is what's |
| 4 | called an Ombudsperson mechanism has been set up that |
| 5 | we'll come to and a complaint can be made to the |
| 6 | Ombudsperson who will investigate that complaint. |
| 7 | |
| 8 | In addition, if your complaint is as against the |
| 9 | individual company themselves, then there are various |
| 10 | alternative dispute resolution mechanisms, a type of |
| 11 | private arbitration effectively, that can be gone to to |
| 12 | resolve these matters.  The Commission has adopted a |
| 13 | decision, it's not an agreement as such between the EU |
| 14 | and the US, it is a Commission decision.  But it's a |
| 15 | Commission decision which says, assuming that all of |
| 16 | these things are done, and we now have these |
| 17 | representations and assurances from the US government |
| 18 | which are set out in a series of letters from various |
| 19 | US government officials in annexes to the Commission |
| 20 | decision, on that basis we the Commission consider that |
| 21 | there is now adequate protection within the meaning of |
| 22 | Articles 25 and 26 for data transfers from the EU to |
| 23 | the US.  And that means that if data transfers are now |
| 24 | made, if you sign up for the Privacy Shield, and you do |
| 25 | have to sign up for it in the sense that you commit to |
| 26 | it in the US and I think the US government publishes |
| 27 | then a list of the companies who have signed up to the |
| 28 | Privacy Shield, at least for certain forms of data. |
| 29 | They may not sign up to it for all transfers of data |

11:15

11:16

11:16

11:16

11:16

35

but they can sign up to it for some and, insofar as
they sign up to it, they can proceed on that basis.

In this instance of course the data transfers with
which we are concerned are made pursuant to the SCCs     11:17
rather than pursuant to the Privacy Shield, but there
is a connection, I think, between them insofar as that,
if there was a dispute about the transfers under the
SCCs, I think there is a facility whereby the Ombudsman
procedure could be invoked in relation to that.         11:17

One of the criticisms of the procedure, however, is
that the Ombudsman procedure is not in fact a type of
judicial redress because it doesn't, for example, give
you any awards or any remedies in terms of a direct      11:17
remedy to the person themselves, although it will
investigate the complaint, but it won't actually tell
you exactly what has happened.  It will tell you that
it has investigated it and that some remedial action
has been taken, and we'll come to the detail of that.    11:18
And there are at the moment, I think, two challenges
under way before the court, and I'll come to that a bit
later, challenging the validity of the Privacy Shield.

But the Commissioner in her decision, when she gave her  11:18
decision the Privacy Shield had not yet come into
operation.
**MS. JUSTICE COSTELLO:**  This was her Draft Decision?
**MR. MICHAEL COLLINS:**  Her Draft Decision, I should say,

36

the Draft Decision.  She refers to it expressly in the
decision and he says, because it hasn't yet come into
force, she hasn't expressly taken account of that in
her evaluation of the adequacy of the protection in the
US.                                                       11:18

Obviously everybody I think acknowledges that if the
matter is to go to the Court of Justice it's important
that the Court of Justice have all the relevant facts
before it and among those relevant facts is clearly the  11:18
fact that the Privacy Shield is now in operation.

So it's a Commission decision but it's not actually a
US law, if I can put it that way, but it is clearly a
matter of importance that would have to be considered    11:18
by the European court, whether on the reference it
chose to consider it alongside or in some conjunction
with the existing challenges that are outstanding
before the court in relation to privacy of the shield,
I just don't know how they would deal with that, but     11:19
it's clearly a matter that's out there.

So that's a very broad and general background.  And
just in case I forget to say it, Judge, could I also
draw your attention to the fact that the Directive with  11:19
which we are dealing is about to be replaced by a new
directive which is called the General Data Protection
Regulations.  Those regulations have been enacted by
the EU but they are not yet in force and will not be in

37

|    |                                                           |       |
|----|-----------------------------------------------------------|-------|
|  1 | force until the 25th May 2018, although sometimes there   |       |
|  2 | is some useful guidance perhaps to be gained from those   |       |
|  3 | regulations.  But just to be aware of the fact that       |       |
|  4 | those regulations are coming down the tracks.  And they   |       |
|  5 | are, I just need to identify them, Judge, they are in     | 11:19 |
|  6 | Book 1 of the core Book of Authorities, the European      |       |
|  7 | authorities at Tab 11.                                    |       |
|  8 | **MS. JUSTICE COSTELLO:**  I will have to find them myself.|       |
|  9 | **MR. MICHAEL COLLINS:**  Yes, because I'm going to ask you|       |
| 10 | to go to Book 1, Judge, because that's where the          | 11:20 |
| 11 | Privacy Shield can also be found.                         |       |
| 12 | **MS. JUSTICE COSTELLO:**  Is this the one that starts off |       |
| 13 | with *"A European Union primary law, B"*?                 |       |
| 14 | **MR. MICHAEL COLLINS:**  Yes, that's the one.            |       |
| 15 | **MS. JUSTICE COSTELLO:**  Excellent.                     | 11:20 |
| 16 | **MR. MICHAEL COLLINS:**  At Tab 11, I'm not asking you to|       |
| 17 | go to it, Judge --                                        |       |
| 18 | **MS. JUSTICE COSTELLO:**  Yes.                           |       |
| 19 | **MR. MICHAEL COLLINS:**  -- but you will see the new     |       |
| 20 | regulations, the General Data Protection Regulations or   | 11:20 |
| 21 | as you will sometimes see the acronym referred to GDPR    |       |
| 22 | and that's what that refers to.                           |       |
| 23 |                                                           |       |
| 24 | Then at 13 you will find the Commission decision          |       |
| 25 | relating to the adequacy of the protection provided by    | 11:21 |
| 26 | what's called the EU-US Privacy Shield.                   |       |
| 27 |                                                           |       |
| 28 | Just to look firstly at the structure of this document,   |       |
| 29 | Judge, it's a long document and I'm not going to open     |       |

|    |                                                                      |       |
|----|----------------------------------------------------------------------|-------|
| 1  | all of it.  But it starts, first of all it's a                       |       |
| 2  | Commission implementing decision and there is an                     |       |
| 3  | introduction section that starts on page 2 which goes                |       |
| 4  | on up to page 42 and that really sets out a full                     |       |
| 5  | description of the whole thing and how it works and I'm              | 11:21 |
| 6  | going to spend some bit of time on that.                             |       |
| 7  |                                                                      |       |
| 8  | The actual decision itself is on page 43 and 44, it's                |       |
| 9  | only a two-page decision, it's very short.  But at this              |       |
| 10 | point I just draw attention to it so that we know what               | 11:21 |
| 11 | we mean by the EU-US Privacy Shield.  If you look at                 |       |
| 12 | Article 1 paragraph 2 of the -- well, I should open                  |       |
| 13 | both 1 and 2, Judge.  This is page 43 Article 1:                     |       |

15  *"For the purpose of Article 25 --"*                                                11:22

16  **MS. JUSTICE COSTELLO:**  Sorry, I haven't got the page.

17  **MR. MICHAEL COLLINS:**  Sorry, Judge.

18  **MS. JUSTICE COSTELLO:**  43?

19  **MR. MICHAEL COLLINS:**  Page 43, Article 1.

20  **MS. JUSTICE COSTELLO:**  Wait a moment.  Tab 13 the       11:22

21  decision?

22  **MR. MICHAEL COLLINS:**  There's the decision, this is all

23  part of the decision.

24  **MS. JUSTICE COSTELLO:**  Yes.

25  **MR. MICHAEL COLLINS:**  The first 42 pages are the        11:22

26  introduction --

27  **MS. JUSTICE COSTELLO:**  Yes.

28  **MR. MICHAEL COLLINS:**  -- which explains it.  Page 43 is

29  the actual decision where it says *"has adopted this*

1    *decision*".

2    **MR. GALLAGHER:**  It may be 35 in yours, Judge.

3    **MS. JUSTICE COSTELLO:**  Yes.

4    **MR. MICHAEL COLLINS:**  I am sorry, Judge.  Thank you,

5    Mr. Gallagher.  So if you have that, Judge?                    11:22

6    **MS. JUSTICE COSTELLO:**  Yes, 35, thank you.

7    **MR. MICHAEL COLLINS:**  Article 1.1 says:

8

9    "*For the purposes of Article 25(2) of Directive 95/46,*

10   *the United States ensures an adequate level of*              11:22

11   *protection for personal data transferred from the Union*

12   *to organisations in the United States under the EU-US*

13   *Privacy Shield.*

14

15   *2.   The EU-US Privacy Shield is constituted by the*         11:23

16   *principles issued by the U.S. Department of Commerce on*

17   *7 July 2016 as set out in Annex II and the official*

18   *representations and commitments contained in the*

19   *documents listed in Annexes I, III to VII.*"

20                                                                 11:23

21   And if you turn over the page, Judge, I'm not going to

22   go through these at the moment, I will refer to some of

23   them later on, Annex 1 is a letter from the US

24   Secretary of Commerce, Penny Pritzker, to the

25   Commissioner.  Then there's an annex to that with a          11:23

26   letter from the Acting Under Secretary for

27   International Trade, Ken Hyatt, which sets out various

28   enhancements to the protection of data in the US under

29   these principles.

40

1    **MS. JUSTICE COSTELLO:**  Mm hmm.

2    **MR. MICHAEL COLLINS:**  And that goes on for some time.

3    The page numbers are on the top right of this document,

4    Judge, and on page 45 they set out in Annex 2 the

5    arbitral model.                                              11:23

6    **MS. JUSTICE COSTELLO:**  Yes.

7    **MR. MICHAEL COLLINS:**  This is to set out a model of

8    private arbitration which if people have complaints can

9    go to arbitration with the companies concerned as a

10   private matter of course.                                    11:24

11

12   On page 48 there is Annex 2 which are the EU-US Privacy

13   Shield framework principles issued by the US Department

14   of Commerce.  This is how they will maintain an

15   authoritative list of US organisations that have            11:24

16   self-certified to the Department that they are going to

17   comply with these principles and the possibility of

18   removal from that list.

19

20   We then move on significantly, sorry, Judge, to page 71     11:24

21   there is a letter from the then US Secretary of State

22   John Kerry.  He sets out in Annex A the EU-U.S. Privacy

23   Shield Ombudsperson mechanism regarding signals

24   intelligence.  That's really quite important because

25   from the viewpoint of redress that somebody has against     11:25

26   the US government or a US government agency, the

27   Ombudsperson mechanism is really the mechanism in

28   question.  And we may need to look at that in just a

29   little bit more detail to understand precisely what

1  that Ombudsperson mechanism is, so that letter from

2  Secretary of State Kerry is one that we will have to

3  come back to.

4

5  Then at page 78 there is a letter from the Federal        11:25

6  Trade Commission Chairwoman, Edel Ramirez.  That's

7  dealing with the fact, Judge, that, as I mentioned

8  I think a day or two ago, the Federal Trade Commission

9  has a jurisdiction in particular to bring proceedings

10  against companies if they are engaged in deceptive       11:25

11  trade practices and things of some sort.  So that if

12  somebody subscribed to the Privacy Shield arrangement

13  but wasn't for example in practice adhering to its

14  principles, then there's the possibility that the

15  Federal Trade Commission or other similar type          11:25

16  administrative enforcement agencies in the US could

17  take some form of action against that company.

18

19  And on page 85 there is an attachment A which is

20  headed:  *"EU-US Privacy Shield framework in context: an* 11:26

21  *overview of US privacy and security landscape."*  That

22  gives from the US perspective a general view of how it

23  operates.

24

25  Annex 5 at page 88 is a letter from the US Secretary of 11:26

26  Transportation Anthony Foxx to the Commissioner and

27  that's dealing with the US Department of Transportation

28  and its role in relation to investigating violations.

29

42

| 1 | On page 91 there's a letter from General Counsel Robert |
| 2 | Litt of the office of the Director of National |
| 3 | Intelligence and he deals specifically with how, you |
| 4 | will recall the Presidential Policy Directive 28 that |
| 5 | I opened to you yesterday issued by President Obama in |
| 6 | January 2014 and he discusses that PPD-28 and how that |
| 7 | operates and the limitations it sets out on |
| 8 | intelligence gathering and so forth.  And he gives a |
| 9 | summary at the end that I'll come to in due course. |
| 10 | |
| 11 | On page 109 there is a letter from Department Assistant |
| 12 | Attorney General and Counselor for International |
| 13 | Affairs Bruce Swartz of the US Department of Justice. |
| 14 | He deals with the question of criminal law enforcement |
| 15 | authorities and goes through some of the procedures |
| 16 | that are followed for criminal law enforcement under |
| 17 | some of the legislation that we discussed yesterday |
| 18 | such as the Electronic Communication Privacy Act, court |
| 19 | orders for pen register and trap and trace devices and |
| 20 | so forth. |
| 21 | |
| 22 | So they are the attachments to the decision, Judge, and |
| 23 | if I go back to the decision itself.  It says in |
| 24 | Article 2 -- sorry, I was on Article 1, at paragraph 3 |
| 25 | it says: |
| 26 | |
| 27 | "*For the purpose of paragraph 1, personal data are* |
| 28 | *transferred under the EU-US Privacy Shield where they* |
| 29 | *are transferred from the Union to organisations in the* |

Timestamps in right margin: 11:26 (line 5), 11:27 (line 10), 11:27 (line 15), 11:27 (line 20), 11:28 (line 25)

43

*United States that are included in the 'Privacy Shield*
*list', maintained and made publicly available by the US*
*Department of Commerce."*

Article 2 says:  *"This Decision does not affect the*                11:28
*application of the provisions of Directive 95/46 other*
*than Article 25(1) that pertain to the processing of*
*personal data within the Member States, in particular*
*Article 4 thereof."*
                                                                      11:28

Article 3 says:  *"Wherever the competent authorities in*
*Member States exercise their powers pursuant to*
*Article 28(3) of Directive 95/46/EC leading to the*
*suspension or definitive ban of data flows to an*
*organisation in the United States that is included in*
*the Privacy Shield List in accordance with Sections I*
*and III of the Principles set out in Annex II in order*
*to protect individuals with regard to the processing of*
*their personal data, the Member State concerned shall*
*inform the Commission without delay."*                               11:28

Article 4 says:  *"The Commission will continuously*
*monitor the functioning of the EU-U.S. Privacy Shield*
*with a view to assessing whether the United States*
*continues to ensure an adequate level of protection of*     11:28
*personal data transferred thereunder from the Union to*
*organisations in the US."*

If I pause there, Judge.  That's a reflection of the

fact that this is not an agreement as such between the
EU and the US in a formal sense, of an agreement they
have signed up.  It's a set of commitments that the US
have given and therefore the EU is going to continually
monitor whether the US policy remains committed to the   11:29
fulfilment of those principles.

At Article 4(2) it says:  "*The Member States and the*
*Commission shall inform each other of cases where it*
*appears that the government bodies in the United States*
*with the statutory power to enforce compliance with the*
*Principles set out in Annex II fail to provide*
*effective detection and supervision mechanisms enabling*
*infringements of the Principles to be identified and*
*punished in practice.*

*3.  The Member States and the Commission shall inform*
*each other of any indications that the interferences by*
*U.S. public authorities responsible for national*
*security, law enforcement or other public interests*
*with the right of individuals to the protection of*
*their personal data go beyond what is strictly*
*necessary, and/or that there is no effective legal*
*protection against such interferences.*

*4.  Within one year from the date of the notification*
*of this Decision to the Member States and on a yearly*
*basis thereafter, the Commission will evaluate the*
*finding in Article 1(1) on the basis of all available*

45

1      *information, including the information received as part*

2      *of the annual joint review."*

3

4      So there will be a review in presumably in June of this

5      year in relation to the adequacy:         <sub>11:30</sub>

6

7      *"5. The Commission will report any pertinent findings*

8      *to the Committee established under Article 31 of the*

9      *Directive.*

10                    11:30

11      *6. The Commission will present draft measures in*

12      *accordance with the procedure referred to in*

13      *Article 31(2) with a view to suspending, amending or*

14      *repealing this decision or limiting its scope, among*

15      *others, where there are indications:*     <sub>11:30</sub>

16

17      *- that the US public authorities do not comply with the*

18      *representations and commitments contained in the*

19      *documents annexed to this Decision, including as*

20      *regards the conditions and limitations for access by*

21      *U.S. public authorities for law enforcement, national*

22      *security and other public interest purposes to personal*

23      *data transferred under the EU-U.S. Privacy Shield."*

24

25      Second bullet point: *"Of a systematic failure to*   <sub>11:30</sub>

26      *effectively address complaints by EU data subjects; or,*

27      *third, of a systematic failure by the Privacy Shield*

28      *Ombudsperson to provide timely and appropriate*

29      *responses to request from EU data subjects as required*

1          *by Section 4(e) of Annex III."*

2

3          And:   "*The Commission will present such draft measures*

4          *if the lack of cooperation of the bodies involved in*

5          *ensuring the functioning of the EU-U.S. Privacy Shield*

6          *in the United States prevents the Commission from*

7          *determining whether the finding in Article 1(1) is*

8          *affected."*

9

10         And Member States have to implement the decision      11:31

11         obviously.

12

13         So that's the decision itself.  But it is necessary to

14         look at the long introduction to it, unfortunately,

15         Judge, to understand it somewhat better.          11:31

16

17         The background is set out on pages 2 and 3 and I don't

18         think I need go to that.  But if you go to paragraph 8,

19         Judge, on page 3 it says:

20                                                               11:31

21         "*Based on evidence gathered by the Commission,*

22         *including information stemming from the work of EU-US*

23         *Privacy Contact Group and the information on U.S.*

24         *intelligence programs received in the ad hoc EU-U.S.*

25         *Working Group, the Commission formulated 13*

26         *recommendations for a review of the Safe Harbour*

27         *scheme."*

28

29         And details those in summary form.

1  Then over the page, Judge, it refers to the <u>Schrems</u>

2  decision and the consequences of that and at 13 it

3  says:  "*The Commission has carefully analysed US law*

4  *and practice, including these official representations*

5  *and commitments."*                                    11:32

6

7  Sorry, I should, to put it properly, Judge, I should go

8  back to 12, I beg your pardon:

9

10  "*In 2014 the Commission had entered into talks with the*  11:32

11  *US authorities in order to discuss the strengthening of*

12  *the Safe Harbour scheme in line with the 13*

13  *recommendations contained in Communication COM (2013)*

14  *847.  After the judgment of the Court of Justice of the*

15  *European Union in the <u>Schrems</u> case, these talks were*

16  *intensified, with a view to a possible new adequacy*

17  *decision which would meet the requirements of Article*

18  *25 of Directive 95/46/EC as interpreted by the Court of*

19  *Justice.  The documents which are annexed to this*

20  *decision and will also be published in the U.S. Federal*

21  *Register are the result of these discussions.  The*

22  *privacy principles (Annex II), together with the*

23  *official representations and commitments by various*

24  *U.S. authorities contained in the documents in Annexes*

25  *I, III to VII, constitute the 'EU-U.S. Privacy Shield'.*

26

27  *13.  The Commission has carefully analysed U.S. law and*

28  *practice, including these official representations and*

29  *commitments.  Based on the findings developed in*

48

1     *recitals 136-140, the Commission concludes that the*

2     *United States ensures an adequate level of protection*

3     *for personal data transferred under the EU-U.S. Privacy*

4     *Shield from the Union to self-certified organisations*

5     *in the United States."*

6

7     And we will look particularly at those recitals, 136 to

8     140.

9

10    But in 14, it says:  "*The Privacy Shield is based on a*     11:33

11    *system of self-certification by which U.S.*

12    *organisations commit to a set of privacy principles.*

13    *It applies to both controllers and processors (agents),*

14    *with the specificity that processors must be*

15    *contractually bound to act only on instructions from*

16    *the EU controller and assist the latter in responding*

17    *to individuals exercising their rights under the*

18    *principles.*

19

20    *15.  Without prejudice to compliance with the national*

21    *provisions adopted pursuant to Directive 95/46/EC, the*

22    *present decision has the effect that transfers from a*

23    *controller or processor in the Union to organisations*

24    *in the U.S. that have self-certified their adherence to*

25    *the Principles with the Department of Commerce and have*

26    *committed to comply with them are allowed.  The*

27    *Principles apply solely to the processing of personal*

28    *data by the U.S. organisation in as far as processing*

29    *by such organisations does not fall within the scope of*

49

1    *Union legislation.  The Privacy Shield does not affect*
2    *the application of Union legislation governing the*
3    *processing of personal data in the Member States."*
4
5    At 17 it says:  "*The Principles apply immediately upon*
6    *certification.  One exception relates to the*
7    *Accountability for Onward Transfer Principle in a case*
8    *where an organisation self-certifying to the Privacy*
9    *Shield already has pre-existing commercial*
10   *relationships with third parties."*
11
12   And it talks about the transition problems.
13
14   At 18 it says:  "*The system will be administered and*
15   *monitored by the Department of Commerce based on its*
16   *commitment set out in the representations from the US*
17   *Secretary of Commerce in Annex 1.  With regard to the*
18   *enforcement of the Principles, the Federal Trade*
19   *Commission and the Department of Transportation have*
20   *made representations that are contained in Annex IV and*
21   *Annex V to the decision."*
22
23   It then summarises what the privacy principles are,
24   Judge, and I don't need, I think, to go into the detail
25   of this but just to outline very briefly the summary.
26
27   20 refers to the Notice Principle under which:
28   "*Organisations are obliged to provide information to*
29   *data subjects on a number of key elements relating to*

1    *the processing of their personal data."*

2

3    And it refers to the necessity to provide links to the

4    Department of Commerce website and the website of an

5    appropriate alternative dispute settlement provider.        11:35

6

7    In 21 it refers to the Data Integrity and Purpose

8    Limitation Principle under which personal data must be

9    limited to what is relevant for the purpose of the

10   processing.                                                 11:35

11

12   At 22 it states:  *"Where a new (changed) purpose is*

13   *materially different but still compatible with the*

14   *original purpose, the Choice Principle gives data*

15   *subjects the right to object or opt out.  The Choice*      11:35

16   *Principle does not supersede the express prohibition on*

17   *incompatible processing."*

18

19   In 23, it says:  *"Still under the Data Integrity and*

20   *Purpose Limitation Principle, personal information may*     11:35

21   *be retained in a form identifying and rendering an*

22   *identifiable (and thus in the form of personal data)*

23   *only for as long as it serves the purpose(s) for which*

24   *it was initially collected or subsequently authorised."*

25                                                               11:35

26   24:  *"Under the Security Principles, organisations must*

27   *take 'reasonable and appropriate' security measures.*

28   *In the case of sub-processing, organisations must*

29   *conclude a contract with the sub-processor guaranteeing*

51

1    *the same level of protection."*

2

3    25:  "*Under the Access Principle, data subjects have*

4    *the right, without need for justification and only*

5    *against a non-excessive fee, to obtain from an*                 11:36

6    *organisation confirmation of whether such organisation*

7    *is processing personal data related to them and have*

8    *the data communicated within reasonable time."*

9

10   About half way down that paragraph, Judge, it says:          11:36

11

12   "*In areas where companies most likely resort to the*

13   *automated processing of personal data to take decisions*

14   *affecting the individual (e.g. credit lending, mortgage*

15   *offers, employment), U.S. law offers specific*

16   *protections against adverse decisions."*

17

18   And it refers in the footnote to the Equal Credit

19   Opportunity Acts, the Fair Credit Reporting Act or the

20   Fair Housing Act:  "*These acts typically provide that*     11:36

21   *individuals have the right to be informed of the*

22   *specific reasons underlying the decision (e.g. the*

23   *rejection of a credit), to dispute incomplete or*

24   *inaccurate information (as well as reliance on unlawful*

25   *factors), and seek redress."*                               11:36

26

27   Then at the bottom of the page says:  "*Nevertheless,*

28   *given the increasing use of automated processing*

29   *(including profiling) as a basis for taking decisions*

52

1    *affecting individuals in the modern digital economy,*

2    *this is an area that needs to be closely monitored."*

3

4    In 26 under the Recourse, Enforcement and Liability

5    Principle: *"Participating organisations must provide*

6    *robust mechanisms to ensure compliance with the other*

7    *principles and recourse for EU data subjects whose*

8    *personal data have been processed in a non-compliant*

9    *manner, including effective remedies."*

10

11   It goes on to refer to the obligations that

12   organisations must verify that their policies conform

13   to the principles and, at the end, that they are

14   subject to the investigatory and enforcement powers of

15   the FTC, the Department of Transportation of another US

16   authorised statutory body that will effectively ensure

17   compliance with the Principles."

18

19   The next paragraph deals with onward transfers,

20   28 deals with the Accountability for Onward Transfer

21   Principle: *"Any onward transfer can only take place*

22   *(i) for limited and specified purposes, (ii) on the*

23   *basis of a contract or (iii) only if that contract*

24   *provides the same level of protection as the one*

25   *guaranteed by the Principles, which includes the*

26   *requirement that the application of the Principles may*

27   *only be limited to the extent necessary to meet*

28   *national security, law enforcement and other public*

29   *interest purposes."*

53

1      If I move on then to the next section, 2.2:

2      *"Transparency, Administration, and Oversight of the*

3      *EU-US Privacy Shield."* It refers to the mechanism set

4      out in the annexes. At 31 it says that the Department

5      of Commerce is going to make available a list of     11:38

6      organisations that have self-certified their adherence

7      to the principles and that's called the Privacy Shield

8      list.

9

10     At 32 it says that the Department of Commerce will make  11:38

11     the list and the re-certification submissions publicly

12     available: *"In addition, if available online, an*

13     *organisations privacy policy must include a hyperlink*

14     *to the Privacy Shield website as well as a hyperlink to*

15     *the website or complaint submission form of the*     11:38

16     *independent recourse mechanism that is available to*

17     *investigate unresolved complaints."*

18

19     I might just pause there, Judge. We'll see it a bit

20     later on, but this mechanism is, there are private    11:38

21     alternative dispute resolution providers in the United

22     States. If one even goes to the websites of some

23     companies you will see it's a growing industry. The

24     company can sign up with any one of these independent

25     alternative dispute resolution providers and they say   11:39

26     we will provide you with an arbitration service or a

27     mediation service or whatever it is and that's the

28     mechanism you adopt. You don't have to adopt any one

29     particular organisation that offers this service and

they are private sector operators who provide that
dispute resolution mechanism.

33 deals with removing people from the Privacy Shield
list who don't comply.  34 deals with the monitoring of
the Department of Commerce on the organisations that
are no longer members of the list.  35 refers at the
bottom of the page to:

"*Any misrepresentation of the general public by an*
*organisation concerning its adherence to the Principles*
*in the form of misleading statements or practices is*
*subject to enforcement action by the FTC, Department of*
*Transportation or other relevant US enforcement*
*authorities.*"

And it is also enforceable on the Department of
Commerce under the False Statements Act and it deals
with the ongoing monitoring by the Department of
Commerce.

2.3 deals with the redress mechanisms, complaint
handling and enforcement.  It says:

"*The EU-US Privacy Shield through the Recourse,*
*Enforcement and Liability Principles requires*
*organisations to provide recourse for individuals who*
*are affected by non-compliance and thus the possibility*
*for EU data subjects to lodge complaints regarding*

55

1    *non-compliance by US self-certified companies and to*

2    *have these complaints resolved, if necessary, by a*

3    *decision providing an effective remedy.*

4

5    *39.   As part of their self-certification, organisations*    11:40

6    *must satisfy the requirements of the Recourse,*

7    *Enforcement and Liability Principle by providing for*

8    *effective and readily available independent recourse*

9    *mechanisms by which each individual's complaints and*

10   *disputes can be investigated and expeditiously resolved*

11   *at no cost to the individual.*

12

13   *40.   Organisations may choose independent recourse*

14   *mechanisms in either the Union or in the United States.*

15   *This includes the possibility to voluntarily commit to*    11:40

16   *cooperate with the EU data protection authorities.*

17   *However, no such choice where organisations process*

18   *human resources data as cooperation with the DPAs is*

19   *then mandatory.   Other alternatives include independent*

20   *Alternative Dispute Resolution or private-sector*    11:40

21   *developed privacy programs that incorporate the Privacy*

22   *Principles into their rules."*

23

24   Over the page on 41 it says that there is a number of

25   options, therefore, open to individuals.  They can    11:41

26   bring a complaint directly to an organisation, so

27   that's to the company itself that has processed your

28   data, to an independent dispute resolution body

29   designated by an organisation, or to the national data

56

| | |
|---|---|
| 1 | protection authority itself or to the FTC if you want |
| 2 | them to go and prosecute or bring some action against |
| 3 | the company. |
| 4 | |
| 5 | 42:  "*In cases where their complaints have not been* <span style="float:right">11:41</span> |
| 6 | *resolved by any of these recourse or enforcement* |
| 7 | *mechanisms, individuals also have a right to invoke* |
| 8 | *binding arbitration under the Privacy Shield Panel.*" |
| 9 | |
| 10 | And that's in Annex 1:  "*Except for the arbitral panel,* <span style="float:right">11:41</span> |
| 11 | *which requires certain remedies to be exhausted before* |
| 12 | *it can be invoked, individuals are free to pursue any* |
| 13 | *or all of the redress mechanism of their choice, and* |
| 14 | *are not obliged to choose one mechanism over the other* |
| 15 | *or to follow a specific sequence.  However, there is a* |
| 16 | *certain logical order that is advisable to follow, as* |
| 17 | *set out below.* |
| 18 | |
| 19 | *43.  EU data subjects may pursue cases of* |
| 20 | *non-compliance with the principles through direct* <span style="float:right">11:42</span> |
| 21 | *contacts with the US <u>self-certified company</u>.*" |
| 22 | |
| 23 | So you go to the company in the first instance and see |
| 24 | how do you get on. |
| 25 | **MS. JUSTICE COSTELLO:**  Mm hmm. <span style="float:right">11:42</span> |
| 26 | **MR. MICHAEL COLLINS:**  44.  The organisation then must |
| 27 | provide a response within 45 days.  If that doesn't |
| 28 | work, at 45, it says: |
| 29 | |

57

1     *"Second, individuals can also bring a complaint*

2     *directly to the independent dispute resolution body*

3     *(either in the United States or in the Union)*

4     *designated by an organisation to investigate and*

5     *resolve individual complaints (unless they are*

6     *obviously unfounded or frivolous). Sanctions and*

7     *remedies imposed by such a body must be sufficiently*

8     *rigorous to ensure compliance by organisations with the*

9     *Principles and should provide for a reversal or*

10    *correction by the organisation of the effects of*

11    *non-compliance and, depending on the circumstances, the*

12    *termination of the further processing of the personal*

13    *data at stake and/or their deletion, as well as*

14    *publicity for findings of non-compliance."*

15                                                            11:42

16    At 46 it refers to the Department of Commerce verifying

17    that the companies do in fact have some independent

18    recourse mechanism in place and the consequences if

19    they fail. They must notify the non-compliance to the

20    Department of Commerce. The third option is at 48:   11:43

21    *"Individuals may also bring their complaints to a*

22    *National Data Protection agency."*

23

24    And at 49 it says: *"The advice of the DPAs will be*

25    *delivered through --"*                     11:43

26    **MS. JUSTICE COSTELLO:** Would that be within the EU or

27    within the US?

28    **MR. MICHAEL COLLINS:** No, within the EU. It's

29    primarily concerned with the complaints by *EU* citizens

| 1 | who have a complaint about the way their data is |
| 2 | processed in the US. |
| 3 | **MS. JUSTICE COSTELLO:** Yes. |
| 4 | **MR. MICHAEL COLLINS:** But you can go in the first |
| 5 | instance, if you wish, to your local data protection |
| 6 | authority in your own Member State. |
| 7 | |
| 8 | It says: "*The advice of the DPAs will be delivered* |
| 9 | *through an informal panel of DPAs established at Union* |
| 10 | *level, which will help to ensure a harmonised and* |
| 11 | *coherent approach to a particular complaint. Advice* |
| 12 | *will be issued after both sides in the dispute have had* |
| 13 | *a reasonable opportunity to comment and to provide any* |
| 14 | *evidence they wish. The panel will deliver advice as* |
| 15 | *quickly as the requirements for due process allows, and* |
| 16 | *as a general rule within 60 days after receiving a* |
| 17 | *complaint. If an organisation fails to comply within* |
| 18 | *25 days of delivery of the advice and has offered no* |
| 19 | *satisfactory explanation for the delay, the panel will* |
| 20 | *give notice of its intention either to submit the* |
| 21 | *matter to the FTC (or other competent U.S. enforcement* |
| 22 | *authority), or to conclude that the commitment to* |
| 23 | *cooperate has been seriously breached. In the first* |
| 24 | *alternative, this may lead to enforcement action based* |
| 25 | *on Section 5 of the FTC Act.*" |
| 26 | |
| 27 | That's I think the deceptive practices action: "*In the* |
| 28 | *second alternative, the panel will inform the* |
| 29 | *Department of Commerce which will consider the* |

11:43

59

*organisation's refusal to comply with the advice of the*

*DPA panel as a persistent failure to comply with the*

*lead to the organisation's removal from the Privacy*

*Shield list."*

11:44

So your local friendly data protection authority

doesn't decide the case in the sense of having the

power to determine it and impose some remedy.  It

considers the case, it gives advice to the organisation

and the parties who have made the complaint and          11:45

hopefully they will take that advice.  If they don't

then the data protection authority refers the matter to

the Federal Trade Commission in the United States and

it then takes action, either by taking such action as

it can itself in terms of its own sanctions of          11:45

enforcement for unfair or deceptive practice, or,

alternatively, it decides that the organisation is not

complying and it removes it from the Privacy Shield

list.

11:45

At 50 it says:  *"If the DPA to which the complaint has*

*been addressed has taken no or insufficient action to*

*address a complaint, the individual complainant has the*

*possibility to challenge such (in-) action in the*

*national courts."*                                       11:45

Fourth at 52:  *"The Department of Commerce has*

*committed to receive and review and undertake best*

*efforts to resolve complaints about an organisation's*

1    *non-compliance with the principles"* and the detail of

2    how that's going to be done is set out.

3

4    At 54:  *"Fifth, a Privacy Shield organisation must be*

5    *subject to the investigatory and enforcement powers of*    11:46

6    *US authorities, in particular the Federal Trade*

7    *Commission that will effectively ensure compliance with*

8    *the Principles."*

9

10   And at the end of that paragraph, it says:  *"The FTC*    11:46

11   *will accept complaints directly from individuals and*

12   *will undertake Privacy Shield investigations on its own*

13   *initiative, in particular as part of its wider*

14   *investigations of privacy issues."*

15                                                              11:46

16   And it can enforce compliance through administrative

17   orders.

18

19   56:  *"Sixth, as a recourse mechanism of 'last resort'*

20   *in case none of the other available redress avenues has*    11:46

21   *satisfactorily resolved an individual's complaint, the*

22   *EU data subject may invoke binding arbitration by the*

23   *'Privacy Shield Panel'.  Organisations must inform*

24   *individuals about that possibility."*

25                                                              11:46

26   And 57 goes on to describe that this is going to be a

27   pool of 20 arbitrators designated by the Department of

28   Commerce and the Commission and it sets out, there is

29   rules set out in the annexes as to how such an

61

1    arbitration is to be conducted.

2

3    At 58 it says:  "*The Privacy Shield panel will have the*

4    *authority to impose 'individual-specific, non-monetary*

5    *equitable relief' necessary to remedy non-compliance*          11:47

6    *with the Principles.*"

7

8    So you cannot award damages but you can make orders

9    saying you must stop the processing of this data that

10   you are engaged in or you must rectify the inaccurate       11:47

11   data or whatever the actual steps that must be taken.

12

13   Half way down 58, it says:  "*Arbitration may not be*

14   *invoked if a DPA has the legal authority to resolve the*

15   *claim at issue with respect to the US self-certified*         11:47

16   *company, namely in those cases where the organisation*

17   *is either obliged to cooperate and comply with the*

18   *advice of the DPAs as regards the processing of human*

19   *resources data collected in the employment context, or*

20   *has voluntarily committed to do so.*                         11:47

21

22   *59.   Seventh, where an organisation does not comply*

23   *with its commitment to respect the Principles, then*

24   *additional avenues for judicial redress may be*

25   *available under the law of the US, which provide for*         11:47

26   *legal remedies under tort law and in cases of*

27   *fraudulent misrepresentation, unfair or deceptive acts*

28   *or practices or breach of contract.*"

29


62

1     Then at 61, it says:  "*In the light of the information*
2     *in this section, the Commission considers that the*
3     *Principles issued by the US Department of Commerce as*
4     *such* - I think that should be 'are such' -- *as ensure a*
5     *level of protection of personal data that is*                11:48
6     *essentially equivalent to the one guaranteed by the*
7     *substantive basic principles laid down in Directive*
8     *95/46/EC.*"
9
10    And that of course is the whole basis of the decision.   11:48
11
12    Then at section 3, Judge, it goes on to deal with
13    access and use of personal data transferred under the
14    EU-US Privacy Shield by US public authorities.  And if
15    I just pause there.  So far what we have been concerned  11:48
16    with, Judge, are essentially private arrangements
17    whereby data is transferred to an organisation in the
18    US and there are private dispute resolution mechanisms
19    available of one sort or another where, if they fail,
20    you make complaint to the FTC who itself will then in    11:48
21    its own administrative functions carry out its
22    functions vis-à-vis the companies, but that of course
23    is not in itself the dispute between the private
24    individual and the company concerned, it's a public
25    enforcement of public law that the FTC then undertakes.  11:48
26
27    At 64 it says:  "*As follows from Annex II, section I5,*
28    *adherence to the Principles is limited to the extent*
29    *necessary to meet national security, public interest or*

63

1     *law enforcement requirements.*

2

3     *65.   The Commission has accessed the limitations and*

4     *safeguards available in US law as regards access and*

5     *use of personal data transferred under the EU-U.S.*

6     *Privacy Shield by US public authorities for national*

7     *security law enforcement and other public interest*

8     *purposes."*

9

10    Then it refers to the letter from the Secretary of

11    State and says:  "*The US government has also committed*

12    *to create a new oversight mechanism for national*

13    *security interference, the Privacy Shield Ombudsperson,*

14    *who is independent from the intelligence community."*

15

16    We will just look more closely, Judge, in just a moment

17    at the Ombudsman because his independence is in fact

18    one of the important points in the matter.

19

20    "*Finally, a representation from the U.S. Department of*

21    *Justice, contained in Annex VII to this decision,*

22    *describes the limitations and safeguards applicable to*

23    *access and use of data by public authorities for law*

24    *enforcement and other public interest purposes."*

25

26    Then at 67, it says:  "*The Commission's analysis shows*

27    *that US law contains a number of limitations on the*

28    *access and use of personal data transferred on the*

29    *EU-US Privacy Shield for national security purposes as*

1    *well as oversight and redress mechanisms that provide*
2    *sufficient safeguards for those data to be effectively*
3    *protected against unlawful interference and the risk of*
4    *abuse.   Since 2013, when the Commission issued its two*
5    *communications, this legal framework has been*                11:50
6    *significantly strengthened as described below."*

7

8    Then at 68:   *"Under the U.S. Constitution, ensuring*
9    *national security falls within the President's*
10   *authority as Commander in Chief, as Chief Executive*         11:50
11   *and, as regards foreign intelligence, to conduct U.S.*
12   *foreign affairs."*

13

14   That's under Article II of the Constitution:

15                                                                 11:50

16   *"While Congress has the power to impose limitations,*
17   *and has done so in various respects, within these*
18   *boundaries the President may direct the activities of*
19   *the U.S. Intelligence Community, in particular through*
20   *Executive Orders or Presidential Directives.   This of*
21   *course also applies in those areas where no*
22   *Congressional guidance exists.   At present, the two*
23   *central legal instruments in this regard are Executive*
24   *Order 12333 and Presidential Policy Directive 28. "*
25                                                                 11:51

26   Both of which of course we have referred to already.

27

28   *"PPD-28 issued on 17th January 2014 and imposes a*
29   *number of limitations for 'signals intelligence'*

65

1    *operations."*

2

3    And I will let the stenographers change, Judge.

4

5    Over the next two pages then, Judge, from about        11:51

6    paragraph 69 to about 75 or 76 it summarises PPD28 and

7    what it provides.  As I say, I've referred to that

8    yesterday and I'm not going to go over that again.  But

9    it says at 77 on page 20:

10

11   *"As a directive issued by the President as the Chief*

12   *Executive, these requirements bind the entire*

13   *Intelligence Community and have been further*

14   *implemented through agency rules and procedures that*

15   *transpose the general principles into specific*

16   *directions for day-to-day operations.  Moreover, while*

17   *Congress is itself not bound by PPD-28, it has also*

18   *taken steps to ensure that collection and access of*

19   *personal data in the United States are targeted rather*

20   *than carried out 'on a generalised basis'.*

21

22   *78. It follows from the available information,*

23   *including the representations received from the US*

24   *government, that once the data has been transferred to*

25   *organisations located in the United States and*

26   *self-certified under the EU-US Privacy Shield, US*

27   *intelligence agencies may only seek personal data where*

28   *their request complies with the Foreign Intelligence*

29   *Surveillance Act (FISA) or is made by the Federal*

66

1    *Bureau of Investigation (FBI) based on a so-called*
2    *National Security Letter (NSL).  Several legal bases*
3    *exist under FISA that may be used to collect (and*
4    *subsequently process) the personal data of EU data*
5    *subjects transferred under the EU-US Privacy Shield."*
6
7    Then it goes on to refer to some of the sections, such
8    as Section 215 and Section 702 and so on that we have
9    already referred to.
10                                                                    11:53
11   Over at page at 81 it refers to the Prism and Upstream
12   programmes, notes that Section 702 is going to be
13   reviewed in 2017.
14
15   *"82. Moreover, in its representations the US government*  11:53
16   *has given the European Commission explicit assurance*
17   *that the U.S. Intelligence Community 'does not engage*
18   *in indiscriminate surveillance of anyone, including*
19   *ordinary European citizens'."*
20
21   Then it deals with the requirements of PPD-28 as
22   regards access to collected data and data security.
23   84 deals with storage and further dissemination of
24   personal data and again recites what PPD-28 states with
25   regard to treating people with dignity and respect.        11:53
26   And at 85 it says:
27
28   *"In this respect, non-US persons will be treated in the*
29   *same way as US persons, based on procedures approved by*

67

1        *the Attorney-General."*

2

3        86 points out that dissemination is limited to cases

4        where the information is relevant to the underlying

5        purpose of the collection and thus responsive to an          11:54

6        authorised foreign intelligence or law enforcement

7        requirement and refers again in the footnote to Section

8        215.

9

10       87 says:                                                     11:54

11

12       "*According to the assurances given by the US*

13       *government, personal information may not be*

14       *disseminated solely because the individual concerned is*

15       *a non-US person and 'signals intelligence about the*

16       *routine activities of a foreign person would not be*

17       *considered foreign intelligence that could be*

18       *disseminated or retained permanently by virtue of that*

19       *fact alone unless it is otherwise responsive to an*

20       *authorized foreign intelligence requirement'.*

21

22       *88. On the basis of all of the above, the Commission*

23       *concludes that there are rules in place in the United*

24       *States designed to limit any interference for national*

25       *security purposes with the fundamental rights of the*

26       *persons whose personal data are transferred from the*

27       *Union to the United States under the EU-US Privacy*

28       *Shield to what is strictly necessary to achieve the*

29       *legitimate objective in question.*

68

1

2       *89. As the above analysis has shown, US law ensures*

3       *that surveillance measures will only be employed to*

4       *obtain foreign intelligence information — which is a*

5       *legitimate policy objective — and be tailored as much*

6       *as possible.  In particular, bulk collection will only*

7       *be authorised exceptionally where targeted collection*

8       *is not feasible, and will be accompanied by additional*

9       *safeguards to minimise the amount of data collected and*

10      *subsequent access...*

11

12      *90. In the Commission's assessment, this conforms with*

13      *the standard set out by the Court of Justice in the*

14      *__Schrems__ judgment, according to which legislation*

15      *involving interference with the fundamental rights*

16      *guaranteed by Articles 7 and 8 of the Charter must*

17      *impose 'minimum safeguards' and 'is not limited to what*

18      *is strictly necessary where it authorises, on a*

19      *generalised basis, storage of all the personal data of*

20      *all the persons whose data has been transferred from*

21      *the European Union' etc."*

22

23      Quoting from __Schrems__.  Section 312 then deals with

24      effective legal protection.  It says at 91:

25

26      "*The Commission has assessed both the oversight*

27      *mechanisms that exist in the United States with regard*

28      *to any interference by US intelligence authorities with*

29      *personal data transferred to the United States and the*

69

1    *avenues available for EU data subjects to seek*
2    *individual redress."*
3

4    First of all, it deals with the oversight procedures
5    under FISA.  There's -- subject to oversight from the     11:55
6    executive branch.  PPD-28 says there will be periodic
7    auditing.  There's other oversight layers at 95 -
8    Inspector Generals, the Office of the Director of
9    National Intelligence Civil Liberties and Privacy
10   Office, the PCLOB, which I think is the Privacy and       11:56
11   Civil Liberties Oversight Board and the President's
12   Intelligence Oversight Board.
13

14   "*These oversight functions are supported by compliance*
15   *staff in all the agencies.*
16

17   *96. As explained by the US government, civil liberties*
18   *or privacy officers with oversight responsibilities*
19   *exist at various departments with intelligence*
20   *responsibilities and intelligence agencies."*
21

22   In 97 it's explained that each intelligence community
23   element has its own Inspector General and describes
24   that they're statutorily independent.  It says at the
25   end of 97:                                                11:56
26

27   "*While the Inspectors General can only issue*
28   *non-binding recommendations for corrective action,*
29   *their reports, including on follow-up action... are*

70

1    *made public and moreover sent to Congress which can on*
2    *this basis exercise its oversight function.*
3
4    *98. Furthermore, the Privacy and Civil Liberties*
5    *Oversight Board, an independent agency within the*
6    *executive branch composed of a bipartisan, five-member*
7    *Board appointed by the President for a fixed six-year*
8    *term with Senate approval, is entrusted with*
9    *responsibilities in the field of counterterrorism*
10   *policies and their implementation, with a view to*
11   *protect privacy and civil liberties.  In its review of*
12   *Intelligence Community action, it may access all*
13   *relevant agency records, reports, audits."*
14
15   And so on.                                                    11:57
16
17   "*99. Finally, the aforementioned oversight mechanisms*
18   *are complemented by the Intelligence Oversight Board...*
19   *which oversees compliance by US intelligence*
20   *authorities with the Constitution."*                         11:57
21
22   At 101 it says:
23
24   "*These oversight functions are moreover supported by*
25   *extensive reporting requirements with respect to*
26   *non-compliance."*
27
28   And again refers to PPD-28.  At 102 it refers to the
29   House and Senate Intelligence and Judicial Committees,

| | |
|---|---|
| 1 | so that there's oversight from Congress.  And at 103 it |
| 2 | says later statutes have extended and refined the |
| 3 | reporting requirement and gives details of that.  And |
| 4 | at 104, under the USA Freedom Act of 2015, it must |
| 5 | disclose publicly the number of FISA orders and <span style="float:right">11:58</span> |
| 6 | directives received.  105 refers to the authorisation |
| 7 | that is required in circumstances from the FISA court, |
| 8 | and again we've gone through all of that yesterday, so |
| 9 | I'll move over that.  And it deals with other |
| 10 | provisions of FISA which we have dealt with.  It <span style="float:right">11:58</span> |
| 11 | contrasts it in paragraph 109 with Section 702 in FISA, |
| 12 | where the FISC does not authorise individual |
| 13 | surveillance measures, but authorises surveillance |
| 14 | programmes like Prism and Upstream.  And again we've |
| 15 | been through all of that yesterday and I don't think I <span style="float:right">11:58</span> |
| 16 | need deal with that. |
| 17 | |
| 18 | At page 31, Judge, there's a heading "Individual |
| 19 | Redress".  It says: |
| 20 | |
| 21 | "*A number of avenues are available under US law to EU* |
| 22 | *data subjects if they have concerns whether their* |
| 23 | *personal data have been processed... by US Intelligence* |
| 24 | *Community elements, and if so, whether the limitations* |
| 25 | *applicable in US law have been complied with.  These* |
| 26 | *relate essentially to three areas: Interference under* |
| 27 | *FISA; unlawful, intentional access to personal data by* |
| 28 | *government officials; and access to information under* |
| 29 | *Freedom of Information Act.* |

72

1

*112. First, the Foreign Intelligence Surveillance Act*
*provides a number of remedies, available also to non-US*
*persons, to challenge unlawful electronic*
*surveillance."*

And it refers to those, Judge.  And we've gone through
those and analysed those yesterday, so I don't need to
deal with that.

113 says:

*"Second, the US government referred the Commission to a*
*number of additional avenues that EU data subjects*
*could use to seek legal recourse against government*
*officials."*

And it refers there to the Computer Fraud and Abuse
Act, the Electronic Communications Privacy Act, which
we went through in detail yesterday, Judge, and Right
to Financial Privacy Act.  And all of these causes of
action, they say, are available under certain
conditions.

*"A more general redress possibility is offered by the*
*Administrative Procedure Act... according to which 'any*
*person suffering legal wrong...', is entitled to seek*
*judicial review."*

73

1     *"Finally, the US government has pointed to the FOIA as*

2     *a means for non-US persons to seek access to existing*

3     *federal agency records, including where these contain*

4     *the individual's personal data."*

5

6     At 115 then the Commission states:

7

8     *"While individuals, including EU data subjects,*

9     *therefore have a number of avenues of redress when they*

10    *have been the subject of unlawful (electronic)*

11    *surveillance for national security purposes, it is*

12    *equally clear that at least some legal bases that US*

13    *intelligence authorities may use (e.g. EO 12333) are*

14    *not covered.  Moreover, even where judicial redress*

15    *possibilities in principle do exist for non-US persons,*

16    *such as for surveillance under FISA, the available*

17    *causes of action are limited."*

18

19    And you see in the footnote 170 there, Judge, they

20    refer to the representations from the Director of     12:00

21    National Intelligence:

22

23    *"According to the explanations provided, the available*

24    *causes of action either require the existence of damage*

25    *or showing the government intends to use or disclose*    12:00

26    *information."*

27

28    And it describes again those statutory provisions that

29    we looked at yesterday and the requirements of

74

```
 1    intention and willfulness and so forth.  And it adds:
 2

 3    "However, as the Court of Justice has repeatedly
 4    stressed, to establish the existence of an interference
 5    with the fundamental right to privacy, it does not        12:00
 6    matter whether the person concerned" --
 7    MS. JUSTICE COSTELLO:  Sorry, which paragraph are you
 8    from now?
 9    MR. MICHAEL COLLINS:   Footnote 170, Judge.
10    MR. GALLAGHER:         It's 169.                          12:01
11    MR. MICHAEL COLLINS:   Is it?
12    MR. GALLAGHER:         It's on ours at 169.
13    MS. JUSTICE COSTELLO:  I've got the official journal
14    version, I think, and Mr. Gallagher's given me the
15    citation.                                                 12:01
16    MR. MICHAEL COLLINS:   Yes.  And I think I have, sorry,
17    I've probably -- yes, I have a version published by the
18    European Commission, but it may be, there may be some
19    slight difference, Judge.
20    MR. GALLAGHER:         There are.  There are             12:01
21    differences.
22    MR. MICHAEL COLLINS:   I see.  I'm terribly sorry about
23    that, Judge.
24    MS. JUSTICE COSTELLO:  No, not to worry.  So footnote
25    169 is the one you're reading from?                      12:01
26    MR. MICHAEL COLLINS:   It must be 169.  I'll take a
27    note of that.  Just at the end of that footnote, Judge,
28    it says:
29
```

75

1            *"However, as the Court of Justice has repeatedly*

2            *stressed, to establish the existence of an interference*

3            *with the fundamental right to privacy, it does not*

4            *matter whether the person concerned has suffered any*

5            *adverse consequence on account of that interference"*.    12:01

6            **MS. JUSTICE COSTELLO:**   Thank you.

7            **MR. MICHAEL COLLINS:**   Then in 116, Judge, they say:

8

9            *"In order to provide for an additional redress avenue*

10           *accessible for all EU data subjects"* -- sorry, Judge,   12:01

11           I've skipped...  Sorry, the end of 115 said:

12

13           *"And claims brought by individuals (including US*

14           *persons) will be declared inadmissible where they*

15           *cannot show 'standing'...*

16

17           *116. In order to provide for an additional redress*

18           *avenue accessible for all EU data subjects, the US*

19           *government has decided to create a new Ombudsperson*

20           *Mechanism as set out in the letter from the US*

21           *Secretary of State to the Commission which is contained*

22           *in Annex III to this decision.  This mechanism builds*

23           *on the designation, under PPD-28, of a Senior*

24           *Coordinator (at the level of Under-Secretary) in the*

25           *State Department as a contact point for foreign*

26           *governments to raise concerns regarding US signals*

27           *intelligence activities, but goes significantly beyond*

28           *this original concept.*

29

1    *117. In particular, according to the commitments from*

2    *the US government, the Ombudsperson Mechanism will*

3    *ensure that individual complaints are properly*

4    *investigated and addressed, and that individuals*

5    *receive independent confirmation that US laws have been*

6    *complied with or, in case of a violation of such laws,*

7    *the non-compliance has been remedied."*

8

9    If I pause there, Judge.  When we see the detail of it

10    in the annex, we'll see that that is quite important.    12:02

11    Because one might think from this that it says the

12    complaint has been properly investigated and addressed,

13    that the person who has the complaint is going to get

14    satisfaction of some sort in terms of understanding

15    what's happened, will see what the remedy is and    12:03

16    there'll be something done to assist him.  But in fact

17    what the Ombudsperson does is they simply tell you that

18    either US laws *have been complied with* – and they tell

19    you that in a broad sense – or they tell you 'The US

20    laws have *not* been complied with and we have taken    12:03

21    remedial action'.  But you're not told the detail of

22    what they've found is the individual noncompliance or

23    what the particular remedial action taken is.  Nor is

24    any particular remedy afforded to the individual in

25    question, other than the satisfaction perhaps of    12:03

26    knowing that the complaint has been investigated and

27    some unknown remedial action has been taken.

28    **MS. JUSTICE COSTELLO:**  This applies to where there's

29    been unlawful use of data transferred, is that right?

77

MR. MICHAEL COLLINS:   Well, where the allegation is
that there has been some breach of the, both the laws
and, presumably, the various principles that are
enunciated in PPD-28, for example, in terms of how the
data will be accessed and treated.                    12:04

It goes on:

"*The Mechanism includes 'the Privacy Shield*
*Ombudsperson', i.e. the Under-Secretary and further*
*staff as well as other oversight bodies competent to*
*oversee the different elements of the Intelligence*
*Community on whose cooperation the Privacy Shield*
*Ombudsperson will rely in dealing with complaints.*"

And we'll see from the detail later on the
Ombudsperson's role within the department.

"*In particular, where an individual's request relates*
*to the compatibility of surveillance with US law, the*
*Privacy Shield Ombudsperson will be able to rely on*
*independent oversight bodies with investigatory powers*
*(such as the Inspector-Generals or the PCLOB).  In each*
*case the Secretary of State ensures that the*
*Ombudsperson will have the means to ensure that its*
*response to individual requests is based on all the*
*necessary information.*

*118. Through this 'composite structure', the*

78

1      *Ombudsperson Mechanism guarantees independent oversight*
 2      *and individual redress.  Moreover, the cooperation with*
 3      *other oversight bodies ensures access to the necessary*
 4      *expertise.  Finally, by imposing an obligation on the*
 5      *Privacy Shield Ombudsperson to confirm compliance or*
 6      *remediation of any non-compliance, the mechanism*
 7      *reflects a commitment from the U.S. government as a*
 8      *whole to address and resolve complaint from EU*
 9      *individuals.*
10
11      *119. First, differently from a pure*
12      *government-to-government mechanism, the Privacy Shield*
13      *Ombudsperson will receive and respond to individual*
14      *complaints.  Such complaints can be addressed to the*
15      *supervisory authorities in the Member States competent*
16      *for the oversight of national security services and/or*
17      *the processing of personal data by public authorities*
18      *that will submit them to a centralised EU body from*
19      *where they will be channelled to the Privacy Shield*
20      *Ombudsperson.*"
21
22      So you make your complaint locally and the authorities
23      in your Member State will then transmit the complaint
24      onwards to the Ombudsperson.
25
26      "*This will in fact benefit EU individuals who can turn*
27      *to a national authority 'close to home' and in their*
28      *own language.  It will be the task of such an authority*
29      *to support the individual in making a request to the*

79

1    *Privacy Shield Ombudsperson that contains the basic*
2    *information and thus can be considered 'complete'.  The*
3    *individual does not have to demonstrate that his/her*
4    *personal data have in fact been accessed by the US*
5    *government through signals intelligence activities.*          12:05

6

7    *120. Second, the US government commits to ensure that,*
8    *in carrying out its functions, the Privacy Shield*
9    *Ombudsperson will be able to rely on the cooperation*
10   *from other oversight and compliance review mechanisms*
11   *existing in US law.  This will sometimes involve*
12   *national intelligence authorities, in particular where*
13   *the request is to be interpreted as one for access to*
14   *documents under the Freedom of Information Act.  In*
15   *other cases, particularly when requests relate to the*
16   *compatibility of surveillance with US law, such*
17   *cooperation will involve independent oversight bodies*
18   *(e.g. Inspector Generals) with the responsibility and*
19   *power to carry out a thorough investigation...  Also,*
20   *the Privacy Shield Ombudsperson will be able to refer*
21   *matters to the PCLOB for its consideration*" - that's
22   the oversight body - "*Where any non-compliance has been*
23   *found by one of these oversight bodies, the*
24   *Intelligence Community element*" - and I think the
25   phrase "Intelligence Community" is in fact a statutory     12:06
26   phrase, Judge, defined somewhere in the legislation -
27   "*(e.g. an intelligence agency) concerned will have to*
28   *remedy the non-compliance as only this will allow the*
29   *Ombudsperson to provide a 'positive' response to the*

80

1   *individual (i.e. that any non-compliance has been*

2   *remedied)."*

3

4   So just pausing there, Judge.  The Ombudsperson, if he

5   or she decides 'Yes, actually something *did* go wrong     12:07

6   here', he or she communicates with the organisation

7   concerned and satisfies themselves that some step has

8   been taken to remedy the matter.  And then on foot of

9   that, when they're so satisfied, they make what is

10  termed the positive response to the individual.  And     12:07

11  the positive response is to say 'The noncompliance of

12  which you have complained about has now been remedied'.

13  That's the extent of the satisfaction that you get from

14  the procedure.

15                                                            12:07

16  *"Also, as part of the cooperation, the Privacy Shield*

17  *Ombudsperson will be informed of the outcome of the*

18  *investigation, and the Ombudsperson will have the means*

19  *to ensure that it receives all the information*

20  *necessary to prepare its response.*

21

22  *121. Finally, the Privacy Shield Ombudsperson will be*

23  *independent from, and thus free from instructions by,*

24  *the US Intelligence Community."*

25

26  And I'll just ask you to hold that thought in your

27  head, Judge, when we look at the description given by

28  Secretary Kerry in the annex to the decision.

29

1     *"This is of significant importance, given that the*
2     *Ombudsperson will have to 'confirm' that (i) the*
3     *complaint has been properly investigated and that (ii)*
4     *relevant US law — including in particular the*
5     *limitations and safeguards... — has been complied with*
6     *or, in the event of non-compliance, such violation has*
7     *been remedied. In order to be able to provide that*
8     *independent confirmation, the Privacy Shield*
9     *Ombudsperson will have to receive the necessary*
10    *information regarding the investigation to assess the*
11    *accuracy of the response to the complaint. In*
12    *addition, the Secretary of State has committed to*
13    *ensure that the Under-Secretary will carry out the*
14    *function as Privacy Shield Ombudsperson objectively and*
15    *free from any improper influence liable to have an*
16    *effect on the response to be provided.*
17
18    *122. Overall, this mechanism ensures that individual*
19    *complaints will be thoroughly investigated and*
20    *resolved, and that at least in the field of*
21    *surveillance this will involve independent oversight*
22    *bodies with the necessary expertise and investigatory*
23    *powers and an Ombudsperson that will be able to carry*
24    *out its functions free from improper, in particular*
25    *political, influence. Moreover, individuals will be*
26    *able to bring complaints without having to demonstrate,*
27    *or just to provide indications, that they have been the*
28    *object of surveillance. In the light of these features,*
29    *the Commission is satisfied that there are adequate and*

82

1     *effective guarantees against abuse.*

2

3     *123. On the basis of all the above, the Commission*
4     *concludes that the United States ensures effective*
5     *legal protection against interferences by its*
6     *intelligence authorities with the fundamental rights of*
7     *the persons whose data are transferred from the Union*
8     *to the United States under the EU-US Privacy Shield."*

9

10    Then they refer to the **Schrems** judgment and quote from     12:09
11    it and say:

12

13    "*The Commission's assessment has confirmed that such*
14    *legal remedies are provided for in the United States,*
15    *including through the introduction of the Ombudsperson*
16    *mechanism."*

17

18    And they say in the framework of the Commission's
19    continued monitoring powers, the effectiveness will be
20    reassessed.                                                    12:09

21

22    The next section deals with access and use by US public
23    authorities for law enforcement and public interest
24    purposes.  And it says:

25

26    "*The US government (through the Department of Justice)*
27    *has provided assurance on the applicable limitations*
28    *and safeguards which in the Commission's assessment*
29    *demonstrate an adequate level of protection."*

83

1

2    And they deal, firstly, with the Fourth Amendment and

3    the necessity for showing probable cause.  At 127 they

4    say:

5

6    "*While the Fourth Amendment right does not extend to*

7    *non-US persons that are not resident in the United*

8    *States*" - and that's perhaps a simplification, as we've

9    seen, Judge, from what the test *actually* is - "*the*

10   *latter nevertheless benefit indirectly from its*

11   *protections, given that the personal data are held by*

12   *US companies with the effect that law enforcement*

13   *authorities in any event have to seek judicial*

14   *authorisation (or at least respect the reasonableness*

15   *requirement).*"

16

17   So I think what that means is that in terms of access

18   by authorities to US companies, the US companies have

19   the benefit of the Fourth Amendment, which somehow

20   indirectly gives protection to EU citizens.  At least

21   that seems to be the logic.

22

23   "*Further protections are provided by special statutory*

24   *authorities, as well as the Department of Justice*

25   *Guidelines, which limit law enforcement access to data*

26   *on grounds equivalent to necessity and proportionality*

27   *(e.g. by requiring that the FBI use the least intrusive*

28   *investigative methods feasible, taking into account the*

29   *effect on privacy and civil liberties).*"

1
2       And these are all what are set out in the
3       representations annex to the decision.
4
5       "*128. Although a prior judicial authorisation by a*
6       *court or grand jury (an investigate arm of the court*
7       *impanelled by a judge or magistrate)*" - it'd not in
8       fact a jury at all, Judge, or it's not, as you know, a
9       court or decision-making body - "*is not required in all*
10      *cases, administrative subpoenas are limited to specific*
11      *cases and will be subject to independent judicial*
12      *review.*"
13
14      Again you know all of this from the review that we've
15      gone through in the legislation.  Then it provides for,
16      refers to the other statutory provisions we've looked
17      at - the Freedom of Information Act, the Electronic
18      Communications Privacy Act and so forth.  It deals more
19      specifically with the provisions of the Electronic
20      Communications Privacy Act.  And then at section 4, on
21      page 38, dealing with adequate level of protection
22      under the EU-US Privacy Shield, at 136 it says:
23
24      "*In the light of the those findings, the Commission*
25      *considers that the United States ensures an adequate*
26      *level of protection for personal data transferred from*
27      *the Union to self-certified organisations in the United*
28      *States under the EU-US Privacy Shield.*
29

85

1    *137. In particular, the Commission considers that the*

2    *Principles issued by the U.S. Department of Commerce as*

3    *a whole ensure a level of protection of personal data*

4    *that is essentially equivalent to the one guaranteed by*

5    *the basic principles laid down in* [the Directive]."

6

7    And it says at 139 -- sorry, it refers to the

8    transparency obligations.  139 says it considers that:

9

10   "*Taken as a whole, the oversight and recourse*

11   *mechanisms... enable infringements of the Principles...*

12   *to be identified and punished in practice and offer*

13   *legal remedies to the data subject to gain access to*

14   *personal data relating to him and, eventually, to*

15   *obtain the rectification or erasure of such data.*

16

17   *140. Finally, on the basis of the available information*

18   *about the US legal order, including the representations*

19   *and commitments from the US*" --

20   **MS. JUSTICE COSTELLO:**  Just pause there about the        12:12

21   erasure.  Where did that arise?

22   **MR. MICHAEL COLLINS:**   Sorry, where does what arise,

23   Judge?

24   **MS. JUSTICE COSTELLO:**  It's at the end of paragraph

25   139.  I mean, I possibly haven't taken this in at the        12:12

26   --

27   **MR. MICHAEL COLLINS:**   Erasure.

28   **MS. JUSTICE COSTELLO:**  -- first reading.  It's talking

29   there about "to obtain the rectification or erasure of

86

| | |
|---|---|
| 1 | data."  Now, I heard the Ombudsperson was meant to say |
| 2 | 'Whatever may have been wrong before has been |
| 3 | rectified'. |
| 4 | **MR. MICHAEL COLLINS:**   Yes. |
| 5 | **MS. JUSTICE COSTELLO:**  Is that what they're referring   <span style="font-size:small">12:13</span> |
| 6 | to or not? |
| 7 | **MR. MICHAEL COLLINS:**   Well, I think that's what they |
| 8 | *are* referring to.  I think what they mean is, supposing |
| 9 | your complaint is that some data is being improperly |
| 10 | stored by a company, you won't be told exactly what has  <span style="font-size:small">12:13</span> |
| 11 | happened, you will simply be told 'Your complaint has |
| 12 | been remedied'.  But that *may* involve the erasure of |
| 13 | data, for example, if the data was being improperly |
| 14 | stored.  You won't be given that level of detail to be |
| 15 | told 'That's the thing we've done to bring about   <span style="font-size:small">12:13</span> |
| 16 | compliance with the law', but there are obviously |
| 17 | anticipating that that is something that could occur -- |
| 18 | **MS. JUSTICE COSTELLO:**  So the Commission is assuming |
| 19 | that that may be one of the remedies which the |
| 20 | Ombudsman achieves?   <span style="font-size:small">12:13</span> |
| 21 | **MR. MICHAEL COLLINS:**   Achieves, even though -- |
| 22 | **MS. JUSTICE COSTELLO:**  But doesn't tell the data |
| 23 | person -- |
| 24 | **MR. MICHAEL COLLINS:**   But doesn't tell the data |
| 25 | person --   <span style="font-size:small">12:13</span> |
| 26 | **MS. JUSTICE COSTELLO:**  -- that subject? |
| 27 | **MR. MICHAEL COLLINS:**   Exactly.  That's the case. |
| 28 | That's *my* understanding anyway, Judge. |
| 29 | **MS. JUSTICE COSTELLO:**  Thank you. |

1    MR. MICHAEL COLLINS:    140:

2

3    "*Finally, on the basis of the available information*

4    *about the US legal order, including the representations*

5    *and commitments from the US government, the Commission*

6    *considers that any interference by US public*

7    *authorities with the fundamental rights of the persons*

8    *whose data are transferred from the Union to the United*

9    *States under the Privacy Shield for national security,*

10   *law enforcement or other public interest purposes, and*

11   *the ensuing restrictions imposed on self-certified*

12   *organisations with respect to their adherence to the*

13   *Principles, will be limited to what is strictly*

14   *necessary to achieve the legitimate objective in*

15   *question, and that there exists effective legal*

16   *protection against such interference.*

17

18   *141. The Commission concludes that this meets the*

19   *standards of Article 25 of* [the Directive], *interpreted*

20   *in light of the Charter... as explained by the Court of*

21   *Justice in particular in* __Schrems__."

22

23   Then it deals with the necessity for the Commission to

24   be informed by Member States about actions taken by the

25   DPAs.  At the end of the page, 144:                          12:14

26

27   "*Consequently, a Commission adequacy decision adopted*

28   *pursuant to Article 25(6)... is binding on all organs*

29   *of the Member States to which it is addressed,*

1     *including their independent supervisory authorities.*

2     *Where such an authority has received a complaint*

3     *putting in question the compliance of a Commission*

4     *adequacy decision with the protection of the*

5     *fundamental right to privacy and data protection and*

6     *considers the objections advanced to be well founded,*

7     *national law must provide it with a legal remedy to put*

8     *those objections before a national court which, in case*

9     *of doubts, must stay proceedings and make a reference*

10     *for a preliminary ruling to the Court of Justice.*"

11

12     So that's, of course, acknowledging the point decided

13     in **Schrems** - Commission decisions are binding.  And

14     Hogan J's question was: Does that mean the DPA has to

15     just accept it? The answer was 'No, the DPA still has    12:15

16     to investigate it'; notwithstanding that there's a

17     Commission decision that says there *is* adequate

18     protection, you still have to look at it and, if you

19     have doubts about it, you have to bring it before the

20     court and you have to ask the court, if it shares the    12:15

21     doubts, to refer it on to the European Court.

22

23     So of course, this is a Commission decision where the

24     Commission is saying 'We think when you put all of this

25     together it does amount to adequate protection within    12:15

26     the meaning of Article 25 and 26'.  But that doesn't,

27     of course, exclude *at all* the jurisdiction that both

28     the Commissioner has and that you have to deal with the

29     matter.  Because this matter is coming before you,

first of all, with regard to the Standard Contractual
Clauses, albeit that I think they themselves could be
the subject of a complaint to the Ombudsman or
Ombudsperson, so there could be an intersection between
them.  But secondly, this is then a factor that one
takes into account and one says, you conceivably could
say 'Actually, in light of all of this, I'm completely
satisfied that there's no doubt whatsoever that there's
adequate compliance and I'm not going to make a
reference to the European Court'.  And you could do
that, that's the argument Mr. Gallagher will be urging
upon you, and some of the amici.

But equally you have to look at it from the viewpoint
that even within the Privacy Shield decision itself,
the Commission has expressly adverted to the fact that
notwithstanding that Commission decisions are binding
in what they've said, there is still this obligation
to, if the complaint is made, to bring it before the
court and for the court to refer it to the European
Court of Justice if it still considers there are
concerns.

So one way perhaps to look at it, Judge, is to
consider, leaving aside the point that I rely upon that
this postdates the Commissioner's decision and the
analysis in terms of the Standard Contractual Clauses,
one way to look at it is to say supposing you were
satisfied, absent the Privacy Shield, that there wasn't

90

| | |
|---|---|
| 1 | in fact, or there's certainly a question that deserved |
| 2 | to be referred to the European Court about adequacy, |
| 3 | does this Ombudsperson mechanism remedy the concerns |
| 4 | and satisfy all those concerns or is there still a |
| 5 | concern that's worthy of reference? 12:17 |
| 6 | |
| 7 | And it is fundamentally the Ombudsperson mechanism that |
| 8 | one is concerned with.  Because the other mechanisms |
| 9 | are essentially a form of private remedy mechanisms |
| 10 | between individual companies in the US who sign up for 12:17 |
| 11 | the Privacy Shield principles, some of whom may, some |
| 12 | of whom may not, some of whom may only sign up for the |
| 13 | principles in relation to some aspects of the transfer |
| 14 | of their data and not in respect of other aspects.  So |
| 15 | in terms of a complaint about what the US Government is 12:17 |
| 16 | doing and what US agencies are doing, the Ombudsperson |
| 17 | mechanism is the one that one has to consider.  And |
| 18 | that's why I'm going to look in just a moment at the -- |
| 19 | **MS. JUSTICE COSTELLO:**  And you were saying that |
| 20 | obviously this case was concerning the Standard 12:17 |
| 21 | Contractual Clauses. |
| 22 | **MR. MICHAEL COLLINS:**  Yes. |
| 23 | **MS. JUSTICE COSTELLO:**  So I think you said at the |
| 24 | beginning that you felt that the Privacy Shield didn't |
| 25 | apply, that this decision didn't apply because it -- is 12:18 |
| 26 | that what you said? I didn't -- |
| 27 | **MR. MICHAEL COLLINS:**   If I did, I didn't quite mean to |
| 28 | say that, Judge. |
| 29 | **MS. JUSTICE COSTELLO:**  No, I may -- I've misunderstood |

91

| | |
|---|---|
| 1 | you.  How does this decision relate to the Standard |
| 2 | Contractual Clauses, in your opinion? |
| 3 | **MR. MICHAEL COLLINS:**   First of all, the data transfers |
| 4 | that Facebook have been making and are continuing to |
| 5 | make continue to be made pursuant to the Standard |
| 6 | Contractual Clauses.  In other words, that's the |
| 7 | mechanism that they say they adopt for the purpose of |
| 8 | saying they meet -- they're making a lawful transfer |
| 9 | under Article 25 and 26.  And of course, it *is* a lawful |
| 10 | transfer for so long as the SCC decisions are there and |
| 11 | are valid decisions, transfers under them are lawful. |
| 12 | So Facebook are correct in saying that the transfers |
| 13 | they're making at the moment are lawful. |
| 14 | |
| 15 | What I'm saying is that they are not making the |
| 16 | transfers insofar as what the Commissioner was dealing |
| 17 | with, the transfers were not being made pursuant to the |
| 18 | Privacy Shield arrangement, they were being made |
| 19 | pursuant to the Standard Contractual Clauses.  And that |
| 20 | is what the Commissioner's decision is about.  And it's |
| 21 | the validity of those Standard Contractual Clauses is |
| 22 | all that she's asking to be referred to, albeit that it |
| 23 | would be impossible, I think, not to know and take |
| 24 | account of - and that's why I'm opening it to you - the |
| 25 | fact of the Privacy Shield. |
| 26 | |
| 27 | But where I think there is this interconnection, I'm |
| 28 | assuming - and I'm open to correction on this, because |
| 29 | I just don't know exactly how it's going to work - but |

12:18
12:18
12:18
12:19
12:19

92

1    supposing somebody had a complaint, an EU citizen had a
2    complaint to say 'You're not complying with the
3    Standard Contractual Clauses', that that mechanism is
4    breaking down, the company, Facebook Inc. in the US is
5    not complying with it; I presume it would be possible    12:19
6    to make that complaint through the Ombudsperson
7    mechanism and to seek to have that complaint
8    ventilated.
9
10   So to that extent, it's been overtaken by events in the  12:19
11   sense that this would appear to provide a mechanism
12   that could be availed of since it is now in force,
13   since the decision is in force.  But as a matter of
14   principle, the SCCs are a different avenue by which the
15   transfer of data is lawful under the Directive.  The --  12:20
16   **MS. JUSTICE COSTELLO:**  So it's not that the transfers
17   are being availed of, but that it sets a scenario where
18   there's another remedy?
19   **MR. MICHAEL COLLINS:**   Exactly so.  And I think it's
20   also the case, Judge, I think Facebook - Mr. Gallagher   12:20
21   will know better than this and can explain it - but I
22   think Facebook *do* make some transfers now by availing
23   of the Privacy Shield and there are, I think, some
24   transfers - not all, I think, but some transfers - that
25   they do pursuant to the Privacy Shield.  But as I say,   12:20
26   that's something that can be perhaps explained in a
27   little more detail.
28
29   Section six then, Judge, deals with, at 145 says:

1

2          "*In the light of the fact that the level of protection*

3          *afforded by the US legal order may be liable to change,*

4          *the Commission, following adoption of this decision,*

5          *will check periodically whether the findings relating*

6          *to the adequacy of the level of protection ensured by*

7          *the United States under the EU-US Privacy Shield are*

8          *still factually and legally justified. Such a check is*

9          *required, in any event, when the Commission acquires*

10         *any information giving rise to a justified doubt in*

11         *that regard.*"

12

13         It then goes on to describe the continuing monitoring

14         that's going to be put in place. The US Government has

15         committed to keep the Commission informed of material          12:21

16         developments in US law in relation to the Privacy

17         Shield and the Commission will assess the level of

18         protection following the entry into application of the

19         GDPR. And again that's of some importance, because the

20         GDPR in some important respects, Judge, strengthens the        12:21

21         level of data protection for EU citizens in Europe. So

22         the bar is raise add little higher, if I can put it

23         that way, when the GDPR comes into force in 2018, and

24         so another assessment will have to be done to see

25         whether the Privacy Shield mechanism adequately meets          12:21

26         the requirements of the GDPR.

27

28         Then it sets out arrangements that will be made,

29         including the Article 29 Working Party for this

94

1    monitoring.  There's an annual joint review as referred

2    to in 148 where:

3

4    "*The Commission will request that the Department of*

5    *Commerce provides comprehensive information on all*

6    *relevant aspects of the functioning of the EU-US*

7    *Privacy Shield, including referrals received by the*

8    *Department of Commerce from DPAs and the results of ex*

9    *officio compliance reviews.*"

10

11   And then the Commission will prepare a public report.

12   Section 7, Judge - happily, coming to the end of this

13   now - says: "*Where, on the basis of*" -- it's headed

14   "Suspension of the Adequacy Decisions":

15

16   "*Where, on the basis of the checks or of any other*

17   *information available, the Commission concludes that*

18   *the level of protection offered by the Privacy Shield*

19   *can no longer be regarded as essentially equivalent to*

20   *the one in the Union, or where there are clear*

21   *indications that effective compliance with the*

22   *Principles in the United States might no longer be*

23   *ensured, or that the actions of US public authorities*

24   *responsible for national security or the prevention,*

25   *investigation, detection or prosecution of criminal*

26   *offenses do not ensure the required level of*

27   *protection, it will inform the Department of Commerce*

28   *thereof and request that appropriate measures are taken*

29   *to swiftly address any potential non-compliance with*

1    *the Principles within a specified, reasonable*
2    *timeframe.  If, after the expiration of the specified*
3    *timeframe, the US authorities fail to demonstrate*
4    *satisfactorily that the EU-US Privacy Shield continues*
5    *to guarantee effective compliance and an adequate level*
6    *of protection, the Commission will initiate the*
7    *procedure leading to the partial or complete suspension*
8    *or repeal of this decision.  Alternatively, the*
9    *Commission may propose to amend this decision, for*
10   *instance by limiting the scope of the adequacy finding*
11   *only to data transfers subject to additional*
12   *conditions.*

14   *151. In particular, the Commission will initiate the*
15   *procedure for suspension or repeal in case of:*

17   *(a) indications that the US authorities do not comply*
18   *with the representations and commitments contained in*
19   *the documents annexed to this decision, including as*
20   *regards the conditions and limitations for access by*
21   *U.S. public authorities for law enforcement, national*
22   *security and other public interest purposes to personal*
23   *data transferred under the Privacy Shield;*
24   *(b) failure to effectively address complaints by EU*
25   *data subjects; in this respect, the Commission will*
26   *take into account all circumstances having an impact on*
27   *the possibility for EU data subjects to have their*
28   *rights enforced, including, in particular, the*
29   *voluntary commitment by self-certified US companies to*

1    *cooperate with the DPAs...*

2    *(c) failure by the Privacy Shield Ombudsperson to*

3    *provide timely and appropriate responses.*"

4

5    And it goes on to say they'll also consider initiating    12:24

6    the procedure leading to the amendment or the repeal of

7    the decision if they fail to get the necessary

8    information and clarifications for the assessment or

9    compliance with the principles, the effectiveness of

10   complaint handling procedures or, perhaps importantly,    12:24

11   any lowering of the required level of protections as a

12   consequence of actions by US national intelligence

13   authorities, in particular as a consequence of the

14   collection or access to personal data that's not

15   limited to what's strictly necessary or appropriate.    12:24

16   And then it refers to the Working Party.

17

18   So it's on that basis it then adopts the decision that

19   I've already opened to you, Judge.  And then there are

20   the various annexes and representations.  They're all    12:24

21   effectively summarised in the introduction and,

22   therefore, I'm not going to go through them.  The only

23   one I want to go through, Judge, is the one involving

24   the Ombudsperson mechanism itself, which is the letter

25   from the Secretary of State John Kerry.  Sorry, Judge,    12:25

26   I've just misplaced it.

27   **MR. GALLAGHER:**        Page 71 in ours.

28   **MR. MICHAEL COLLINS:**   I'm actually back on the

29   official one here.  I think it's page 71, Judge.

97

1    **MS. JUSTICE COSTELLO:**  Yes, I have it.  I put a yellow

2    sticky on it when we were going through it the first

3    time.

4    **MR. MICHAEL COLLINS:**   Yes, I had too, but I just

5    haven't marked it.  On page 72, Judge, after the --          12:25

6    well, sorry, the letter is of importance, I should read

7    the letter I think.  It says:

8

9    "*Dear Commissioner Jourová*

10                                                               12:26

11    *I am pleased we have reached an understanding on the*

12    *EU-US Privacy Shield that will include an Ombudsperson*

13    *mechanism through which authorities in the EU will be*

14    *able to submit requests on behalf of EU individuals*

15    *regarding US signals intelligence practices.*              12:26

16

17    *On January 17 2004 President Obama announced important*

18    *intelligence forms... PPD-28.  Under PPD-28 I*

19    *designated Under Secretary of State Catherine A.*

20    *Novelli, who also serves a Senior Coordinator*            12:26

21    *International Information Technology Diplomacy, as our*

22    *point of contact for foreign governments that wish to*

23    *raise concerns regarding US signal intelligence*

24    *activities.  Building on this role, I have established*

25    *a Privacy Shield Ombudsperson mechanism in accordance*     12:26

26    *with the terms set out in Annex A, which have been*

27    *updated.*"

28

29    And he's directed Under Secretary Novelli to perform

1     this function.

2

3     "*Under Secretary Novelli is independent from the US*

4     *Intelligence Community and reports directly to me.*"

5                                                                    12:26

6     And he's directed his staff to devote the necessary

7     resources to it and so on.

8

9     Over the page, Judge, halfway down, at paragraph one:

10                                                                   12:26

11    "*The Senior Coordinator will serve as the Privacy*

12    *Shield Ombudsperson and designate additional State*

13    *Department officials as appropriate to assist in her*

14    *performance of the responsibilities detailed in this*

15    *memorandum.  The Privacy Shield Ombudsperson will work*    12:27

16    *closely with the appropriate officials from other*

17    *Departments who are responsible for processing*

18    *requests.  The Ombudsperson is independent from the*

19    *Intelligence Community.  The Ombudsperson reports*

20    *directly to the Secretary of State, who will ensure*      12:27

21    *that the Ombudsperson carries out its function*

22    *objectively and free from improper influence that is*

23    *liable to have an effect on response to be provided.*"

24

25    So the Ombudsperson, Judge, is independent, it is said,    12:27

26    from the Intelligence Community, although looked at in

27    a moment at the connection between the Intelligence

28    Community and the Secretary of State or the Department

29    of State, but clearly not independent in the sense of

99

the way a judge is independent as appointed from the
government, because it is, in effect, a public servant
who is responsible to the Secretary of State.

"*2. Effective*" -- sorry, Judge, could I just take          12:27
instructions on one aspect that I've presumably made a
bags of? Sorry, Mr. Young has quite rightly directed my
attention, Judge, to the previous paragraph, which
explains the connection between the SCCs and the
Ombudsperson mechanism that I was trying to explain a        12:28
moment ago and no doubt *was* making a bags of it.  It
says:

"*This memorandum describes a new mechanism that the
Senior Coordinator will follow to facilitate the*           12:28
*processing of requests relating to national security*
*access to data transmitted from the EU to the US*
*pursuant to the Privacy Shield Standard Contractual*
*Clauses, binding corporate rules*" - that's one of the
other avenues of transfer - "*derogations or possible*      12:28
*future derogations through established avenues under*
*applicable US laws and policy and the response to those*
*requests.*"

So the Ombudsperson can deal with the SCC avenue of          12:28
transfer, but if you've got a complaint about how that
avenue of transfer is operating, you can make a
complaint through this Ombudsperson mechanism.

1     "*2. Effective coordination.*

2     *The Privacy Shield Ombudsperson will be able to*

3     *effectively use and coordinate with the mechanisms and*

4     *officials described below, in order to ensure that the*

5     *Ombudsperson's response to requests from submitting EU*     12:29

6     *individual complaints to handling bodies is based on*

7     *the necessary information.  When the request relates to*

8     *the compatibility of surveillance of the US law, the*

9     *Privacy Shield Ombudsperson will be able to co-operate*

10    *with one of the independent oversight bodies with*     12:29

11    *investigatory powers.*"

12

13    She'll work closely with the other US Government

14    officials, as is said in (a).  (b), the US government

15    will rely on mechanisms for coordinating and overseeing     12:29

16    national security matters interests across departments

17    and agencies to help ensure that she's able to respond.

18    She may refer other matters to the Privy and Civil

19    Liberties Oversight Board for consideration.

20                                                            12:29

21    Then it deals with the procedure, Judge, submitting

22    requests:

23

24    "*A request will initially be submitted to the*

25    *supervisory authorities in the Member States competent*     12:29

26    *for the oversight of national security services and/or*

27    *the processing of personal data by public authorities.*

28    *The request will be submitted to the Ombudsperson by an*

29    *EU centralised body*" - called the EU Individual

101

| | |
|---|---|
| 1 | Complaints Handling Body. |
| 2 | |
| 3 | So the complaint is transmitted at EU level to state |
| 4 | level rather than from the individual directly to the |
| 5 | Ombudsperson. Then the EU Individual Complaint |
| 6 | Handling Body ensures that the request is complete and |
| 7 | sets out the various things that would need to be put |
| 8 | in place to make sure the request can be processed. |
| 9 | There are commitments set out at 4 to communicate with |
| 10 | the submitting EU Individual Complaints Handling Body. |
| 11 | |
| 12 | Over the page, Judge, at paragraph (e) it says: |
| 13 | |
| 14 | "Once a request has been completed as described in |
| 15 | section three of this memorandum, the Privacy Shield |
| 16 | Ombudsperson will provide in a timely manner an |
| 17 | appropriate response to the submitting EU Individual |
| 18 | Complaints Handling Body subject to the continuing |
| 19 | obligation to protect information under applicable laws |
| 20 | and policies. The Privacy Shield Ombudsperson will |
| 21 | provide a response to the submitting EU individual |
| 22 | complaint handling body confirming (1) that the |
| 23 | complaint has been properly investigated and (2) that |
| 24 | the US law, Statutes, Executive Orders, Presidential |
| 25 | Directives and Agency Policies providing the |
| 26 | limitations and safeguards described in the Office of |
| 27 | the Director of National Intelligence letter have been |
| 28 | complied with, or in the event of noncompliance, that |
| 29 | such noncompliance has been remedied." |

12:30
12:30
12:30
12:30
12:31

So you get a letter with two things: 'We have properly
investigated your complaint' and 'All the laws,
policies, Presidential Directives and so on of the
United States have been properly complied with', or 'if       12:31
they haven't been properly complied with, that
noncompliance has been remedied'.  And that's the
extent of the information and the decision that you
get.  And in particular it goes on then to be express
about it, Judge:                                              12:31


"*The Privacy Shield on Ombudsperson will neither*
*confirm nor deny whether the individual has been the*
*target of surveillance.*"
                                                              12:31

And that, of course, is understandable why that would
be so, Judge.  Because otherwise a terrorist could find
out 'Am I being the subject of targeted surveillance or
not?' by simply submitting a complaint.  So I'm not
necessarily criticising the fact that this is so, but        12:32
I'm just saying from the perspective of the ordinary EU
citizen who has a complaint about data processing, what
does he get and how does it look at it from his or her
perspective?
                                                              12:32

"*Nor will the Privacy Shield Ombudsperson confirm the*
*specific remedy that was applied.  As further explained*
*in Section 5, Freedom of Information requests will be*
*processed as provided for under the statute and the*

103

1    *applicable regulations.  The Privacy Shield*
2    *Ombudsperson will communicate directly with the EU*
3    *Individual Complaints Handling Body who will be*
4    *responsible for communicating with the individual*
5    *submitting the request."*                              12:32

6

7    At (g) it says:

8

9    "*Commitments in this memorandum will not apply to*
10   *general claims that the EU-US Privacy Shield is*        12:32
11   *inconsistent with European Union data protection*
12   *requirements.  Commitments in this memorandum are made*
13   *based on the common understanding by the Commission and*
14   *the US Government that given the scope of the*
15   *commitments under this mechanism, there may be resource* 12:33
16   *constraints that arise, including with respect to the*
17   *Freedom of Information Act requests.  Should the*
18   *carrying out of the Privacy Shield Ombudsperson's*
19   *functions exceed reasonable resource constraints and*
20   *impede the fulfillment of these commitments, the US*     12:33
21   *Government will discuss with the Commission any*
22   *adjustments that may be necessary."*

23

24   Then it deals with the processing of requests for
25   information over the page at six.  There can be            12:33
26   requests for further action, including a request
27   alleging violation of law or other misconduct will be
28   referred to the appropriate US Government body,
29   including the independent oversight bodies.  And it

104

1    refers to those oversight bodies such as Inspectors

2    General, the Privacy and Civil Liberties Offices and so

3    on and the Office of Privacy and Civil Liberties at the

4    Department of Justice.

5                                                      12:33

6    So that's the way the Ombudsperson mechanisms works,

7    Judge.  It's a person who is responsible to the

8    Secretary of State and who operates, I think, within

9    the Secretary of State.  And of course, the Secretary

10   of State ultimately has the responsibility in relation   12:34

11   to the Intelligence Community as well, but the

12   Ombudsperson is intended to be independent from the

13   Intelligence Community as such and operates outside -

14   in other words, outside the National Intelligence

15   Agency, the CIA, the FBI and all the other agencies      12:34

16   that are concerned.

17

18   The issue in present circumstances, Judge, is, when one

19   is looking at the question of adequacy and in terms of

20   analysing whether the legal rules that are referred to   12:34

21   and the mechanisms of compliance with those legal rules

22   as contemplated under *our* interpretation of Articles 25

23   and 26, whether this has any significant impact on that

24   analysis.

25                                                      12:34

26   We respectfully say, Judge, that, first of all, the

27   Privacy Shield mechanism is not a matter of law within

28   the United States or United States law, it's a matter

29   of a series of commitments that have been given to the

105

| 1 | European Commission which the European Commission have |
| 2 | said that they rely upon, but reserve the right to |
| 3 | repeal their decision if those commitments are departed |
| 4 | from, if it looks as if those policies are not being |
| 5 | implemented.  And significant reliance is, of course, | 12:35 |
| 6 | placed on the Presidential and Executive Orders and in |
| 7 | particular PPD-28 and the way in which the US |
| 8 | Government is going to approach it, as set out in |
| 9 | PPD-28 and matters of that sort. |
| 10 | | 12:35 |
| 11 | So I respectfully say that while undoubtedly it would |
| 12 | be wrong to proceed without knowledge of the Privacy |
| 13 | Shield mechanism that is there, the essential question |
| 14 | remains as I've outlined to you at the start of these |
| 15 | proceedings. | 12:35 |
| 16 | **MR. GALLAGHER:**          Judge, I'm sorry to interrupt |
| 17 | Mr. Collins.  Of course he's right to draw your |
| 18 | attention to the Privacy Shield.  He just made one |
| 19 | remark that's incorrect, that the Secretary of State, |
| 20 | he said the Ombudsman is part of the Secretary of State | 12:35 |
| 21 | apparatus and the Secretary of State is head of the |
| 22 | Intelligence Community.  Just as a matter of fact, |
| 23 | that's incorrect.  It's not. |
| 24 | **MS. JUSTICE COSTELLO:**  I thought he said they reported |
| 25 | to him, but maybe I missed -- | 12:36 |
| 26 | **MR. GALLAGHER:**          They reported to him, exactly. |
| 27 | But he said he is then head of the Intelligence |
| 28 | Community, which is not the case. |
| 29 | **MR. MICHAEL COLLINS:**  Oh, I'm sorry.  If I said that, |

|    |                                                              |       |
|----|--------------------------------------------------------------|-------|
| 1  | I misspoke.  I think the President is the person who is      |       |
| 2  | ultimately responsible for the Intelligence Community.      |       |
| 3  | But my understanding is that the intelligence agencies      |       |
| 4  | themselves report to the Secretary of State, as does        |       |
| 5  | the Ombudsperson, if I'm right about that.  Am I wrong       | 12:36 |
| 6  | about that?                                                  |       |
| 7  | **MR. GALLAGHER:**        I understand you are.              |       |
| 8  | **MR. MICHAEL COLLINS:**  Sorry, am I right or wrong?        |       |
| 9  | **MR. GALLAGHER:**        I understand you're *wrong* about  |       |
| 10 | it, sorry.                                                   | 12:36 |
| 11 | **MR. MICHAEL COLLINS:**  Oh, I'm wrong? Okay.  Well, I'm    |       |
| 12 | sorry, Judge, I'll take instructions over lunch just to      |       |
| 13 | make sure I get that right.  Because I certainly don't       |       |
| 14 | want to say anything that's wrong in that respect.          |       |
| 15 |                                                              | 12:36 |
| 16 | The Article 29 Working Group, Judge, which was looking      |       |
| 17 | at all of this, it had expressed concerns when the          |       |
| 18 | Privacy Shield arrangement was being negotiated and,        |       |
| 19 | subsequent to the Privacy Shield arrangement, it            |       |
| 20 | expressed its concerns in the form of a note that           | 12:36 |
| 21 | I'll -- I'm not sure it's in your books, Judge, it's        |       |
| 22 | the Article 29 Working Party statement.  And I think        |       |
| 23 | I'll just hand in a loose copy of it, Judge, it's very      |       |
| 24 | short, it's just a one-page statement (Same Handed).        |       |
| 25 | **MS. JUSTICE COSTELLO:**  Thank you.                        | 12:37 |
| 26 | **MR. MICHAEL COLLINS:**   This was issued on 1st July 2016  |       |
| 27 | when the Privacy Shield arrangement came into force.        |       |
| 28 | And it says:                                                 |       |
| 29 |                                                              |       |

107

1    "*On 12th July 2016 the European Commission adopted*
2    *EU-US Privacy Shield Adequacy Decision.  The WP29*
3    *welcomes the improvements brought by the Privacy Shield*
4    *mechanism prepared for the __Safe Harbour__ decision.  In*
5    *its opinion WP238 on the draft EU-US Privacy Shield*          12:37
6    *adequacy decision, the WP29 expressed concerns and*
7    *asked for various clarifications.  The WP29 commends*
8    *the Commission and the US authorities for having take*
9    *them into consideration in the final version of the*
10   *Privacy Shield documents.  However, a number of these*       12:37
11   *concerns remain regarding both the commercial aspects*
12   *and the access by US public authorities to data*
13   *transferred from the EU.*

15   *Concerning commercial aspects, the WP29 regrets, for*        12:37
16   *instance, the lack of specific rules on automated*
17   *decisions and of a general right to object.  It also*
18   *remains unclear how the Privacy Shield principle shall*
19   *apply to processors.  Concerning access by public*
20   *authorities to data transferred to the US under the*         12:38
21   *Privacy Shield, the WT29 would have expected stricter*
22   *guarantees concerning the independence and powers of*
23   *the Ombudsperson mechanism.*

25   *Regarding bulk collection of personal data, WP29 notes*      12:38
26   *the commitment of the ODNI not to conduct mass and*
27   *indiscriminate collection of personal data.*
28   *Nonetheless, it regrets the lack of concrete assurances*
29   *that such practice does not take place.*

1

2      *The first joint annual review will therefore be a key*

3      *moment for the robustness and efficiency of the Privacy*

4      *Shield mechanism to be further assessed.  In this*

5      *regard, the competence of DPAs in the course of the*          12:38

6      *joint review should be clearly defined.  In particular,*

7      *all members of the Joint Review Team shall have the*

8      *possibility to directly access all of the information*

9      *necessary for the performance of their review,*

10     *including elements allowing a proper evaluation of the*        12:38

11     *necessity and proportionality of the collection and*

12     *access to data transferred by public authorities.*

13

14     *When participating in the review, the national*

15     *representatives of WP29 will not only assess if the*          12:38

16     *remaining issues have been solved, but also if the*

17     *safeguards under the EU-US Privacy Shield are workable*

18     *and effective.  The results of the first joint review*

19     *regarding access by US public authorities to data*

20     *transferred under the Privacy Shield may also impact*         12:39

21     *transfer tools, such as binding corporate rules and*

22     *Standard Contractual Clauses.*

23

24     *In the meantime and now the Privacy Shield has been*

25     *adopted and with the Schrems judgment and opinion WP238*  12:39

26     *in mind, the DPAs within WP 29 commit themselves to*

27     *pro-actively and independently assist the data subjects*

28     *to exercise their rights under the Privacy Shield*

29     *mechanism."*

109

1
2      And they set out various links and so forth.  There
3      have been --
4      **MS. JUSTICE COSTELLO:**  Can you just refresh me as to
5      who is comprised in the Article 29 Working Party?          12:39
6      **MR. MICHAEL COLLINS:**   They are, as I understand it,
7      representatives of all the Data Protection Authorities
8      across Europe who operate -- they certainly input into
9      it.  I think there may be other people on WP29 as well,
10     but I think it's primarily made up of representatives     12:39
11     of the Data Protection Authorities from the Member
12     States.  I can get the detail for you over lunch as to
13     exactly who is on that, Judge.
14
15     I'm not going to go into any detail in relation to        12:40
16     this, Judge, but just to note that two actions have
17     been brought against the European Commission alleging
18     in one form or another that the decision is invalid as
19     contrary to Articles 7 and 8 and 47 of the Charter.
20     One of those decisions is brought by a French             12:40
21     organisation called <u>La Quadrature du Net and Others -v-</u>
22     <u>Commission</u>.  That action was brought on 25th October
23     2016, Judge, it's case T738/16.  And the other action
24     was brought on 16th September 2016 and that was brought
25     by <u>Digital Rights Ireland -v- Commission</u>.  And there's   12:40
26     questions still of the admissibility of those claims or
27     things still have to be determined, but just to be
28     aware of the fact that both of those...
29     **MS. JUSTICE COSTELLO:**  Who brought these proceedings

110

1    where? You told me what they're called, but --

2    **MR. MICHAEL COLLINS:**  Before the European Court of

3    Justice, or the Court of Justice, ultimately for

4    declarations that the Privacy Shield decision of the

5    Commission is invalid. <span style="float:right">12:41</span>

6    **MS. JUSTICE COSTELLO:**  Before the Court of First

7    Instance or the full court, the Court of Justice?

8    **MR. MICHAEL COLLINS:**  No, before the Court of Justice

9    itself -- sorry, before the general court.

10    **MS. JUSTICE COSTELLO:**  The general court, yes. <span style="float:right">12:41</span>

11    **MR. MICHAEL COLLINS:**  The general court.  The old

12    Court of First Instance.

13    **MS. JUSTICE COSTELLO:**  Yes.  Sorry.

14    **MR. MICHAEL COLLINS:**  No, no, not at all, Judge.

15    **MS. JUSTICE COSTELLO:**  Old money/new money. <span style="float:right">12:41</span>

16    **MR. MICHAEL COLLINS:**  We may be able to get you,

17    Judge, a very short summary of those -- sorry, there's

18    a short summary I can hand you in, Judge (Same Handed).

19    I'm not going to go through them at all, it's just for

20    record to have them available as to what's involved <span style="float:right">12:41</span>

21    with them.  In one of them at least, I think they still

22    have to decide on the admissibility of the complaint.

23

24    I should say, Judge, the Working Party, Judge, is

25    referred to in Article 29 and 30.  And it says in <span style="float:right">12:41</span>

26    Article 29, Judge, that the Working Party shall be

27    composed of a representative of the supervisory

28    authority or authorities designated by each Member

29    State and of a representative of the authorities

1   established for the Community institutions and bodies

2   and of a representative of the Commission.  So they

3   seem to be the persons who make up the Working Party.

4

5   The experts have looked at this question of the Privacy <span style="float:right">12:42</span>

6   Shield, Judge, and I might refer you, ask you to look

7   again at their document, because they have reached

8   something of a position on the Privacy Shield which I

9   think is helpful.  And I think it immediately follows

10   the standing section that I was looking at previously, <span style="float:right">12:42</span>

11   so it starts on page 36 of the --

12   **MS. JUSTICE COSTELLO:**  Thank you, yes.

13   **MR. MICHAEL COLLINS:**  Of the experts' document.  If

14   you have that, Judge?

15   **MS. JUSTICE COSTELLO:**  I do. <span style="float:right">12:43</span>

16   **MR. MICHAEL COLLINS:**  The first issue is the question

17   of the Standard Contractual Clauses.  The

18   Commissioner's experts --

19

20   *"Richards states that civil remedies between a consumer*

21   *and a private company cannot provide relief for*

22   *government privacy violations."*

23

24   And that's the point about all the various remedies of

25   the alternative dispute resolutions and so on.  They <span style="float:right">12:43</span>

26   are private as between the parties, but not a remedy as

27   against the government.

28

29   Prof. Swire, on behalf of Facebook, states that:

112

*"Where private companies are compelled to share data*
*with the US government, civil remedies against private*
*companies for unlawful data sharing with the US*
*constitute a remedy for the surveillance activity."*  12:43

And that, of course, is a remedy by the government.

*"Reconciled position: The Privacy Shield Alternative*
*Dispute Resolution system and the availability of suit*  12:43
*for violation of Standard Contractual Clauses are*
*available against private companies that share data*
*with the US government, but not against the US*
*government directly.  Where a compulsory order applies*
*from a US judge, the Privacy Shield Dispute Resolution*
*system does not legally overside the judge's order."*

The second issue is the Ombudsperson's reporting
capabilities:

*"Gorski states that the Ombudsperson can neither*
*confirm nor deny that a complaint was subject to*
*surveillance, or let the individual know the specific*
*remedial action taken."*

*"Richards agrees with Gorski."*

*"Swire states that confirming or denying that a subject*
*is subject to surveillance would create a risk of*

113

```
 1        exploitation by hostile actors" - which I don't think
 2        its disagreement, it's just a comment.
 3
 4        And the agreed position is:
 5                                                              12:44
 6        "The Privacy Shield Ombudsperson may not confirm or
 7        deny that an individual was subject to surveillance or
 8        what remedies, if any, were taken in response."
 9
10        Then the Ombudsperson's authority:                    12:44
11
12        "Gorski states that the Ombudsperson cannot hind an
13        executive branch agency to implement a remedy, or
14        investigate a claim beyond whether surveillance
15        complied with relevant regulations."
16
17        "Swire states that the Ombudsperson can impact
18        surveillance activities through binding remedies on US
19        companies, and its recommendations trigger an
20        inter-agency process requiring high-level review.  The
21        Privacy Shield also does not prohibit the Ombudsperson
22        from investigating beyond compliance with relevant
23        regulations."
24
25        And the reconciled position:                          12:45
26
27        "The Privacy Shield Ombudsperson does not have direct
28        authority over US federal agencies, but recommendations
29        from the Ombudsperson trigger an inter-agency process
```

114

*requiring high-level review.  Privacy Shield is silent*
*on whether investigations may go beyond compliance with*
*relevant regulations."*

Then there's the issue of the Privacy and Civil
Liberties Oversight Board and the Inspectors General
authority - these are some of the oversight bodies in
the US.

"*Gorski states that both the PCLOB and the Inspectors*
*General lack the authority to issue binding*
*recommendations on the executive branch."*

"*Swire writes that published findings by the PCLOB*
*require the US to address them in relation to other*
*agreements, including the Privacy Shield.  Inspectors*
*General have broad investigatory authority."*

And the reconciled position is:

"*The PCLOB and agency Inspectors General cannot issue*
*binding orders to the US executive branch.  They can,*
*however, issue public findings, and Inspectors General*
*have broad investigatory authority behind their*
*reports."*

Then finally, the question of Ombudsperson
independence:

115

1   "*Gorski states that, as a part of the State Department,*
2   *the ombudsperson is not independent from the*
3   *intelligence community.*"
4
5   "*Richards states that the Ombudsperson is a political*
6   *appointee who serves at the pleasure of another*
7   *political appointee, the Secretary of State.*"
8
9   "*Swire states that, within the State Department, only*
10  *the Bureau of Intelligence and Research is part of the*
11  *Intelligence community, and does not include the*
12  *Ombudsperson.*"
13
14  I think that's what I was thinking about earlier,
15  Judge, when I was talking about not just the reporting          12:46
16  to the Secretary of State, but the connection between
17  them, that the Bureau of Intelligence and Research *is*
18  part of the Intelligence Community and that *is* within
19  the State Department.
20                                                                  12:46
21  The reconciled position is:
22
23  "*The Privacy Shield Ombudsperson is part of the US*
24  *State Department, other parts of which are part of the*
25  *Intelligence Community.*"                                      12:47
26
27  So I may have mis-expressed it earlier, but that's what
28  I was trying to express in terms of the agreed
29  position.

116

1

So I think that's helpful, Judge, because I think the
experts *have* reached a significant measure of
agreement.  And I'm sorry it's taken me so long to do
all of that.  There is one other aspect that's          12:47
relevant, I think, to the Privacy Shield arrangement
and if I could ask you to look at again book one of the
authorities - European, sorry.

**MS. JUSTICE COSTELLO:**  The European authorities, yes.
That's the one we were looking at just with the          12:47
Commission decision?

**MR. MICHAEL COLLINS:**  I'm wrong, sorry, not book one
of the European authorities.  I think it's book one of
the US authorities.  Sorry, it's book three of the US
authorities, I beg your pardon.  You will see, Judge,    12:48
if you look at the index to book three - sorry, you may
not have it yet, Judge.

**MS. JUSTICE COSTELLO:**  I do, just a moment.  Yes?

**MR. MICHAEL COLLINS:**  You will have noted from the
submissions so far and what was said in the Privacy      12:48
Shield Commission decision the importance that is
attached to Executive Orders and the Presidential
Policy Directives, because they represent -- they're
obviously changeable, but they represent the policy of
the US administration at any particular point in time    12:48
in terms of what they're committing to.  And so you see
the executive branch documents are there at tab 43
onwards.  Tab 43 we already looked at yesterday, that's
PBD28.  And there are various particular procedures

117

| 1 | associated with that which are at 44.  45 is the |
| 2 | Executive Order 12333 that we've spoken about under |
| 3 | which intelligence activities outside the United States |
| 4 | are operated under the presidential authority.  46 is |
| 5 | the Federal register about the notice of designations |
| 6 | under the Judicial Redress Act that we spoke about |
| 7 | yesterday, and we'll update that, Judge, in terms of |
| 8 | the designations made on 1st October about the covered |
| 9 | countries that I spoke about yesterday. |

12:49

12:49

But the one I want to draw attention to is, of course,
the well known and topical one at 47, Executive Order
of 25th January 2017.  This is President Trump's order
that is on the immigration policies of the US enhancing
public safety in the interior of the United States,
which as you know, Judge, is the currently the subject
of numerous challenges in the United States.  I didn't
count them.  There is, the Court of Appeals hearing the
matter in California has a website in which it lists
all of the outstanding actions, I think there are 10 or
12 actions challenging this particular Executive Order.
And as you know, the temporary restraining order, which
I'm not clear is in terms of suspending the operation
of the Executive Order in its entirety --

MS. JUSTICE COSTELLO:  I know you are saying "as I
*know*", but strictly speaking, that's not facts before
me.  But I understand you're setting the background for
it and I take it I'm meant to know this sort of in the
way that -- am I taking judicial notice of it, that's

12:49

12:50

12:50

118

| 1 | what I'm asking you? |
| 2 | MR. MICHAEL COLLINS:   Yes, judicial notice of the fact |
| 3 | that the Executive Order is -- |
| 4 | MR. GALLAGHER:         A new form of judicial notice. |
| 5 | Judicial notice of something that happens in another    12:50 |
| 6 | country, I think. |
| 7 | MR. MICHAEL COLLINS:   Well, it may be without |
| 8 | precedent certainly in terms of substance of it, but |
| 9 | undoubtedly you know what I'm talking about, Judge - |
| 10 | the application and the appeal that's currently pending  12:50 |
| 11 | -- |
| 12 | MR. GALLAGHER:         I don't think the rules apply. |
| 13 | MR. MICHAEL COLLINS:   Well, if it's being dealt with |
| 14 | by *so-called* judges then I think we can probably take |
| 15 | judicial notice of it.                                  12:51 |
| 16 | MS. JUSTICE COSTELLO:  Is there going to be so-called |
| 17 | judicial notice? |
| 18 | MR. MICHAEL COLLINS:   S-called judicial notice, yes. |
| 19 | Can I bring you to tab 47, Judge, and the Executive |
| 20 | Order itself? Section 1 sets out its purpose:          12:51 |
| 21 | |
| 22 | *"Interior enforcement of our Nation's immigration laws* |
| 23 | *is critically important to the national security and* |
| 24 | *public safety of the United States.  Many aliens who* |
| 25 | *illegally enter the United States and those who* |
| 26 | *overstay or otherwise violate the terms of their visas* |
| 27 | *present a significant threat to national security and* |
| 28 | *public safety.  This is particularly so for aliens who* |
| 29 | *engage in criminal conduct in the United States."* |

119

1

2       Then it refers to what are, or it terms sanctuary

3       jurisdictions across the United States who willfully

4       violate Federal law in an attempt to shield aliens from

5       removal from the United States.  And they are referred       12:51

6       to as removable aliens.  And they've been --

7

8       "*Tens of thousands of removable aliens have been*

9       *released into communities across the country, solely*

10      *because their home countries refuse to accept their*

11      *repatriation.  Many of these aliens are criminals who*

12      *have served time in our Federal, State, and local*

13      *jails.*"

14

15      Then at the end of that section 1 it says:                   12:52

16

17      "*The purpose of this order is to direct executive*

18      *departments and agencies to employ all lawful means to*

19      *enforce the immigration laws of the United States.*"

20                                                                   12:52

21      Then the policy of the executive branch is then set out

22      at section 2.  To:

23

24      "*Ensure the faithful execution of the immigration laws*

25      *of the United States, including the INA, against all*

26      *removable aliens, consistent with Article II, Section 3*

27      *of the United States Constitution and section 3331 of*

28      *title 5.*"

29

120

| | |
|---|---|
| 1 | And it continues on: |
| 2 | |
| 3 | "*Ensure that aliens ordered removed from the United* |
| 4 | *States are promptly removed; and* |
| 5 | *(e)  Support victims, and the families of victims, of* |
| 6 | *crimes committed by removable aliens.*" |
| 7 | |
| 8 | In section 4 the President directs agencies to employ |
| 9 | all lawful means to ensure the faithful execution of |
| 10 | the immigration laws of the US against all removable |
| 11 | aliens.  And there's a prioritisation given in |
| 12 | section 5 for those who've been charged with or |
| 13 | committed criminal offences. |
| 14 | |
| 15 | There's a number of other sections that I don't think |
| 16 | are directly relevant.  But the one I want to draw |
| 17 | attention to for present purposes, Judge, is section |
| 18 | 14, because that deals specifically with the Privacy |
| 19 | Act.  And that says: |
| 20 | |
| 21 | "*Agencies shall, to the extent consistent with* |
| 22 | *applicable law, ensure that their privacy policies* |
| 23 | *exclude persons who are not United States citizens or* |
| 24 | *lawful permanent residents from the protections of the* |
| 25 | *Privacy Act regarding personally identifiable* |
| 26 | *information.*" |
| 27 | |
| 28 | Now, that's a statement in the Presidential Order, or |
| 29 | the Executive Order that is, in terms of its policy |

12:52

12:53

121

| | |
|---|---|
| 1 | terms, Judge, it is obviously completely contrary to |
| 2 | the policy that underpins both the Privacy Shield and |
| 3 | PPD-28 - which remains, however, still in place - in |
| 4 | the sense that the part of the Privacy Act as amended |
| 5 | by the Judicial Redress Act as we've spoken about was |
| 6 | for the purpose of extending the protections of the |
| 7 | Privacy Act to non-US persons.  And section 14 of the |
| 8 | Executive Order is setting out a policy that, to the |
| 9 | extent consistent with applicable law - and it's |
| 10 | unclear what that important phrase means - but to that |
| 11 | extent, all the agencies are now directed to adopt as |
| 12 | their policy that they are to ensure that their privacy |
| 13 | policies exclude persons who are not United States |
| 14 | citizens or lawfully permanent residents. |
| 15 | |
| 16 | And that particular provision, in the community of |
| 17 | lawyers, academics and others who are interested in |
| 18 | this field, has provoked enormous interest and |
| 19 | controversy and debate as to what exactly does it mean. |
| 20 | There are a number of schools of thought, Judge.  On |
| 21 | one view of it, it underpins the whole policy purpose |
| 22 | behind the Privacy Shield, because it is adopting a |
| 23 | policy that seems contrary to the whole purpose of |
| 24 | extending the privacy protections to non-US persons -- |
| 25 | MR. GALLAGHER:        Judge, I'm sorry to interrupt |
| 26 | Mr. Collins.  I am genuinely worried about inviting the |
| 27 | court to get involved in matters that are certainly |
| 28 | outside the court's area of concern.  This is a matter |
| 29 | that has been dealt with by the experts and I think it |

122

would be appropriate that Mr. Collins' comments be
confined to what the experts, who are giving evidence,
have said and agreed in relation to the matter.  But he
has made comments like it's completely contrary to the
policy underpinning the PPD-28 - that's not what the          12:55
experts say.  And he should be confined to that, rather
than embroil the court in what certainly has a very
significant political dimension.  And the court *must* be
confined to the evidence before it and that's the
evidence of the experts.                                     12:56
**MR. MICHAEL COLLINS:**   I don't disagree with any of
that, Judge, and I'm not intending to do anything
otherwise.  But I *am* making an important point in
relation to the legal principle that you have to adopt.
Because great reliance is placed by my Friends on the        12:56
extent to which there are protections that go beyond
purely the legal rules of the US and that there are
policies in place, there are oversight mechanisms in
place, there are non-judicial remedies, all of which
have to be taken account of when evaluating the              12:56
adequacy concept within the meanings of Articles 25 and
26.  And one of the points that the experts make is
that many of these policies are in fact based on
Executive Orders or presidential orders, which are of
course subject to change with a change of                    12:56
administration and a change of a different view.  And
I'm drawing attention to an Executive Order, which is
like any other Executive Order that is there and is --
if I made reference to PPD-28, I'm quite happy to

123

1    withdraw that, Judge, because that may have a misspoke

2    on my part.

3

4    But it *is* contrary to the policy that was adopted as

5    part of this arrangement whereby the Judicial Redress        12:57

6    Act was enacted expressly to extend the protections of

7    the Privacy Act to non-US persons.  And this is a

8    policy which, in it its own terms, refers to the

9    Privacy Act and says that agencies are, to the extent

10   consistent with applicable law, are to implement their       12:57

11   policies in a way that does *not* extend those policies

12   to -- or those protections to non-US persons.

13   **MS. JUSTICE COSTELLO:**  Now, I presume the experts will

14   be able to address to what extent that can impact on

15   the redress, the Judicial Redress Act?                       12:57

16   **MR. GALLAGHER:**        Absolutely, Judge.  But again in

17   fairness - and I'm sorry, but this is of some

18   importance - that's not how the experts put it in terms

19   of the JRA.  They don't put it in terms of the effect

20   that Mr. Collins has put before the court.  And I do         12:57

21   just caution that you have enough issues to deal with.

22   I do think it's very important that when a document

23   like this is put before the court and Mr. Collins seeks

24   to interpret it, that he shouldn't do so and he should

25   rely on what the experts discussed and agreed at the         12:58

26   very document that he's been referring to, page two,

27   and that's what he should be confined to.

28   **MR. MICHAEL COLLINS:**  Well, sorry, that's exactly what

29   I'm going to do, Judge, because I'm going to finish

124

this section by opening that document to you.  But I
*was* going to explain to you and I think I'm fully
entitled to explain to you that there are differences
of views as to what effect this has.  One view is that
it doesn't change the fact that the Privacy Act and the
Judicial Redress Act are still law.  And they *are* still
law.  The other view is that because the law, in its
implementation, depends on policies that it does in
fact have a very significant change, even though the
Judicial Redress Act is, of course, still in place.  So
they are some of the competing views in relation to
that.

I was going to finish this section of my submission,
Judge, by referring to the experts' joint document
where they deal with this.  At the very start of the
document, Judge – you may have read this already, of
course – they deal with developments of US law and
practice since the filing of the expert reports.  They
deal first with the designation of the EU Member States
under the Judicial Redress Act.  And then at section
two they deal with Executive Order on immigration, with
section 14 on Privacy Act:

"*On January 25, 2017 President Trump issued an*
*Executive Order, much of it on the topic of*
*immigration.  Section 14 of the Executive Order*
*stated.*"

And then it's quoted.  I've already read it.

*"The understanding of Mr. Swire is that one legal
effect of the Executive Order is to stop agencies from
offering Privacy Act protections to 'mixed' systems of
records, which are databases that contain both US and
non-US person information.  Since 2007, for instance,
the Department of Homeland Security has offered
administrative Privacy Act protections to such mixed
systems of records.  The protections have applied to
actions within the Department, but non-US persons did
not have a right to appeal agency decisions under the
Privacy Act to the US courts.  This policy applied to
components of the Department of Homeland Security,
which include immigration-related components such as:
(1) Immigration and Customs Enforcement; and (2) Border
and Customs Protection.*

*Mr. Swire's best estimate at this time is that the
Executive Order does not have legal effect on
protections under the Judicial Redress Act – the Order
did not, for instance, explicitly instruct the Attorney
General to change the designation of the European Union
and any of its Member States under the JRA.  Mr. Swire
is not aware of any legal effect of the Executive Order
on the Privacy Shield agreement.*

*The experts agree that this provision is a change in
policy from the Obama Administration, which had*

126

1    *expanded the number of agencies that applied*

2    *administrative Privacy Act protections to mixed systems*

3    *of records.   The experts do not speculate on what other*

4    *changes in policy may occur.*"

5

6    And I think that is a summary of the position, Judge.

7    **MS. JUSTICE COSTELLO:**  Perhaps we might break at that

8    point.

9    **MR. MICHAEL COLLINS:**   Yes.

10                                                                    13:01

11

12                        (LUNCHEON ADJOURNMENT)

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

127

**THE HEARING RESUMED AFTER THE LUNCHEON ADJOURNMENT AS**

2 **FOLLOWS**

3

4 **MS. JUSTICE COSTELLO:** Good afternoon.

5 **MR. MICHAEL COLLINS:** Good afternoon, Judge. 14:08

6 **REGISTRAR:** Data Protection Commissioner -v- Facebook

7 Ireland Ltd.

8 **MR. MICHAEL COLLINS:** May it please you, Judge. Judge,

9 what I'm proposing now to do is to move on to the

10 expert reports with the assistance, I hope, of the 14:08

11 agreed experts document as well which may help to

12 identify and narrow the issues.

13

14 What I propose to do, Judge, with your leave, is to

15 start in fact with Ms. Gorski's report. Given that she 14:08

16 is giving evidence tomorrow I think it's just important

17 to make sure that report is opened just in case I run

18 out of time.

19

20 And what I hope to do after I have opened her report is 14:09

21 to bring you through the joint experts document in

22 relation to Ms. Gorski's points so that you can see

23 where there is agreement and disagreement and that may

24 help narrow the issues for tomorrow.

25 14:09

26 Her report, Judge, and affidavit is in Trial Book 6.

27 She swears a very short affidavit I don't think I need

28 open, Judge, because her expertise is set out in the

29 body of her report and she exhibits her report. She

explains who she is, Judge, in an appendix to the book
of her report at page 24.  She is a graduate of Yale
University and Harvard Law School.  She has clerked
with a number of senior judges in the US and she is a
member of the ACLU's, that's the American Civil

Liberties Union's National Security Project.  She
describes what the ACLU is.  Her work is largely
litigating civil and criminal challenges to the
lawfulness of government surveillance under Section
702.  She is the lead attorney in a Freedom of

Information Act lawsuit seeking key legal
interpretations and regulations governing Executive
Order 12333.  She regularly participates in other media
outlets and public audiences such as providing expert
testimony for the German Bundestag's First Committee of

Inquiry on NSA surveillance.

She sets out her understanding of her obligations and
her independence on page 3 of her report.  And on page
4, Judge, at paragraph 7 she says:

"*The discussion below focuses on two of the most
significant U.S. government surveillance authorities:
Section 702 of FISA.*"

Which she exhibits in its original form, Judge, a
slightly more readable form I must say I think than in
the Code:  "*which authorizes warrantless surveillance
that takes place on U.S. soil; and Executive Order*

129

*12333 which authorizes warrantless electronic*
*surveillance that largely takes place abroad.  After*
*describing surveillance conducted under these two*
*authorities, I discuss Presidential Policy Directive*
*28, a directive issued by President Barack H. Obama in*
*2014 that has resulted in modest but insufficient*
*reforms to surveillance law.*

*8.  In describing the parameters of surveillance*
*conducted under Section 702 and Executive Order 12333,* 14:11
*I do not intend to imply that these surveillance*
*authorities or the government's interpretation of these*
*authorities comply with the US Constitution or the*
*United States' international commitments.  Indeed the*
*constitutionality of Section 702 and EO 12333 is deeply* 14:11
*contested; however, for the reasons I discuss in the*
*second part of this report, there are significant*
*barriers to challenging the lawfulness of this*
*surveillance in civil litigation.*

*9.  In sum, under Section 702 and Executive Order*
*12333, the U.S. government claims extraordinary access*
*to the private communications and data of U.S. and*
*non-U.S. persons around the world.  Although there are*
*guidelines governing the collection, retention, and use*
*of this information, the U.S. government maintains that*
*it is authorized to engage in what is known as 'bulk*
*collection' when it is operating abroad.  Even when the*
*government conducts so-called 'targeted' surveillance*

1    *under Section 702 or 12333, the standards for targeting*

2    *a non-U.S. person located overseas are extraordinarily*

3    *low.  In addition, in order to locate communications*

4    *to, from, and about its targets, the government*

5    *routinely searches the contents of countless*

6    *communications in bulk.  To understand just how*

7    *permissive the current U.S surveillance law is, it*

8    *helps to understand the constraints and safeguards that*

9    *were historically put in place by the U.S. Congress in*

10   *1978 in the FISA Act.  Today, however, with respect to*

11   *surveillance directed at non-U.S. persons located*

12   *abroad, those safeguards have been eliminated.*

13

14   *10.  In 1978, largely in response to congressional*

15   *investigations of wrongful surveillance by U.S.*

16   *intelligence agencies, Congress enacted FISA to*

17   *regulate surveillance conducted for foreign*

18   *intelligence purposes.  The statute created a secret*

19   *court, known as the Foreign Intelligence Surveillance*

20   *Court and empowered it to review government*

21   *applications for surveillance in certain foreign*

22   *intelligence investigations.*

23

24   *11.  As originally enacted, FISA generally required the*

25   *government to obtain an individualized order from the*

26   *FISC before conducting electronic surveillance on U.S.*

27   *soil.  To obtain a FISA order, the government was*

28   *required to make a detailed factual showing with*

29   *respect to both the target of the surveillance and the*

131

*specific communications facility - such as a telephone*
*line - to be monitored.  The FISC could issue an order*
*authorizing surveillance only if it found that, among*
*other things, there was 'probable cause to believe that*
*the target of the electronic surveillance [was] a*
*foreign power or an agent of a foreign power,' and*
*'each of the facilities or places at which the*
*electronic surveillance is directed is being used, or*
*is about to be used, by a foreign power or an agent of*
*a foreign power'.*

*12.  The basic framework established by FISA, which I*
*refer to below as 'traditional' FISA, remains in effect*
*today, but it has been significantly weakened by 2008*
*amendments to the statute that permit the acquisition*
*of international communications without probable cause*
*or individualized suspicion, as described below."*

Then she deals with Section 702:

*"13.  In 2008 Congress enacted Section 702 of FISA, a*
*statute that radically revised the FISA regime by*
*authorizing the government's warrantless acquisition of*
*U.S. persons' international communications from*
*companies - such as telecommunications and internet*
*service providers - inside the United States.  Like*
*FISA surveillance, surveillance conducted under Section*
*702 takes place on U.S. soil.  However, surveillance*
*under Section 702 is far more sweeping than*

132

*surveillance traditionally conducted under FISA, and it*
*is subject to only a very limited form of judicial*
*oversight.*

*14.  First, unlike traditional FISA, Section 702 allows*
*the government to warrantlessly monitor communications*
*between people inside the United States and non-US*
*persons abroad.  Specifically, it authorizes the*
*government to intercept communications when at least*
*one party to a phone call or internet communication is*
*a non-US person abroad, and a 'significant purpose' of*
*the surveillance is 'foreign intelligence' collection."*

And she refers to quotes from a statute, section
1881a(a) and refers to the 'significance purpose'
requirement.

*"Importantly surveillance conducted under Section 702*
*may be conducted for many purposes, not just*
*counterterrorism.  The statute defines 'foreign*
*intelligence information' broadly to include, among*
*other things, any information bearing on the foreign*
*affairs of the United States.*

*15.  Second, whereas surveillance under traditional*
*FISA is subject to individualized judicial*
*authorization, surveillance under Section 702 is not.*
*The FISC's role in authorizing Section 702 surveillance*
*is 'narrowly circumscribed' by the statute - citing*

133

*authority – and consists principally of reviewing the*
*general procedures the government proposes to use in*
*carrying out the surveillance of tens of thousands of*
*targets.  Before obtaining a Section 702 order, the*
*government must provide to the FISC a written*
*certification attesting that the FISC has approved, or*
*that the government has submitted to the FISC for*
*approval, both 'targeting procedures' and 'minimization*
*procedures'.  These procedures dictate, at a high level*
*of generality, who may be targeted for surveillance by*
*the executive branch and how communications are to be*
*handled once intercepted.  The role that the FISC plays*
*under Section 702 bears no resemblance to the role it*
*has traditionally played under FISA.*

*16.  Third and relatedly, unlike traditional FISA,*
*Section 702 auth01izes surveillance that is not*
*predicated on the probable cause standard.  When the*
*government submits a Section 702 application to the*
*FISC, it need not demonstrate that its surveillance*
*targets are agents of foreign powers, engaged in*
*criminal activity, or connected even remotely with*
*terrorism.  Rather, Section 702 permits the government*
*to target any non-U.S. person located outside the*
*United States to obtain foreign intelligence*
*information.  Further, Section 702 does not require the*
*government to identify to the FISC the specific*
*'facilities, places, premises, or property at which'*
*its surveillance will be directed.  Thus, the*

134

*government may direct its surveillance at major*

*junctions on the internet, through which flow the*

*communications of millions of people, rather than at*

*individual telephone lines or e-mail addresses.*

*Because Section 702 requires neither particularity nor*

*probable cause, the government can rely on a single*

*FISC order to intercept the communications of countless*

*individuals for up to a year at a time.*


*17. The statute itself contains no protections for the* 14:16

*privacy of non-US persons located abroad. To the*

*extent the statute provides safeguards, these*

*safeguards take the form of 'minimization procedures'.*

*The statute's minimization requirements are supposed to*

*protect against the collection, retention, and* 14:16

*dissemination of take the collection retention and*

*dissemination of US person communications that may be*

*intercepted 'incidentally' or 'inadvertently'.*

*Significantly, however, these provisions include an*

*exception that allows the government to retain*

*communications of both U.S. and non-U.S. persons if the*

*government concludes that they contain any information*

*broadly considered 'foreign intelligence'.*


*18. Because the legal threshold for targeting non-US* 14:17

*persons is so low, and because the minimisation*

*requirements are so permissive, Section 702 effectively*

*exposes every international communication - that is*

*every communication between an individual in the US and*

135

*a non-US abroad - to potential surveillance.*

*The Government's Implementation of Section 702*

*19.   The The government has interpreted and implemented* 14:17
*Section 702 broadly, relying on the statute to*
*intercept and retain huge volumes of communications.*
*In 2011, Section 702 surveillance resulted in the*
*retention of more than 250 million communications - a*
*number that does not reflect the far larger quantity of*
*communications whose contents the NSA searched before*
*discarding them.  In 2015, the government targeted the*
*communications of 94,368 individuals, groups, and*
*organizations under a single FISC order.  Whenever the*
*communications of these targets - who may be*
*journalists, academics, or human rights advocates -*
*are stored in, routed through, or transferred to the*
*United States, they are subject to interception and*
*retention by communications providers acting at the*
*direction of the U.S. government.*

*20.  As required by Section 702, the government has*
*proposed targeting and minimization procedures and the*
*FISC has approved them.  Although these procedures are*
*ostensibly meant to protect the privacy of U.S.*
*persons, the procedures are weak and riddled with*
*exceptions.  By design they give the government broad*
*latitude to analyse and disseminate both US and non-US*
*persons' communications.*

136

1

2      *21.  Although the government has not made public its*

3      *Section 702 targeting procedures, it has published*

4      *partially redacted versions of its Section 702*

5      *minimization procedures for the NSA, FBI, CIA, and*

6      *National Counterterrorism Center.  These procedures*

7      *provide the government with broad authority to retain,*

8      *analyze, and use the data it has collected.  It can*

9      *retain communications indefinitely if they are*

10     *encrypted or are found to contain foreign intelligence*

11     *information.  Even for data that does not fall into*

12     *either of these categories, the government may retain*

13     *the hundreds of millions of communications collected*

14     *pursuant to Section 702 in its databases for years."*

15

16     And the default retention period, she says in the

17     footnote, for PRISM is five years and two years for

18     Upstream:

19

20     *"During that time, the communications may be reviewed*     14:19

21     *and queried by analysts in both intelligence and*

22     *criminal investigations.*

23

24     *22.  Official government disclosures show the*

25     *government uses Section 702 to conduct at least two*     14:19

26     *types of surveillance:  'PRISM' and 'Upstream'*

27     *surveillance.  Given the broad parameters of Section*

28     *702, the government may rely on the statute to conduct*

29     *other surveillance programs as well.*

137

1

2          *23.  Government disclosures and media reports indicate*
3          *that PRISM surveillance involves the acquisition of*
4          *communications content and metadata directly from U.S.*
5          *companies like Facebook, Google, and Microsoft.  The*
6          *government identifies the user accounts it wishes to*
7          *monitor, and then collects from the provider all*
8          *communications to or from those accounts, including any*
9          *and all communications with U.S. persons.  As of April*
10         *2013, the NSA was monitoring at least 117,675 targeted*    14:19
11         *accounts via PRISM."*

12

13         Judge, I'm not going to refer to it, but out of
14         interest perhaps you may see that she is referring
15         there to the NSA programme PRISM slides which were part    14:19
16         I think of the Snowden disclosures and you will find
17         those at Tab 16 and 17 of the book.  I'm not going to
18         open them but they are just, I suppose, of interest
19         because they featured considerably in the background to
20         this case and you may want to look at them yourself in     14:19
21         due course but I'm not going to open them.

22

23         "*24.  The disclosures by former NSA contractor Edward*
24         *Snowden and related media reports indicate that*
25         *Facebook is one of the internet service providers*        14:20
26         *compelled to participate in PRISM.  According to one*
27         *publicly released NSA slide, Facebook began*
28         *participating in PRISM on June 3, 2009.*
29         *25.  Government disclosures and media reports indicate*

*that Upstream surveillance, which the government claims*
*is authorized by Section 702, involves the mass copying*
*and searching of Internet communications flowing into*
*and out of the United States.  With the help of*
*companies like Verizon and AT&T, the NSA conducts this*
*surveillance by tapping directly into the Internet*
*backbone inside the United States - the physical*
*infrastructure that carries the communications of*
*hundreds of millions of US persons and others around*
*the world.  There, the NSA searches the metadata and*
*content of international Internet communications for*
*key terms, called 'selectors', that are associated with*
*its tens of thousands of foreign targets.  (Selectors*
*used in connection with this particular form of*
*surveillance are identifiers such as e-mail addresses*
*or phone numbers).  Communications containing selectors*
*- as well as those that happen to be bundled with them*
*in transit - are retained on a long-term basis for*
*further analysis and dissemination.  Thus, through*
*Upstream surveillance, the NSA has generalized access*
*to the content of communications, as it*
*indiscriminately copies and searches through vast*
*quantities of personal metadata and content.*

*26.  Based on the public information concerning the*
*scope of Upstream surveillance, I believe that there is*
*a substantial likelihood that this surveillance results*
*in the NSA's accessing, copying, and searching of data*
*transmitted from Facebook Ireland to Facebook in the*

United States.  While some or all of this data may be
encrypted, that would not prevent the NSA from copying,
examining, and seeking to decrypt the intercepted
Facebook data.  As noted in paragraph 21 above, when
the agency collects encrypted communications under
Section 702, it can retain those communications
indefinitely, and public disclosures indicate that the
NSA has succeeded in circumventing encryption protocols
in various contexts."

Then she deals with Executive Order 12333:
"27.  Executive Order 12333 is the primary authority
under which the NSA gathers foreign intelligence.  It
provides broad latitude for the government to conduct
surveillance on U.S. and non-US persons alike -
without any form of judicial review or the limitations
that apply to surveillance conducted under Section 702.
Electronic surveillance under 12333 is largely
conducted outside the United States.  Collection,
retention, and dissemination of data under 12333 is
governed by directives and regulations promulgated by
federal intelligence agencies and approved by the
Attorney General, including U.S. Signals Intelligence
Directive 0018 and other agency policies.  In addition,
as discussed in greater detail below, PPD-28 and its
associated agency policies further regulate 12333
activities.

28.  12333's stated goal is to provide authority for

140

*the intelligence community to gather information*
*bearing on the 'foreign, defense, and economic*
*policies' of the United States with particular emphasis*
*on countering terrorism, espionage, and weapons of mass*
*destruction.  12333 is used to justify surveillance for*
*a broad range of purposes, discussed below, resulting*
*in the collection, retention, and use of information*
*from large numbers of US and non-US persons who have no*
*nexus to foreign security threats.*

*29.  Despite its breadth, surveillance under 12333 has*
*not been subject to meaningful oversight by either the*
*US Congress or the US courts.  Surveillance programs*
*operated under EO 12333 have never been reviewed by any*
*court.  Moreover, these programs are not governed by*
*any statute, including FISA, and, as the former*
*Chairman of the Senate Intelligence Committee has*
*conceded, they are not overseen in any meaningful way*
*by Congress.*

*30.  12333 and its accompanying regulations place few*
*restrictions on the collection of U.S. or non-US person*
*information.  The order authorizes the government to*
*conduct electronic surveillance abroad for the purpose*
*of collecting 'foreign intelligence' - a term defined*
*so broadly that it appears to permit surveillance of*
*any non-US person, including surveillance of their*
*communications with U.S. persons.*
*31.  In addition, the order in its implementing*

141

1      *regulations permit at least two forms of bulk*
2      *surveillance.  First, they permit the government to*
3      *engage in what is sometimes termed 'bulk collection' –*
4      *that is the indiscriminate collection of electronic*
5      *communications or data.  As explained further below,*
6      *existing policies state that the U.S. government will*
7      *use data collected in bulk for only certain broadly*
8      *defined purposes.  But there is no question that these*
9      *policies permit collection of electronic communications*
10     *in bulk.  Thus, these policies plainly contemplate*          14:23
11     *'access on a generalized basis to the content of*
12     *electronic communications'.*  Quoting from **Schrems**.

13

14     *"32.  Second, the order and its implementing*
15     *regulations allow what can be termed 'bulk searching',*
16     *in which the government searches the content of vast*
17     *quantities of electronic communications for 'selection*
18     *terms', as it does with Upstream surveillance under*
19     *Section 702.  In other words, the NSA subjects the data*
20     *and communications content of the global population to*
21     *real-time surveillance as the agency looks for specific*
22     *information of interest.  Under EO 12333, the selection*
23     *terms the NSA uses to search communications in bulk may*
24     *include a wide array of keywords.  Indeed, unlike the*
25     *selectors the government claims to use under Section*
26     *702's Upstream surveillance, EO 12333 procedures permit*
27     *selectors that are not associated with particular*
28     *targets (such as an e-mail address or phone number).*
29     *Thus, it appears that the government can use selectors*

*likely to result in the collection of even larger*

*amounts of information, such as the names of countries*

*or political figures.*

*33.  Indeed even targeted forms of EO 12333* <span>14:24</span>

*surveillance are extremely permissive, as the executive*

*order authorizes the government to target non-U.S.*

*persons abroad for virtually any 'foreign intelligence'*

*reason, broadly defined.*

<span>14:24</span>

*34.  EO 12333 permits the retention and dissemination*

*of both U.S. and non-U.S. person information.  Under*

*the relevant policies the U.S. government has*

*promulgated, it can generally retain data for up to*

*five years.  In addition, it can retain data*

*permanently in numerous circumstances, including data*

*that is (1) encrypted or in unintelligible form; (2)*

*related to a foreign-intelligence requirement; (3)*

*indicative of a threat to the safety of a person or*

*organization; or (4) related to a crime that has been,*

*is being, or is about to be committed.  The government*

*may also retain data if it determines in writing that*

*retention is in the broad 'national security interest'*

*of the United States.  Information in categories (2),*

*(3), and (4), including identifiers of a specific U.S.*

*or non-U.S. person, may be disseminated for use*

*throughout the government.*

***The Government's Implementation of Executive Order***

*12333.*

*35.   Recent disclosures indicate that the U.S.*
*government operates a host of large-scale programs*
*under EO 12333, many of which appear to involve the*
*collection of vast quantities of U.S. and non-U.S.*
*person information.  These programs have included, for*
*example, the NSA's collection of billions of cell phone*
*location records each day, its recording of every*
*single cell phone call into, out of, and within at*
*least two countries; and its surreptitious interception*
*of data from Google and Yahoo user accounts as that*
*information travels between those companies' data*
*centers located abroad.*

*36.   According to media repolts, under EO 12333, the*
*NSA also taps directly into fiber-optic cables at*
*'congestion points' overseas - junctions through which*
*flow vast quantities of communications.  Indeed, as*
*observed by the European Commission in its Privacy*
*Shield Adequacy Decision, the U.S. government may*
*access E.U. citizens' personal data 'outside the United*
*States, including during their transit on the*
*transatlantic cables from the Union to the United*
*States'.*

*37.   In addition to the U.S. government's Section 702*
*collection of Facebook users' communications and data,*
*media reports indicate that the NSA collects Facebook*

144

1    *users' communications and data under EO 12333 as well.*

2    *For example, under this authority, the NSA has*

3    *collected hundreds of millions of contact lists and*

4    *address books from personal e-mail and*

5    *instant-messaging accounts - including contact lists*

6    *from Facebook accounts.  Numerous other Snowden*

7    *disclosures describe the collection or analysis of*

8    *information from Facebook users."*

9

10   Then she deals with PPD-28:                                    14:26

11

12   *"38.  In January 2014 President Barack Obama issued*

13   *PPD-28, an executive-branch directive that articulates*

14   *broad principles to govern surveillance for*

15   *intelligence purposes, and that imposes certain*

16   *constraints on (i) the use of electronic communications*

17   *collected in 'bulk' under EO 12333; (ii) the retention*

18   *of communications containing personal information of*

19   *non-US persons; and (iii) the dissemination of*

20   *communications containing personal information of*

21   *non-U.S. persons.*

22

23   *39.  While PPD-28 recognises the privacy interests of*

24   *non-US persons, the directive includes few meaningful*

25   *reforms - and these reforms can easily be modified or*      14:27

26   *revoked by the next US President.*

27

28   *40.  The broad principles articulated in PPD-28 include*

29   *the following:*

145

*  The U.S. shall not collect signals intelligence for
the purpose of suppressing or burdening criticism or
dissent, or for disadvantaging persons based on their
ethnicity, race, gender, sexual orientation, or
religion.
- The collection of foreign private commercial
information or trade secrets is authorized only to
protect the national security of the U.S. or its
partners and allies.
- Signals intelligence activities shall be as tailored
as feasible.  In determining whether to collect signals
intelligence, the U.S. shall consider the availability
of other information, including from diplomatic and
public sources.
-  All persons should be treated with dignity and
respect, regardless of their nationality or wherever
they might reside, and all persons have legitimate
privacy interests in the handling of their personal
information.  U.S. signals intelligence activities
must, therefore, include appropriate safeguards for the
personal information of all individuals, regardless of
the nationality of the individual to whom the
information pertains or where that individual resides.

41.  Despite these policy commitments, as discussed
below, PPD-28 includes few meaningful constraints on
the government's surveillance practices.

## Bulk Collection

146

1
2       *42.   PPD-28 provides that when the U.S. collects*
3       *nonpublicly available signals intelligence in bulk, it*
4       *shall use that data only for the purposes of detecting*
5       *and countering six types of activities:*
6       *- espionage and other threats and activities directed*
7       *by foreign powers or their intelligence services*
8       *against the U.S. and its interests;*
9       *- threats to the U.S. and its interests from terrorism;*
10      *- threats to the U.S. and its interests from the*
11      *development, possession, proliferation, or use of*
12      *weapons of mass destruction;*
13      *- cyber security threats;*
14      *- threats to U.S. or allied arms forces or US or allied*
15      *personnel;*                                                        14:29
16      *- transnational criminal threats, including illicit*
17      *finance and sanctions evasion related to the other*
18      *purposes above.*
19
20      *43.   Taken together these categories are very broad and*   14:29
21      *open to interpretation, and they effectively ratify the*
22      *practice of bulk, indiscriminate surveillance.*
23
24      *44.   Moreover the PPD-28's limitations on 'bulk*
25      *collection' do not extend to other problematic types of*
26      *mass surveillance - including the 'bulk searching of*
27      *Internet communications described in paragraph 32*
28      *above.   PPD-28 defines bulk collection to include only:*
29      *'The authorized collection of large quantities of*

147

*signals intelligence data which, due to technical or*
*operational considerations, is acquired without the use*
*of discriminants (e.g. specific identifiers, selection*
*terms, etc.').  This definition explicitly excludes*
*data that is 'temporarily acquired to facilitate*
*targeted collection'.  In other words, these*
*restrictions on use do not apply to data that is*
*acquired in bulk and held for a short period of time,*
*such as data copied and searched in bulk using Upstream*
*surveillance under Section 702,*

## *Retention, Dissemination and Use*

*45.  PPD-28's most significant reforms are with respect*
*to the retention and dissemination of communications*
*containing 'personal information' of non-U.S. persons.*
*However, even these reforms impose few constraints on*
*the government.*

*46.  Under the directive, the government may retain the*
*personal information of non- U.S. persons only if*
*retention of comparable information concerning U.S.*
*persons would be permitted under Section 2.3 of*
*Executive Order 12333.  Similarly, the government may."*

Sorry, I should look at the footnote there, Judge.  It
says PPD-28:  *"Requires that departments and agencies*
*apply the term 'personal information' in a manner that*
*is consistent for US persons and non-US persons."*

148

And again cross references to section 2.3 of 12333.

*"Similarly, the government may disseminate the personal information of non-U.S. persons only if the dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333.*

*47. Critically, however, section 2.3 of 1233 is extremely permissive: it authorizes the retention and dissemination of information concerning U.S. persons when, for example, that information constitutes 'foreign intelligence' or the information is obtained in the course of a lawful foreign intelligence investigation.*

*48. By default, under the under the NSA's procedures implementing PPD-28, the government can generally retain data for up to five years, and it can retain data permanently if, for example, the data is encrypted or related to a foreign-intelligence requirement. The government may also retain data if it determines in writing that retention is in the 'national security interest' of the United States.*

*Obstacles to Redress*

*49. Below, I discuss ways in which the US government*

149

*routinely seeks to prevent individuals from obtaining*

*redress for Section 702 and EO 12333 surveillance*

*through civil litigation in U.S. courts. I also*

*briefly address two other purported redress mechanisms*

*recently highlighted by the U.S. government in the*

*Privacy Shield agreement.*

**GOVERNMENT DEFENSES: STANDING AND STATE SECRETS**

**DOCTRINES.**

*50. For the overwhelming majority of individuals whose*

*rights are affected by U.S. government surveillance*

*under Section 702 and 12333, the government's*

*invocation and interpretation of the 'standing' and*

*'state secrets' doctrines have thus far proven to be*

*barriers to adjudication of the lawfulness of its*

*surveillance.*

*51. First, because virtually none of the individuals*

*who are subject to either Section 702 or 12333*

*surveillance ever receive notice of that surveillance,*

*it is exceedingly difficult to establish what is known*

*as 'standing' to challenge the surveillance in the US*

*courts."*

14:32

She says in footnote 45, Judge: "*The US government's*

*position is that it generally has no obligation to*

*notify the targets of its of its foreign-intelligence*

*surveillance, or the countless others whose*

150

*communications and data have been seized, searched,*

*retained, or used in the course of this surveillance.*

*The sole exception is when the government intends to*

*use information against an 'aggrieved person' in a*

*trial or proceeding where that information was obtained*

*or derived from FISA.  In those circumstances the*

*government is statutorily required to provide notice."*

*"Without standing to sue, a plaintiff cannot litigate*

*the merits of either constitutional or statutory*   14:32

*claims.*

*52.  To establish a U.S. federal court's jurisdiction*

*over a claim in the first instance, a plaintiff's*

*complaint must include factual allegations that,*

*accepted as true, plausibly allege the three elements*

*of standing under U.S. doctrine: (1) an injury in fact,*

*(2) a sufficient causal connection between the injury*

*and the conduct complained of, and (3) a likelihood*

*that the injury will be redressed by a favorable*

*decision.  The asserted injury must be 'concrete and*

*particularized' and 'actual or imminent, not*

*conjectural or hypothetical'.  A plaintiff must*

*eventually establish these three elements of standing*

*by a preponderance of the evidence.*

*53.  Because Section 702 and 12333 surveillance is*

*conducted in secret, the U.S. government routinely*

*argues to courts that plaintiffs' claims of injury are*

151

*mere 'speculation' and insufficient to establish*

*standing.  In 2013, the U.S. Supreme Court accepted*

*such an argument, holding that Amnesty International*

*USA and nine other plaintiffs lacked standing to*

*challenge Section 702, because they could not show with*

*sufficient certainty that their communications were*

*intercepted under the law."*


*Referring to the **Clapper** case.*

*"54.  The ACLU is currently representing nine human*

*rights, legal, media, and educational organizations –*

*including Wikimedia, operator of one of the*

*most-visited websites in the world – in another civil*

*challenge to Section 702 surveillance.  In October*

*2015, a U.S. district court dismissed this suit on the*

*grounds that the plaintiffs lacked standing."*


She refers to the **Wikimedia** case that I referred to

this morning, Judge.

**MS. JUSTICE COSTELLO:**  Mm hmm.

**MR. MICHAEL COLLINS:**  *"In particular, the court held*

*that wikimedia had not plausibly alleged that any of*

*its international communications – more than one*

*trillion per year – were in fact subject to Upstream*

*surveillance.  The ACLU has appealed the case, and we*

*hope that the district court's opinion will be*

*overturned.  Nevertheless, the district court's opinion*

*illustrates the difficulties that plaintiffs face in*

152

1 *establishing standing, even at the outset of a case,*

2 *when a plaintiff's allegations must be merely*

3 *plausible.*

4

5 *55.  Second, courts hearing civil suits have agreed*

6 *with the government's invocation of the 'state secrets*

7 *privilege', preventing those courts from addressing the*

8 *lawfulness of government surveillance.  When properly*

9 *invoked, this privilege allows the government to block*

10 *the disclosure of particular information in a lawsuit*

11 *where that disclosure of that specific information*

12 *would cause harm to national security."*

13

14 Citing **US -v- Reynolds**.

15                                                                                                 14:34

16 *"In recent years, however, the government has*

17 *increasingly sought to use the state secrets privilege,*

18 *not merely to shield particular information from*

19 *disclosure, but to keep entire cases out of court based*

20 *on their subject matter."*

21

22 Referencing **Mohamed -v- Jeppesen Dataplan**:

23 *"(Dismissing challenge to U.S. government's*

24 *extraordinary rendition and torture program on state*

25 *secrets grounds) Although courts have held that FISA*

26 *preempts the application of the state secrets privilege*

27 *for FISA-related claims."*

28

29 She cites **Jewel -v- National Security Agency**:  *"The*

153

*government has nevertheless raised the privilege in*
*challenges to Section 702 surveillance."*

See <u>**Jewel -v- National Security Agency**</u>, which I think
is another case: *"Dismissing a Fourth Amendment*                14:35
*challenge".*
**MS. JUSTICE COSTELLO:** It's a different case, is it?
**MR. MICHAEL COLLINS:** Yes. It may be part of the same
litigation. There are a number of <u>**Jewel**</u> cases, Judge,
but those are two different cases there that she is        14:35
referring to.


And in the second one: *"It is dismissing a Fourth*
*Amendment challenge to Upstream surveillance under*
*Section 702 on standing and state secrets grounds.*            14:35


*56. To date, as a result of the government's*
*invocation and the courts' acceptance of the standing*
*and state secret objections described above, no civil*
*lawsuit challenging Section 702 or Executive Order*            14:35
*12333 surveillance has ever produced a U.S. court*
*decision addressing the lawfulness of that*
*surveillance.*


*GOVERNMENT DEFENSE: APPLICABILITY OF US CONSTITUTION TO*  14:36
*NON-US PERSONS ABROAD*


*57. The US government has taken the position that*
*non-U.S. persons located abroad have no right to*

*challenge surveillance under the U.S. Constitution.  In*
*particular, the U.S. government has stated in court*
*filings that '[b]ecause the Fourth Amendment generally*
*does not protect non- U.S. persons outside the United*
*States', the 'foreign targets of Section 702 collection*
*lack Fourth Amendment rights'."*

Referring to **US -v- Mohamud**:

*"The government bases this argument on **United States**
**-v- Verdugo-Urquidez**."*

You will recall that was the Mexican person whose case
I opened to you:  *"In which the Supreme Court declined
to apply the Fourth Amendment's warrant requirement to
a U.S. government search of physical property located
in Mexico and belonging to a Mexican national.
Although the ACLU maintains that the government's
analysis is incorrect, when evaluating the availability
of redress for non-U.S. persons, it is significant that
the U.S. government regularly argues that non-U.S.
persons seeking to challenge warrantless surveillance
programs are not entitled to constitutional protection
or redress.*

*OTHER 'REDRESS' MECHANISMS HIGHLIGHTED BY THE
GOVERNMENT*

*Freedom of Information Act*

155

1    *58.  The Freedom of Information Act is not a form of*
2    *redress per se.  Rather, the U.S. Congress enacted this*
3    *law to provide transparency to the public about U.S.*
4    *government activities.  However, because the FOIA*
5    *permits the government to withhold properly classified*
6    *information from disclosure, and because data gathered*
7    *pursuant to foreign intelligence authorities is*
8    *invariably classified, FOIA has not been an effective*
9    *mechanism to obtain information related to the U.S.*
10   *government's surveillance of a particular individual's*
11   *communications or data.*
12
13   *59.  I am not aware of any instance in which an*
14   *individual has succeeded in obtaining information*
15   *through FOIA that would establish the surveillance of*
16   *his or her communications under either Section 702 or*
17   *EO 12333.  In fact, the government prevailed in*
18   *blocking the disclosure of similar information in*
19   *response to an FOIA request brought by attorneys who*
20   *represented detainees held at the U.S. naval facility*
21   *at Guantanamo Bay, Cuba, and who sought information*
22   *concerning the surveillance of their communications by*
23   *the NSA."*
24
25   Citing **Wilner -v- NSA**.                              14:37
26
27   "*Privacy Shield Ombudsperson*
28
29   *60.  Earlier this year, the negotiations between the*

156

1  *European Union and the United States over the Privacy*
2  *Shield agreement led to the U.S. executive branch's*
3  *creation of the Privacy Shield Ombudsperson position.*
4  *But the Ombudsperson's legal authority and ability to*
5  *provide meaningful redress are severely limited.*
6
7  *61. When the Ombudsperson receives a proper complaint,*
8  *she will investigate and then provide the complainant*
9  *with a response 'confirming (i) that the complaint has*
10  *been properly investigated, and (ii) that U.S. law,*
11  *statutes, executive orders, presidential directives,*
12  *and agency policies, providing the limitations and*
13  *safeguards described in the ODNI letter, have been*
14  *complied with, or, in the event of non-compliance, such*
15  *non-compliance has been remedied'. However, even where*
16  *the Ombudsperson does find that data was handled*
17  *improperly, she can neither confirm nor deny that the*
18  *complainant was subject to surveillance, nor can she*
19  *inform the individual of the specific remedial action*
20  *taken.*
21
22  *62. The Ombudsperson's authority is restricted in*
23  *other ways as well. Most importantly, there is no*
24  *indication that the Ombudsperson can in fact require an*
25  *executive-branch agency to implement a particular*
26  *remedy. Nor is there any indication that she is*
27  *empowered to conduct a complete and independent legal*
28  *and factual analysis of the complaint - e.g. to assess*
29  *whether surveillance violated the Fourth Amendment, as*

1      *opposed to simply examining whether surveillance*

2      *complied with the relevant regulations.  Although the*

3      *Ombudsperson may cooperate with intelligence agencies'*

4      *Inspectors General and may refer matters to the Privacy*

5      *and Civil Liberties Oversight Board, neither the*

6      *Inspectors General nor the PCLOB can issue*

7      *recommendations that are binding on the executive*

8      *branch.  Moreover, the Ombudsperson cannot respond to*

9      *any general claims that the Privacy Shield agreement is*

10     *inconsistent with E.U. data protection laws.  Finally,*

11     *because the Ombudsperson is part of the State*

12     *Department, this position is not entirely independent*

13     *from the intelligence community.*

14

15     *63.  In short an individual who complains to the*          14:39

16     *Ombudsperson is extremely unlikely to ever learn how*

17     *his complaint was analyzed, or how any non-compliance*

18     *was in fact remedied.  He also lacks the ability to*

19     *appeal or to enforce the Ombudsperson's decision.*

20                                                              14:39

21     *CONCLUSION.*

22

23     *64.  In summary, US surveillance extremely permissive,*

24     *as the government claims broad authority to acquire the*

25     *communications and data of non- U.S. persons located*      14:39

26     *abroad.  For the vast majority of individuals subject*

27     *to Section 702 and 12333 surveillance, there has to*

28     *date been no viable avenue to obtain meaningful redress*

29     *for the rights violations resulting from this*

158

surveillance."

And there are two volumes of exhibits to that, Judge,
but I'm not going to refer to any of those.

**MS. JUSTICE COSTELLO:**  Mm hmm.                    14:40

**MR. MICHAEL COLLINS:**  But could I ask you to look at
the experts agreed document and it may be helpful if
I just try to identify the bits on Ms. Gorski's report
that have been the subject of discussion between the
experts.                                              14:40

If I start on page 5, Judge, the US government
surveillance authority.

**MS. JUSTICE COSTELLO:**  Yes.

**MR. MICHAEL COLLINS:**  And the issue is the scope of    14:40
Section 702 targeting.  The Schrems expert position is:

"*Gorski states that Section 702 permits the US
government to target any non-US person located outside
the United States to obtain foreign intelligence
information.  Gorski states that Section 702 dues not
require particularity, and thus permits the US
government to intercept the communications of countless
individuals.*"

The Facebook position:  "*Swire states there are
multiple constraints on how to target persons under
Section 702, including for a well-defined foreign
intelligence purpose and the implementation of the*

159

1    *PCLOB recommendations.  Also Swire states that there is*
2    *publicly available data showing the actual scope of*
3    *Section 702 targeting, and that the number of total*
4    *Section 702 targets is a 'vanishingly small fraction of*
5    *internet users."*                                        14:41
6
7    The reconciled position is that it's not reconciled,
8    Judge.  The experts disagree about how much constraint
9    exists in practice for targeting under Section 702.
10                                                             14:41
11   The second topic is:  *"The effectiveness of protections*
12   *contained in the minimisation procedures.  Gorski*
13   *states that Section 702 minimization procedures are not*
14   *effective because they are weak and contain a number of*
15   *exceptions.  Gorski also states that Section 702*        14:41
16   *minimization procedures are not effective because they*
17   *permit queries for intelligence and criminal*
18   *investigations.*
19
20   *Swire states that Section 702 is governed by extensive*  14:42
21   *minimization procedures, including rules regulating*
22   *access to 702 - collected data; transparency of*
23   *procedures; significant external oversight and reforms*
24   *initiated in response to PCLOB recommendations.  Swire*
25   *also states that both Section 702 and PPD-28 place a*    14:42
26   *number of significant restrictions on the information*
27   *collected under Section 702 and subject to query."*
28
29   And for minimisation the experts disagree on how strong

160

the protections are and how large the exceptions are in
practice:


"*Number of Section 702 programs in existence.  Gorski*
*states that there may be more Section 702 programs than*  14:42
*PRISM and Upstream.  Swire states there are only two*
*Section 702 programs: PRISM and upstream.*"


The reconciled position is:  "*The PCLOB report - sorry,*
*the PCLOB Section 702 report has stated there are two*  14:42
*types of Section 702 acquisition: what has been*
*referred to as 'PRISM' collection and Upstream*
*collection.*


*4.  US Government Access to Company Servers under*  14:43
*PRISM.*


*Gorski states that the Section 702 PRISM program*
*involves the US government obtaining direct access to*
*data held by US technology companies such as Google and*  14:43
*Facebook.  Swire states that initial press reports*
*alleging NSA access to US technology company data were*
*incorrect.  Instead, PRISM operates similarly to other*
*court directives to produce evidence, by the government*
*serving a directive to companies requiring them to*  14:43
*collect and produce relevant communications.*"


And the reconciled position is:  "*Under Section 702,*
*the government serves directives on US providers, and*

161

1    *providers are compelled to give communications sent to*

2    *or from identified selectors to the government.  The*

3    *precise technological means by which the government*

4    *transmits selectors to providers and providers send*

5    *data to the government, to the best of the experts'*

6    *knowledge, has not been made public."*

7

8    5:  *"Section 702 Upstream access to communications.*

9

10   *In response to Swire, Gorski states that, under*      14:43

11   *upstream surveillance, the NSA copies and searches*

12   *through a far greater body of communications than the*

13   *set of communications it ultimately acquires for*

14   *long-term use.  Gorski states that Section 702 Upstream*

15   *collection should be characterized as indiscriminate*

16   *surveillance and generalized access.*

17

18   *Swire states that, under Upstream surveillance,*

19   *'[e]mails and other transactions that make it through*

20   *the filters are stored for access by the NSA, while*

21   *information that does not make it through the filters*

22   *is never accessed by the NSA or anyone else'.*

23   *Swire states that Upstream is better viewed as targeted*

24   *collection and not as mass or indiscriminate*

25   *surveillance."*      14:44

26

27   And the experts disagree about the extent of the NSA's

28   access to communications that are not to, from or about

29   a target:

162

"6.   Relevance of Executive Order 12333.  Gorski states
that 12333 places few restrictions on US intelligence
activities and that 12,333 programs are relevant to
this proceeding.  As the European Commission observed
in its Privacy Shield Adequacy Decision, the US may
access EU citizens' personal data during its transit on
transatlantic cables from the EU to the US.

Swire states that EO 12333 applies to intelligence
collections made outside the US, and is thus not
relevant unless it is clarified that different rules
apply to data that has been transferred to the US."

The reconciled position is:  "12333 intelligence          14:45
programs are generally conducted outside of the US.
They are not conducted within the US with the exception
of the for Transit Authority and certain radio
collection discussed elsewhere in this chart.
                                                            14:45
7.   Scope of targeting permitted under 12333.
Gorski states that EO 12333 permits indiscriminate bulk
collection of electronic communications data.  Swire
states that collections done under PPD-28, which
include Executive Order 12333 programs, are subject to    14:45
significant restrictions at the targeting,
minimization, use, and retention level, such that even
bulk collection cannot be characterised as
indiscriminate."

163

The reconciled position is that: "*Information
collected in bulk under 12333 may be used only for the
six purposes set forth in PPD-28.*

14:45

*The scope of data retention under 12333 programs.*

*Gorski states EO 12333 and PPD-28 permit the US
government to retain improperly large quantities of
personal data.  Swire states that under PPD-28 the same* 14:46
*rules that apply to the retention of US person data
apply to retention of EU person data.*"

The reconciled position:  "*PPD-28 provides that
retention rules for data of non-US persons must be* 14:46
*comparable to those for data of US persons under
section 2.3 of Executive Order 12333.*

*Congressional Oversight.*

14:46

*In response to Vladeck - that's the other Facebook
witness, Judge -- Gorski states that EO 12333 is the
primary authority under which the NSA conducts foreign
intelligence, and the former chair of the Senate
Intelligence Committee has conceded that EO 12333* 14:46
*programs are not overseen in any meaningful way by
Congress.*

*Vladeck states that, with regard to statutory*

164

surveillance authorities such as FISA, Congress
'exercises significant oversight responsibilities with
respect to U.S. foreign intelligence activities'.
Swire also discusses the role of Congressional
oversight.  The experts disagree as to how to
characterise Congressional oversight of US foreign
intelligence activities.

10.  Whether Section 702's Lawfulness has been reviewed
by a Court.

Gorski states that, because of the standing and state
secrets doctrines of US law, no public US civil court
has evaluated the lawfulness of Section 702 or 12333.
Swire states that general facial challenges to Section
702 have either been dismissed at, or are presently
being litigated at, the admissibility stage.  However,
three criminal cases have resulted in court decisions
which merits determinations that Section 702 is
constitutional."

The reconciled position is:  "Specific challenges to
Section 702 by individuals or public interest groups
have not made a civil trial due to obstacles including
standing and state secret doctrines.  However, US lower
court judges have done merits review of the
constitutionality of Section 702 in criminal cases.

11.  FISC modifications to Upstream under Section 702.

165

*In entire response to Swire, Gorski observes that the*
*modifications to Upstream were not 'substantial'.*
*Swire states that the FISC's responses to compliance*
*incidents have resulted in substantial modifications to*
*the Upstream program."*

The reconciled position:  "*The experts agree that the*
*FISC impose certain modifications on Upstream*
*surveillance but disagree about the significance of*
*those modifications."*                                         14:48

"*Use of 12333 for collection within the US.  In*
*response to Swire and Vladeck, Gorski observes that the*
*government continues to rely on an authority known as*
*'Transit Authority' under EO 12333 to intercept some*     14:48
*non-U.S. to non-U.S. communications while in transit on*
*U.S. soil.  In addition, the government relies on EO*
*12333 to obtain radio communications within the United*
*States that are one-end non-U.S.*
                                                               14:48
*Swire states that for collection in the US, any other*
*authority such as Executive Order 12333 does not apply.*
*Vladeck states that 12333 simply does not apply to EU*
*citizen data held by US companies within the United*
*States."*                                                     14:48

The reconciled position:  "*The expert agree that*
*Transit Authority under 12333 is an exception to the*
*general rule that 12333 applies to collection only*

166

outside of the US.  The expert's understanding is that
the Transit Authority would apply for instance to an
e-mail that went from a foreign origin across the
telecommunications network within the US without having
a U.S. destination, and then went to a foreign
destination.  Transit authority would likely not apply
to the e-mail if its destination was a corporate server
in the U.S. that forwarded the e-mail to a destination
outside the US.  The experts agree that 12333
authorizes the government to obtain radio
communications within the U.S. that are one-end
non-U.S.

13.  Effect of Section 702 compared to prior law.  In
response to Swire, Gorski states that the enactment of
Section 702 resulted in fewer legal restrictions than
previously existed for wire communications that were
collected in the U.S. and had one-end in the U.S.
Swire states Section 702 was enacted after the FISC
court denied the NSA's application in 2007 to continue
the Stellar Wind program, versions of which had been in
place since 2001.  Swire states that Section 702
'provides more detailed legal restrictions than applied
previously to non-US to non-US communications, for
communications collected with the US, under the Stellar
Wind program."

The reconciled position:  "The legal safeguards under
Section 702 are less strict than requiring an

167

*individualised FISA or law enforcement authorisation*
*for access to electronic communications.  They are in*
*some respects stricter than were applied by the*
*government between 2001 and the termination of the*
*Stellar Wind program in 2007."*                    14:50

*"14.  Access to communications under Section 702.*

*In response to Swire, Gorski observes that targeted*
*individuals invariably communicate with individuals who*
*are not targets.  Moreover, the government interprets*
*section 702 as authorizing the acquisition of*
*communications to, from and about targets.*

*Finally, under Section 702, the government also*
*acquires certain communications, unrelated to the*
*target, that happen to be bundled with communications*
*to, from, or about a target.  These communication*
*bundles are known as multi-communication transactions."*
                                                     14:51
And you will recall I talked about the 'about
communications' this morning and tried to explain what
they are.

*"Swire states that Section 702 only authorises access*  14:51
*to the communications of targeted individuals.  Swire*
*notes that a detailed discussion of 'about collection'*
*is contained in the PCLOB Section 702 report."*
That's a report, Judge, that is exhibit the, I think

168

it's exhibit the by Ms. Gorski and I think it's
possibly elsewhere as well.  I haven't opened it to
you, but it's a huge document, I forget how many
hundreds of pages it is, but it's a very significant
document.                                                    14:51


The reconciled position:  "*(1) The experts agree that
targeted individuals often communicate with individuals
who are not targets.*
*(2) The experts agree that the government interprets
Section 702 to authorize the acquisition of
communications to, from, and about targets.*
*(3) The experts agree that the government acquires
certain multi-communications transactions.*"


And I think, Judge, if I understand that correctly,
that is where you have an e-mail chain of a sort that
involves a number of communications that are packaged
or bundled within the one piece of communication.
                                                             14:52
I'm sure that's a very wrongly technical description:
"*The Foreign Intelligence Surveillance Court court in
2011 found a then existing form of the Upstream
programme unconstitutional as applied to these MCTs.*"
**MS. JUSTICE COSTELLO:**  MCTs are the                      14:52
multi-communications transactions?
**MR. MICHAEL COLLINS:**  The multi-communications
transactions:  "*The NSA subsequently instituted
additional safeguards, and the Court approved the*

169

*program"*.  I think that reference, Judge, to a decision
of the FISC in 2011 is a reference to a decision by,
from memory, a judge called Judge Bates, I think, who
was a member of the FISC court at the time and was very
critical in the decision of the practices as they were        14:52
at the time which led to certain changes in the
practices subsequently:

*"15.  FISC role in approving Section 702 targeting*
*procedures.*                                                 14:53

*In response to Swire, Gorski clarifies that, under*
*Section 702, the FISC does not approve agency analysts'*
*individual targeting decisions.  Rather, the FISC's*
*role consists principally of reviewing the general*          14:53
*procedures that the government proposes to use in*
*carrying out its surveillance of more than 94,000*
*targets.  Swire states that, with respect to Section*
*702, '[t]he FISC annually reviews and must approve*
*targeting criteria, documenting how targeting of a*          14:53
*particular person will lead to the acquisition of*
*foreign intelligence information."*

And the reconciled position:  *"The experts agree that,*
*under Section 702, the FISC does not approve agency*         14:53
*analysts' individual targeting decisions."*

*"16.  FISC's role in supervising queries.  In response*
*to Swire, Gorski clarifies that the FISC has no role in*

170

1  *authorizing individual querying decisions under Section*
2  *702.  Swire states that under Section 702 'overly broad*
3  *queries are prohibited and supervised by the FISC'.*
4  *The experts agree that the FISC does not authorise*
5  *individual querying decisions in advance under*          14:53
6  *Section 702.*
7
8  *17.  FISC role in supervising PRISM collection.  In*
9  *response to Swire, Gorski clarifies that the FISC has*
10 *no role in approving agency analysts decisions to*          14:54
11 *employ particular selectors.  Swire states that, in*
12 *PRISM collection, 'the government sends a judicially*
13 *approved and judicially supervised directive requiring*
14 *collection of certain selectors' to electronic*
15 *communications service providers.  The experts agree*     14:54
16 *that the FISC does not approve in advance agency*
17 *analysts' decisions to employ particular selectors.*
18
19 *18.  Meaning of 'target' in US government transparency*
20 *reports.*                                                 14:54
21
22 *In response to Swire, Gorski clarifies that a number of*
23 *targets reported in government transparency reports is*
24 *not limited to targeted individuals.  The US government*
25 *also includes targeted groups and organisations in the*   14:54
26 *reported figure.  Swire states that, due to government*
27 *transparency reports, the public now has access to*
28 *information about the number of individuals targeted*
29 *under Section 702.  The experts agree that the*

171

*government's transparency reports refer collectively to*
*the number of individuals, groups and organisations*
*targeted under Section 702.*

*19.   Section 702 and the acquisition of communications* 14:55
*of ordinary citizens.*

*In response to Swire, Gorski observes that the*
*government has not provided any information about how*
*many of its targeting decisions are based on evidence* 14:55
*linking the particular target to terrorism.  Gorski*
*also disputes that this statistic demonstrates a low*
*likelihood of communications being acquired for*
*ordinary citizens.  First, given the government's*
*extremely broad targeting criteria, many of these*
*targets may be 'ordinary citizens' themselves.  Second,*
*these targets invariably communicate with individuals*
*who are not targeted by the government.  Third, the*
*government likely surveils several selectors or*
*accounts for each of these targets, and each account*
*may communicate with dozens or hundreds of other*
*individuals.*

*Swire states, in 2015, there were 94,368 'targets'*
*under the Section 702 programs, many of whom are*
*targeted due to evidence linking them to terrorism.*
*That is a tiny fraction of US, European, or global*
*Internet users.  It demonstrates the low likelihood of*
*the communications being acquired for ordinary*

172

1     *citizens.*

2

3     *The experts disagree about the significance of the*

4     *number of targets of Section 702 surveillance.*

5                                                                    14:56

6     *20.  Declassification of FISC opinions.  In response to*

7     *Swire, Gorski states that more context is necessary.*

8     *Notably, the executive branch has argued in litigation*

9     *that it is not obligated to declassify significant FISC*

10    *opinions issued prior to the enactment of the USA*

11    *Freedom Act."*

12

13    Which was in 2015:  "*Swire states that 'the*

14    *administration has made an energetic effort to review*

15    *FISC opinions in order to declassify them to the extent*  14:56

16    *consistent with national security.  The experts agree*

17    *that the declassified opinions of the FISC are*

18    *available at a website that's detailed there.*

19

20    *21.  Limitations of private sector transparency*       14:56

21    *statistics.  In response to Swire, Gorski states that*

22    *more context is necessary.  These statistics do not*

23    *include any information about the government's*

24    *real-time wire surveillance of these companies' users*

25    *under section 702, Upstream or 12333.  Swire states*       14:56

26    *that private sector statistics about national security*

27    *requests for information provide important evidence*

28    *about the actual scope of national security*

29    *investigations in the US."*

And there is no particular reconciled position, Judge,
I think they are not necessarily inconsistent:


*"22.  PPD-28 and feasibility.  In response to Swire,*
*Gorski states that 'as tailored as feasible' is an*                     14:57
*extraordinarily broad and flexible standard.  Swire*
*states that PPD-28 contains safeguards, including the*
*requirement that 'Signals intelligence activities shall*
*be as tailored as feasible'.  He notes that although*
*this language does not refer to necessity or*
*proportionality, it is an example of a safeguard that*
*addresses those concerns.  The experts disagree about*
*the significance of PPD-28's requirement that signals*
*intelligence be tailored as feasible.*
                                                                        14:57

*23.  PPD-28 and limitations on the use of information*
*collected in bulk.  In response to Vladeck, Gorski*
*states that PPD-28 does not limit the bulk collection*
*of non-US personal data.  Rather, it limits the use of*
*information collected in bulk.  Moreover, PPD-28's*
*limitations on the use of information collected in bulk*
*have no application to communications collected under*
*Section 702.  PPD-28 defines 'signals intelligence*
*collected in bulk' as data acquired 'without the use of*
*discriminants', and it excludes 'signals intelligence*
*data that is temporarily acquired to facilitate*
*targeted collection', as under Section 702 Upstream.*

*Vladeck states that 'one of the central reforms of*

174

1    *PPD-28 is to expand application of [Section 702's*
2    *targeting and minimization requirements] to collection*
3    *of non-U.S. person data, as well.  Under section 2 of*
4    *PPD-28, signals intelligence collected in bulk can only*
5    *be used for six specific purposes.*
6
7    *The experts agree that PPD-28 does not expressly limit*
8    *bulk collection and that its limits on the use of*
9    *information acquired in bulk do not apply to*
10   *communications acquired under Section 702.*                    14:58
11
12   *24.  PPD-28 and limitations on retention and*
13   *dissemination.*
14
15   *In response to Swire, Gorski states that PPD-28 does*      14:58
16   *not require US intelligence agencies to apply the same*
17   *Section 702 minimization protections to non-U.S.*
18   *persons that apply to U.S. persons.  PPD-28 instead*
19   *imposes limits on the retention and dissemination of*
20   *non-U.S. person communications with reference to*       14:58
21   *Section 2.3 of Executive Order 12333, which contains*
22   *several significant exceptions.*
23
24   *Swire states that PPD-28 requires US intelligence*
25   *agencies to apply the same minimisation procedures to*    14:59
26   *non-US persons as they apply to US persons.  Swire also*
27   *suggests that the NSA's section 4 procedures*
28   *implementing PPD-28 limit the dissemination of*
29   *information about non-U.S. persons if the information*

175

1    *is not relevant to national security.*

2

3    *The experts agree that PPD-28 limits on the retention*

4    *and dissemination of non-US person communications are*

5    *defined with respect to the limits imposed on the*        14:59

6    *retention and dissemination of U.S. person*

7    *communications under Section 2.3 of 12333."*

8

9    *"25.  Scope of application of the Fourth Amendment.*

10                                                              14:59

11   *Gorski states that the Fourth Amendment applies to*

12   *searches and seizures that take place within the US but*

13   *notes that the US government has taken the position*

14   *that no judicial warrant is required for foreign*

15   *intelligence collection within the US that is targeted*

16   *at foreign persons abroad.  Separately, with respect to*

17   *surveillance conducted outside of the US, the Supreme*

18   *Court has adopted a functional approach to the Fourth*

19   *Amendment's warrant requirement that considers several*

20   *factors.*

21

22   *Swire states:  Briefly, the Fourth Amendment applies to*

23   *searches and seizures that take place within the US*

24   *(such as on data transferred to the US), and to*

25   *searches against US persons (US citizens as well as*

26   *permanent residents) that take place outside of the US.*

27

28   *Vladeck states under the Supreme Court's 1990 ruling in*

29   *United States -v- Verdugo-Urquidez, non-citizens*

176

1    *lacking substantial voluntary connections to the United*

2    *States are not protected by the Fourth Amendment.*

3    *Although the Supreme Court has never addressed whether*

4    *the Fourth Amendment might apply to searches of those*

5    *individuals' data if the data is located within the*

6    *United States, the prevailing assumption is that the*

7    *answer is no."*

8

9    The reconciled position:  *"Swire concurs with his*

10   *previous conclusion of the Fourth Amendment applying*

11   *for searches within the US, where the non-citizen has*

12   *'substantial voluntary connections' to the US, such as*

13   *physical presence in the country.  By contrast, Swire*

14   *agrees with Vladeck that the Supreme Court has not*

15   *addressed whether the Fourth Amendment would apply to*

16   *searches of non-citizens' data where the data is*

17   *located within the US but there has been no*

18   *'substantial voluntary connection' to the US.  To the*

19   *extent Vladeck's earlier testimony stated that the*

20   *Fourth Amendment applies in such circumstances, he*

21   *amends the testimony to say that the Supreme Court has*

22   *not addressed the issue.  The experts agree that the*

23   *Supreme Court has not directly addressed this issue."*

24

25   We then turn to a separate overall topic *"Causes of*      15:01

26   *Action"* and again I'm just going to deal with the ones

27   that involve Ms. Gorski.  So if I go to page 21 at 3.

28   **MS. JUSTICE COSTELLO:**  Yes.

29   **MR. MICHAEL COLLINS:**  *"Individual remedies"*:  *"In*

1    *response to Swire, Gorski observes that individual*
2    *remedies serve as an important deterrent to rights*
3    *violations and play an essential role in advancing*
4    *justice.  Swire states: 'As discussed in Chapter 8,*
5    *I therefore believe that individual remedies for*
6    *foreign surveillance issues are often ill-advised –*
7    *they create a vector of attack for hostile actors to*
8    *learn the details of the top secret information."*
9
10   I suppose two comments that don't necessarily require a    15:02
11   reconciliation.
12
13   If I go to page 23, Judge, at 5, the Totten Bar:  *"In*
14   *response to Vladeck, Gorski states --"*
15   **MS. JUSTICE COSTELLO:**  We might just --                 15:02
16   **MR. MICHAEL COLLINS:**  Sorry, yes.  *"In response to*
17   *Vladeck, Gorski states that the government may very*
18   *well invoke the Totten bar if a litigant were to*
19   *challenge a particular surveillance program that had*
20   *not yet been publicly disclosed, even if that program*
21   *operated under a known surveillance authority.  Gorski*
22   *does not take the position that the invocation of the*
23   *Totten bar would be 'appropriate', but a court may take*
24   *the opposite view."*
25
26   *"Vladeck states that, in the context of the*
27   *surveillance authorities discussed in his affidavit,*
28   *'it would be difficult to fathom an appropriate case*
29   *for invocation of the Totten bar'."*

178

*"The experts agree that the government may invoke the Totten bar if a litigant were to challenge a particular surveillance program that had not yet been publicly disclosed, but that it could not invoke the Totten bar to challenge PRISM or Upstream.  In any event, the Reynolds privilege could also result in the dismissal of a challenge to PRISM or Upstream"*.

**MS. JUSTICE COSTELLO:**  Sorry, have we looked at or heard of the Totten bar before now?  15:03

**MR. MICHAEL COLLINS:**  No, we haven't, Judge.  And I'm afraid I've come to the limits of my knowledge on this matter and --

**MS. JUSTICE COSTELLO:**  Right, we'll move on.

**MR. MICHAEL COLLINS:**  -- I don't know what the Totten  15:03 bar is.  But I'll find out.

**MR. GALLAGHER:**  It's state in respect, I think, of the entire cause of action.  Reynolds is in respect of evidence within the cause of action, so that it's like **Murphy -v- Dublin Corporation**, Reynolds is.  15:04

**MR. MICHAEL COLLINS:**  I clearly overlooked **Murphy -v- Dublin Corporation**.  I'm grateful to Mr. Gallagher for that, thank you.


*"6. Applicability of states secrets privilege.*  15:04


*In response to Vladeck, Gorski states that she agrees as a normative matter that the state secrets privilege should not apply.  However, the government may very*

179

*well attempt to invoke the state secrets privilege in a*
*Case raising only a FISA claim."*

*"Vladeck states that the state secrets privilege should*
*not apply when an EU citizen challenges US data*
*collection under Section 702."*

*"The experts agree that, notwithstanding district court*
*precedent on the matter, the government may attempt to*
*invoke the state secrets privilege in a challenge*
*brought under FISA."*

If I go over to page 24, the "Exclusionary rule":

*"In response to Swire, Gorski states that additional*      15:04
*context is necessary.  There are several significant*
*exception to the application of the suppression*
*remedy."*

This, Judge, is, as you know, when a piece of evidence      15:04
is brought up in a prosecution or a civil case and it's
alleged that it's been acquired improperly and should
be excluded.

*"In addition, because of concerns about the*               15:05
*government's interpretation of its obligation to notify*
*defendants of its intent to use evidence against them*
*that as derived from secret surveillance, defendants*
*may not even know that a deeply contested surveillance*

*authority was used in their case.  Finally, even when*
*defendants have received notice of surveillance under*
*FISA or Section 702, no defendant or his security*
*cleared counsel has ever been granted access to the*
*underlying surveillance application, hampering*               15:05
*defendants' ability to challenge the surveillance."*

*"Swire states that in a criminal trial in the US,*
*courts enforce constitutional rights by excluding*
*evidence that the government obtains illegally."*              15:05

If I go to page 26 at 13, "The Significance of the
Suppression Remedy Provided by Section 1806:

*"Gorski notes the relevance of 1806, but emphasises*
*that 'the government has refused to disclose its*
*interpretation of what constitutes evidence derived*
*from' FISA.  To date, only eight criminal defendants*
*have received notice of Section 702 surveillance,*
*despite the US government's collection of hundreds of*
*millions of communications under that authority."*

*"Serwin states that 'The person against whom the*
*evidence is being introduced has the right to bring a*
*motion to suppress the evidence gained by electronic*
*surveillance if it is shown that the information was*
*unlawfully obtained, or that the surveillance was not*
*made in conformity with an order of authorisation or*
*approval.'  Serwin also notes that the motion to*

181

1  *suppress would typically be brought in the context of*

2  *an action brought against the person, and not as an*

3  *independent affirmative claim."*

4

5  *"Vladeck critiqued the DPC Draft Decision for*

6  *downplaying the importance of 1806, because it thereby*

7  *'neglects the very distinct possibility that a motion*

8  *to suppress may result in litigation of a substantive*

9  *legal issue of transcendent importance — including the*

10  *legality of particular collection methods and programs*

11  *under Section 702 of FISA'."*

12  **MS. JUSTICE COSTELLO:** Could you just translate for me

13  "motion to suppress"? Is that a motion to dismiss?

14  **MR. MICHAEL COLLINS:** No, to exclude the evidence as

15  inadmissible evidence because it was collected

16  unlawfully, or allegedly collected unlawfully.

17

18  *"The experts agree (1) that Section 1806 could be an*

19  *important means of obtaining accountability for*

20  *unlawful government surveillance; and (2) that the only*

21  *adversarial rulings by US courts on the legality of*

22  *surveillance under FISA Section 702 to date have come*

23  *through Section 1806. The experts also agree that the*

24  *United States has failed in the past to comply with its*

25  *notice obligations under Section 1806, although we*

26  *disagree about the likelihood that such violations of*

27  *the notice requirement are still occurring today."*

28

29  If I go to page 28, item 15, "FISA As Remedy":

15:06

182

1
2       *"In response to Swire, Gorski states that more context*
3       *is necessary.  The overwhelming majority of individuals*
4       *subject to FISA surveillance win not receive notice of*
5       *that fact.  Without notice, it is exceedingly difficult*
6       *to establish standing to challenge the unlawful acts of*
7       *individual government officers."*
8
9       *"Swire states that FISA 'provides individual remedies*
10      *for data subjects against unlawful acts of individual*
11      *government officers'."*
12
13      And again it doesn't seem to call for an agreed
14      position, as there seems no real difference.  If I go
15      to page 32, Judge, "APA As Remedy", that's the                    15:08
16      Administrative Procedure Act:
17
18      *"In response to Vladeck, Gorski states that more*
19      *context is necessary"* - this is the judicial review
20      type remedy, Judge - *"The overwhelming majority of*          15:08
21      *individuals subject to secret foreign intelligence*
22      *surveillance will not receive notice of that fact.*
23      *Without notice, it is exceedingly difficult to*
24      *establish standing pursue an Administrative Procedure*
25      *Act claim."*                                                      15:08
26
27      *"Vladeck discusses the Administrative Procedure Act as*
28      *A private civil remedy to challenge allegedly unlawful*
29      *Surveillance, emphasizing that the DPC Draft Decisions*

183

*Omission of any discussion of the APA necessarily*
*colours its assessment of the US legal regime."*

Then we turn to the last section of this document,
Judge, dealing with the standing doctrine.  And I've
read a good bit of this, Judge.  I've read the agreed
propositions this morning when I was dealing with
standing and I think I have read the bits, including
the one on page 35 in relation to Vladeck and Gorski
and I've read the disagreements.  So I'll move on to
"Privacy Shield".

**MS. JUSTICE COSTELLO:**   Mm hmm.

**MR. MICHAEL COLLINS:**   And if I move to page 37.
Paragraph, or item two:

"*Privacy Shield Ombudsperson reporting capabilities.*
*Gorski states that the Ombudsperson can neither confirm*
*nor deny that the complaint was subject to a*
*surveillance or let the individual know the specific*
*remedial action taken."*

Oh, sorry, I beg your pardon.  I opened, sure I did the
Privacy Shield this morning, I did all that.  So I
don't need to refer to any more there, Judge.  So that,
I think, I certainly hope is helpful, Judge.  There's
measures of agreement to a large extent between the
parties and there are some identified issues of
disagreement, some of which may be more relevant and
may not be relevant to the ultimate decision that you

have to take, although obviously the questions of US

law, as I say, you do have to ultimately decide as a

question of fact.

So that's all I'm going to say about Ms. Gorski's          15:10

evidence, Judge.  And if I might move on then to, I was

going to open Mr. Serwin's report next, which was the

foundation of the Data Protection Commissioner's

report.  I might just take a minute, Judge, just to

find it (Short Pause).  You should have trial book two,  15:10

Judge, which contains Mr. Serwin's initial report -

which was not given for the purpose of the litigation,

Judge, this was simply the advice which the

Commissioner had sought when she was considering

Mr. Schrems' complaint and she needed advice on US law   15:11

and she obtained a report from Mr. Serwin, who is an

attorney at Morrison & Forester in San Diego in

California and who obviously has expertise in this area

and we thought it appropriate to bring to the court's

attention the nature of that advice that she had         15:11

received originally, which underpins the decision.  He

has also subsequently furnished a very short second

report in response to some of the issues that were

raised by Prof. Swire or Prof. Vladeck.

                                                          15:11

The other report in this document, Judge, is the report

of Prof. Richards, who is the other expert that has

been retained for the purpose of these proceedings by

the Controller -- the Commissioner, I should say.

185

Sorry, I keep making that mistake.

Mr. Serwin refers in his affidavit to the fact that he's a partner of Morrison & Forester, he's currently co-chair of that firm's global privacy and data security group.  He's a lawyer since 1995 in California and admitted in the District of Columbia and New York.

He refers to his retention by the Commissioner in April 2016 to provide an expert opinion in connection with certain matters of US law set to arise in the context of a draft decision then under preparation by the Commissioner.  And he sets out the background to that.

He sets out his instructions in relation to the **Schrems** case and he was asked to prepare a memorandum of advice, which he details in paragraph five:

"*(a) setting out my expert opinion on the remedies in fact available under federal law in the United States to EU citizens in respect of alleged violations of their data privacy rights against certain entities and individuals arising from the collection or processing of EU citizens' personal data by US security and/or intelligence agencies for national security purposes; (b) advising on the manner of the application of such remedies in practice; (c) identifying such constraints or limitations (if any) to which such remedies may be subject; and,*

186

*(d) identifying any difference(s) as regards the nature*
*and extent of the remedies available to EU citizens as*
*compared to those available to citizens of the United*
*States.*

*6. I was informed that, upon receipt of my memorandum,*
*the Commissioner would consider my advices and proceed*
*to form a view as to whether, as a matter of EU law,*
*the remedies available in the US can properly be*
*considered adequate.*

*7. whilst proceedings were not then in being, my*
*instructions requested that I approach the exercise at*
*hand as if preparing a report to be directly relied on*
*in evidence in civil proceedings, taking into account*
*the duties owed by an expert witness to the Court,*
*details of which were set out in my instructions.*

*8. I delivered the requested memorandum to the*
*Commissioner on 24 May 2016...*

*9. I was subsequently requested to give evidence in the*
*within proceedings. In that context, I was instructed*
*by Philip Lee, the solicitors on record for the*
*Commissioner, to prepare a supplement to my First*
*Memorandum, taking account of the pleadings filed by*
*the parties to date and, more particularly, the expert*
*reports filed by the defendants and certain of the*
*amici curiae to the extent that such reports addressed*

187

*matters that were the subject of my First Memorandum."*

And he delivered that supplemental memorandum on 30th
November 2016.  And he makes the affidavit for the
purpose of verifying the contents of those memoranda.     15:14
And he confirms at 11 that the principles and rules of
US law are correctly set out and that in the
preparation of the memoranda, he's made clear which
facts and matters are within his own knowledge.

15:14

He sets out his understanding of his duties as an
expert at paragraph 13 and it overrides any duty --
sorry, to assist the court "*as to matters within my
field of expertise and this overrides any duty or
obligation I may owe to the party by whom I have been*     15:14
*engaged.*"

He says at 14:

"*I confirm that neither I nor any person connected with
me has any financial or economic interest in any
business or economic activity of the Plaintiff, other
than any fee agreed for the preparation of my First
Memorandum...*

*15. In the interests of full disclosure, and having
regard to the duties I owe to this Honourable Court, I
consider it appropriate that I would disclose to the
Court that other lawyers at Morrison Foerster have done*

1  *legal work on other matters for Facebook Inc., the*

2  *parent company of the First Named Defendant, and for*

3  *affiliates of Facebook Inc.  I am satisfied that*

4  *acceptance of the Commissioner's instructions did not*

5  *give rise to any conflict of interest for my firm or*

6  *for me.  For completeness, I wish to confirm that, for*

7  *my part, I have not worked on any such other matter.*

8  *Furthermore, I confirm that none of those persons*

9  *within my firm who undertake such other work for*

10 *Facebook Inc. or its affiliates contributed to the*

11 *preparation of my First Report and Supplemental*

12 *Report."*

13

14 And he refers to his qualifications in the biographical

15 summary.  If I then turn to his memorandum, Judge.          15:15

16 Sorry, Judge, I just wanted to check something.  His

17 first memorandum, Judge, is 24th May 2016.  He sets

18 out -- I don't need to read all of it, but:

19

20 *"This memorandum provides a non-exclusive overview of*

21 *private remedies available to EU citizens, under*

22 *federal law in the United States, against certain*

23 *entities and individuals for alleged violations of data*

24 *privacy arising from the gathering of personal*

25 *information in the context of* national security.  It

26 provides an overview of the most likely potential

27 claims in the above-referenced situation, as well as a

28 discussion of standing, which is an overarching issue.

29 It further provides the contours of relief, including

189

1     examples of significant open issues or splits in U.S.

2     case law as well as potential limitations on recovery.

3     Potential remedies arise under a number of different US

4     laws, resulting in the potential for a non-uniform

5     approach to relief.

6

7     *This memorandum does not opine on the effectiveness of*

8     *these remedies for purposes of Article 47 of the*

9     *Charter of Fundamental Rights of the European Union, or*

10    *on whether such causes of action would be appropriate*

11    *in any particular circumstance.  Where relevant,*

12    *however, it identifies those factors that may be*

13    *barriers to suit or otherwise limit recovery.*

14    *One point of reference for the discussion below relates*

15    *to the structure of the Courts in the United States."*

16

17    And he sets out a description there of the courts and

18    the circuits and so forth.  And I don't think I need

19    dwell on that, Judge, you're familiar with that.

20                                 15:16

21    *"II.   REMEDIES AVAILABLE TO EU CITIZENS UNDER US LAW*

22    *A. Foreign Intelligence Surveillance Act*

23    *The Foreign Intelligence Surveillance Act authorizes*

24    *warrantless electronic surveillance where a*

25    *'significant purpose' of the surveillance is the*

26    *gathering of foreign intelligence.  Remedies under FISA*

27    *are generally available to both U.S. citizens and*

28    *foreign nationals under multiple statutory sections."*

29

190

1    Then he starts with Section 2712 - you'll recall that's

2    the section in the Stored Communications Act that

3    cross-references to a number of different sections and

4    provides remedies.

5                                                                    15:17

6    "*Section 2712(a) permits a person who is aggrieved by a*

7    *willful violation of certain potions of FISA, including*

8    *the following, to bring a claim for money damages.*"

9

10   Then: "*Section*" - and I'll refer to it in the code        15:17

11   sections, Judge, just to try to avoid confusion –

12   "*Section 1806(a) which prohibits the use or disclosure*

13   *by federal officers or employees except for lawful*

14   *purposes of information acquired from an electronic*

15   *surveillance within the United States for foreign*

16   *intelligence purposes;*

17

18   *Section 1825 which prohibits the use or disclosure by*

19   *federal officers or employees except for lawful*

20   *purposes of information acquired from physical searches*  15:17

21   *within the United States...*"

22

23   And 1845, which is the same, except in respect of pen

24   registers and trap and trace devices installed and used

25   for foreign intelligence purposes.  Over the page:        15:18

26

27   "*The Court may award as damages: (1) actual damages,*

28   *but not less than $10,000, whichever amount is greater;*

29   *and (2) litigation costs, reasonably incurred.  In*

191

1　　　*addition to damages, administrative discipline is*

2　　　*available under Section 2712(e)."*

3

4　　　Now, I can't recall if I opened that section to you,

5　　　Judge, but I think it refers to the possibility of a

6　　　stay on the proceedings that might be brought if the

7　　　proceedings are likely to affect the ability to conduct

8　　　a related investigation, so you may have to stay those

9　　　particular proceedings.

10

11　　　"*The requirement for a 'willful' violation serves as a*

12　　　*limitation to anyone, including an EU citizen, in*

13　　　*bringing a suit under this provision.*

14

15　　　*Sections 106(a) and 305(a) also provide that*

16　　　*information acquired under FISA concerning any United*

17　　　*States person may be used and disclosed only in*

18　　　*accordance with certain minimisation procedures."*

19

20　　　Which he outlines in the footnote and I don't think I

21　　　need read.

22

23　　　"*Section 405(a)*" - and that's - I keep getting mixed up

24　　　myself - that's 1845 - "*also provides further*

25　　　*provisions that must be complied with for use and*

26　　　*disclosure of information acquired from pen registers*

27　　　*or trap and trace devices concerning United States*

28　　　*persons. Because the minimization procedures or further*

29　　　*provisions apply only to United States persons -*

1   *defined as U.S. citizens and lawful residents or U.S.*
2   *corporations - EU citizens who are not U.S. citizens or*
3   *residents would not be able to bring a claim under*
4   *Section 2712 for non-compliance with these minimization*
5   *procedures or further provisions."*
6
7   Then he deals with Section 1810:
8
9   *"Under Section 1810, an affected person (other than a*
10  *foreign power or an agent of a foreign power) who has*
11  *been subjected to an electronic surveillance, or about*
12  *whom information obtained by electronic surveillance of*
13  *such person has been disclosed or used, in violation of*
14  *the provisions of this law, can recover (1) actual*
15  *damages, but not less than liquidated damages of $1,000*
16  *or $100 per day for each day of the violation,*
17  *whichever is greater; (2) reasonable attorneys' fees*
18  *and other costs; and (3) punitive damages.  The Ninth*
19  *Circuit, however, has held that Section 1810 does not*
20  *operate as a waiver of sovereign immunity, which means*
21  *that the United States cannot be held liable under this*
22  *section."*
23
24  And the reference, Judge, is the **Al-Haramain Islamic**
25  **Foundation** case that you'll recall I opened to you.      15:20
26
27  *"III.  Section 1806.*
28  *In addition to claims brought for willful violations of*
29  *this provision under Section 2712, Section 1806 also*

193

*provides an exclusionary remedy for a person against*
*whom evidence gained by electronic surveillance is*
*being introduced.  The person against whom the evidence*
*is being introduced has the right to bring a motion to*
*suppress the evidence"* - that's to exclude the evidence
- *"gained by electronic surveillance if it is shown*
*that the information was unlawfully obtained, or that*
*the surveillance was not made in conformity with an*
*order of authorisation or approval."*

He then moves off the FISA and he turns to the Privacy
Act:

"*The Privacy Act allows US citizens to access their*
*records or information pertaining to those individuals*
*held by governmental agencies, and to review those*
*records and have a copy made.  Heads of agencies may*
*promulgate rules to exempt certain systems of records.*
*The Privacy Act provides that the head of any agency*
*may promulgate rules to exempt any system of records*
*within the agency if the System of records is subject*
*to the exemption found in Section 552(b)(1) of the*
*Freedom of Information Act.  This provision of FOIA*
*exempts matters that are properly classified pursuant*
*to an Executive Order to be kept secret in the interest*
*of national defense or foreign policy.  The head of any*
*agency may also promulgate rules to exempt a system of*
*records if it is maintained by the Central Intelligence*
*Agency or an agency engaged in investigatory efforts*

194

*pertaining to the enforcement of criminal laws.  These*
*are not blanket exemptions, and the agency must take*
*the affirmative action of promulgating rules before an*
*exemption applies to a system of records.  There is one*
*further exemption for information compiled in*
*reasonable anticipation of a civil action or*
*proceeding, which does not require an implementing*
*regulation.*

*As noted, there is no blanket exemption for records*
*collected by a particular agency such as the NSA.*
*Certain regulations do, however, set forth the*
*exemptions that the National Security Agency ('NSA')*
*may claim under the Privacy Act, and list specific*
*systems of records that have been exempted.  In*
*particular, these regulations confirm that disclosure*
*of records pertaining to the functions and activities*
*of the NSA is prohibited.  Furthermore, all systems of*
*records maintained by the NSA are exempt from*
*disclosure to the extent that the system contains*
*information properly classified under an Executive*
*Order and that is... 'required by executive orders to*
*be kept secret in the interests of national defence or*
*foreign policy'.*

*The Privacy Act also limits the extent to which federal*
*agencies can share and disclose information about*
*individuals.  Certain exceptions apply.  For example,*
*federal agencies may disclose information about*

1    *individuals when the disclosure is for a 'routine use',*

2    *is for law enforcement investigations, or is required*

3    *under FOIA."*

4

5    And I think you may recall, Judge, there in fact were    15:22

6    12 exceptions that I drew your attention to in the

7    legislation.

8

9    "*An individual may bring a civil lawsuit against a*

10   *governmental agency pursuant to the Privacy Act in*

11   *certain situations.  For instance, an individual may*

12   *bring suit if a governmental agency refuses to comply*

13   *with an individual request for records or fails to*

14   *comply with any other provision of the Privacy Act or*

15   *any rule promulgated thereunder in such a way as to*

16   *have an adverse effect on an individual.  A court may*

17   *enjoin the governmental agency from withholding records*

18   *and order the production to the complainant of any*

19   *agency records improperly withheld from him or her.*

20   *The US Supreme Court recently held that financial harm,*

21   *as opposed to non-economic harm, is required to state a*

22   *claim for compensatory damages under the Privacy Act."*

23

24   And that's the **Federal Aviation Administration -v-**

25   **Cooper** case, Judge, that I opened to you.    15:23

26

27   "*There is an open issue as to whether an agency can*

28   *exempt its system of records from the civil remedies*

29   *provision of the Privacy Act."*

196

Then he turns to the Judicial Redress Act:

"*The Judicial Redress Act was signed by President Obama on February 24, 2016 and goes into effect 90 days after the date of enactment.  The Act has its origins in negotiations between the United States and the EU on a Data Protection and Privacy Agreement (often referred to as the 'umbrella agreement').  Those negotiations (which commenced in 2011) seek the continuation of robust information sharing between the United States and EU for law enforcement purposes.  The Act provides EU citizens with 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.  In practical terms, it extends certain remedies afforded to US citizens and lawful residents under the Privacy Act to citizens of countries designated as 'covered" countries'.  It provides that, with respect to covered records, a citizen of a covered country may bring a civil action against a federal agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, as a US citizen or permanent legal resident may under the following provisions of the Privacy Act.*"

First, Section 552(a)G1D.  We're dealing here, you'll recall, Judge, the four subsections, the (a), (b), (c)

1 and (d), the first two dealing with correcting the

2 records or getting access to the records and (c) and

3 (d) dealing with where there were adverse consequences

4 for a person.  So he's dealing with (d) first, the one

5 where it's a breach of *any* provision of the Act which          15:24

6 has adverse consequences.


8 "*But only with respect to disclosures intentionally or*

9 *willfully made in violation of 552a(b).  Thus, a*

10 *plaintiff may bring a civil action under the Judicial*

11 *Redress Act when an agency intentionally or willfully*

12 *discloses a record in violation of any provision of the*

13 *Privacy Act that is not listed in subsections*

14 *(g)(1)(A)-(C)*" - that's because (d) is the catchall -

15 "*and the disclosure has 'an adverse effect' on the*          15:25

16 *individual.  A plaintiff in a suit brought under this*

17 *provision may recover actual damages (though 'in no*

18 *case shall a person... receive less than the sum of*

19 *$1,000'), as well as costs and attorneys' fees.*"

20                                                              15:25

21 Then he deals with (A) and (B):


23 "*Subsection (A) authorises a civil action when an*

24 *agency 'makes a determination under 552a(d)(3) not to*

25 *amend an individual's record in accordance with his*

26 *request, or fails to make such review in conformity*

27 *with that subsection.'  Subsection (B) authorises a*

28 *civil action when an agency 'refuses to comply with an*

29 *individual request under 552a(d)(1)' which enables an*

198

*individual to gain access to his own records or any*
*information pertaining to him contained in the agency's*
*system. An action under either of these subsections*
*may only be brought against a designated Federal agency*
*or component. Plaintiffs in suits brought under these*
*provisions may receive injunctive relief (i.e. an order*
*to amend or produce his records), as well as costs and*
*attorneys' fees where the plaintiff has 'substantially*
*prevailed', but not damages. Notably, the Judicial*
*Redress Act does not authorize a civil action for*
*violation of 552a(d)(1)(C), which provides for a civil*
*action under the Privacy Act where an agency 'fails to*
*maintain any record concerning any individual with such*
*accuracy, relevance, timeliness, and completeness as is*
*necessary to assure fairness in any determination*
*relation to the qualifications, character, rights, or*
*opportunities of, or benefits to the individual that*
*may be made on the basis of such record. And*
*consequently a determination is made which is adverse*
*to the individual'.*

*Because the Judicial Redress Act operates by extending*
*the range of persons who may access remedies under the*
*Privacy Act, the starting point is that existing*
*limitations that apply to such remedies as are*
*available under the Privacy Act will also apply to the*
*Judicial Redress Act. So far as the exemption of*
*systems of records relating to national security are*
*concerned, existing limitations under the Privacy Act*

199

*are an important touchpoint to consider in any*
*assessment of the manner in which the Judicial Redress*
*Act will operate in practice.  However, it cannot be*
*assumed that the way in which such limitations are*
*applied under the Privacy Act will provide an accurate*
*guide as to how they will be applied under the Judicial*
*Redress Act.  Because the Judicial Redress Act was very*
*recently enacted, questions as to the precise manner in*
*which the exemptions provided for in the Privacy Act*
*will apply under the Judicial Redress Act have not yet*
*been resolved.*

*There are potential ambiguities relating to certain of*
*the definitions deployed in the Judicial Redress Act*
*that could also be read to limit the remedies afforded*
*non-US citizens by its terms.  The definition of the*
*terms 'designated Federal agency or component',*
*'covered record' and 'covered country' require*
*consideration in this context.  The term 'designated*
*Federal agency or component' means a Federal agency or*
*component of an agency designated in accordance with*
*subsection (e) of this Act.  An agency/component may be*
*designated under subsection (e) if the Attorney General*
*determines."*

And he sets out the requirements there that we looked
at yesterday in the Act, Judge, that there are certain
agreements in place with the other country, it's in the
law enforcement interests of the United States and so

1    forth.  So at the top of the next page -- and, sorry,
2    and he draws attention to the point it can't be
3    designated without the concurrence of the head of the
4    relevant agency or the agency to which the component
5    belongs.                                                    15:28

6

7    "In principle, therefore, it would be open to an agency
8    to opt-out of the Act.  This could greatly narrow the
9    Act's intended scope depending on the agency.  Because
10   the Act was very recently enacted, it is not yet clear
11   whether particular agencies, such as the NSA, will be
12   designated in the manner and for the purposes
13   described."

14

15   And I've updated you on that, Judge.                        15:28

16

17   "A country or regional economic integration
18   organization must meet certain requirements to be
19   designated a 'covered country', including entering into
20   an agreement with the United States regarding privacy
21   protections for shared information.  A reading of this
22   definition on its face implies that the United States
23   itself would not be considered a 'covered country'."

24

25   Obviously because it couldn't enter into an agreement       15:28
26   with itself.

27

28   "The Act provides that the term 'covered record' has
29   the same meaning as the term 'record' in the Privacy

201

1　　*Act, once the record is transferred 'by a public*

2　　*authority of, or private entity within' a covered*

3　　*country, 'to a designated Federal agency or component*

4　　*for purposes of preventing, investigating, detecting or*

5　　*prosecuting criminal offenses'.  This definition is*

6　　*potentially ambiguous in two respects.  First, it is*

7　　*not clear if a record originating in a foreign covered*

8　　*country (or a private entity therein) that was provided*

9　　*to the designated agency or component indirectly (for*

10　　*example, by or through a related private entity*

11　　*established in the US) could still be considered a*

12　　*'covered record'.  Second, interpretation of the term*

13　　*'covered country' affects the designation of a record*

14　　*as a 'covered record'.  As noted above, a strict*

15　　*reading of the definition of the term 'covered country'*

16　　*would indicate that the United States itself would not*

17　　*be considered a 'covered country'.*

18

19　　*Because the Judicial Redress Act implicates sovereign*

20　　*immunity, a court may strictly construe the statutory*

21　　*language to find that a record that was transferred to*

22　　*a designated US Federal agency or component, not*

23　　*directly by an authority or private entity within a*

24　　*foreign covered country but indirectly by or through a*

25　　*related private entity established within the United*

26　　*States, would thus not qualify as a 'covered record'."*

27

28　　If I just add to that, Judge; I think he's referring

29　　there to the authorities, some of which you have seen

1  referenced, that in general, if sovereign immunity is

2  waived expressly so that you can sue, a narrow

3  construction is going to be taken as to the

4  circumstances under which you're entitled to sue the US

5  Government and, if there's an interpretation that

6  favours a barring of the suit, that interpretation

7  would be favoured.

8

9  *"Clearly, a narrow reading of the terms 'covered*

10  *country' and 'covered record' would greatly limit the*

11  *accessibility of remedies under the Judicial Redress*

12  *Act.  Until such time as such matters have been*

13  *addressed by a court of competent jurisdiction,*

14  *however, it remains unclear whether such an approach*

15  *would in fact be adopted or whether, in the*

16  *alternative, a court would interpret the statutory*

17  *language in light of the purpose of the Act and find,*

18  *for example, that a record that originated in a foreign*

19  *covered country but was provided to the designated*

20  *agency or component indirectly could still be*

21  *considered a 'covered record'.  No court has addressed*

22  *these issues to date.*

23

24  *While the approach of courts when examining other*

25  *statutes that implicate sovereign immunity may not*

26  *accurately predict how the Judicial Redress Act will be*

27  *interpreted, the decision of the US Supreme Court in*

28  *Department of Army -v- Blue Fox Inc. is nonetheless*

29  *considered to be of some significance in this context."*

203

1

2          Although I haven't opened that to you, Judge, that's

3          just another case on the sovereign immunity and the way

4          the courts approach it.

5                                                                          15:31

6          "*The Judicial Redress Act provides that the District*

7          *Court for the District of Columbia shall have exclusive*

8          *jurisdiction over any claim arising under this*

9          *section.*"

10                                                                         15:31

11         And he refers to the standing point that he discusses

12         later.  He then turns to the Electronic Communications

13         Privacy Act:

14

15         "*The Electronic Communications Privacy Act is a law*

16         *that governs when electronic communications and wire*

17         *communications can be intercepted or monitored.  It*

18         *consists of the Wiretap Act and the Stored*

19         *Communications Act (SCA).  The Wiretap Act applies only*

20         *to conduct that occurs during transmission.  This is in*

21         *contrast to conduct that violates the SCA, which*

22         *relates to the improper acquisition of the contents of*

23         *stored communications - i.e. after their transmission.*

24         *Thus, the difference between the two titles is a*

25         *temporal one.  The Wiretap Act applies only to the*

26         *interception or accessing of information while in*

27         *transmission, while the SCA applies to the unauthorized*

28         *access of stored communications.*

29

*Under the Wiretap Act, it is a crime for persons to intentionally intercept or procure electronic communications, including e-mail, unless certain exceptions apply. It is also a violation of the Wiretap Act to disclose communications if the person making the disclosure knew or had reason to know that the communication was intercepted in violation of the ECPA.*

*Under the SCA, it is illegal to 'obtain, alter, or prevent authorised access to a wire or electronic communication while it is in electronic storage in such system' if a person 'intentionally accesses without authorisation a facility through which an electronic communication service is provided' or 'intentionally exceeds an authorization to access that facility'."*

If I just ask you to look, Judge, at footnote 46 just on page nine. He says:

"*The term 'intentional' under the ECPA is narrower than the dictionary definition of 'intentional'. In certain cases employees continuing to access e-mails on a network, unless some barrier is put up or other notice is given, is not actionable under the SCA because of a lack of intent.*"

And he cites **Lasco Foods -V- Hall and Shaw Sales**, holing that because the employee was permitted access

205

to the network, misuse of trade secret information was
not actionable under the SCA.  So going back to page
ten:

"*Under Section 2712, any person who is aggrieved by any
willful violation of the Wiretap Act or the SCA may
commence an action in US District Court against the
United States to recover money damages.  The Court may
assess as damages (1) actual damages, but not less than
$10,000, whichever amount is greater; and (2)
litigation costs, reasonably incurred.  Before an
action against the United States is commenced, the
plaintiff must present the claim to the appropriate
department or agency under the Federal Tort Claims Act.
Actions against the United States ate barred unless the
plaintiff presents it in writing to the appropriate
Federal agency within two years after the claim
accrues, or the action is begun within six months of
the final denial of the claim by the agency.  In
addition to damages, administrative discipline is
available under 2712(e).  For Section 2712 claims under
the ECPA, wrongful collection (and not just use and
disclosure) is actionable.*"

Then refers there to one of the **Jewel** cases, Judge, in
footnote, **Jewel -v- National Security Agency**:

"*The plain language of Section 2712(a) does not limit
the waiver of sovereign immunity for damages claimed*

206

1    *under the SCA and the Wire Tap Act to claims for the*

2    *use and disclosure of information."*

3

4    "*There is an uncertainty in the statutory language as*

5    *to whether government entities can be held liable for*

6    *violations of the Wiretap Act because the definition of*

7    *a 'person' under the Act does not include governmental*

8    *entities.*"

9

10   And he refers to three cases in the footnote, Judge.

11

12   "*There is also a split among the courts as to whether*

13   *damages are permitted against governmental entities*

14   *that violate the Act.  While certain courts have held*

15   *that government entities are liable for violations of*

16   *the SCA*" - and he cites authority - "*others have held*

17   *that government entities are not liable under the ECPA,*

18   *though government officials can be*" - again cites

19   authority - "*Relying upon the provisions of Section*

20   *2701(a) as an interpretive guide, one court recently*

21   *concluded that government entities are liable for*

22   *wiretap violations.*"

23

24   That's **Walden -v- City of Providence**.  He then turns to

25   the Freedom of Information Act:

26

27   "*The Freedom of Information Act gives individuals the*

28   *right to access information from the federal*

29   *government.  These disclosure obligations on the*

*federal government are broad, but they are subject to*
*several exemptions. For example, classified national*
*defense information shared via a classified channel is*
*typically exempt from disclosure under FOIA. FOIA also*
*exempts records that are specifically exempted from*
*disclosure by statute, if such statute either 'requires*
*that the matters be withheld from the public in such a*
*manner as to leave no discretion on the issue' or*
*'establishes particular criteria for withholding or*
*refers to particular types of matters to be withheld.'*
*Additionally, FOIA exempts records compiled for law*
*enforcement purposes, including for purposes of an*
*active law enforcement investigation.*

*F. Computer Fraud and Abuse Act ('CFAA')*
*The Computer Fraud and Abuse Act is a law that started*
*as an anti-hacking law, but its application has*
*expanded, and it protects more than US departments and*
*financial institutions. The CFAA makes it a crime for*
*anyone to intentionally access a computer without*
*authority or exceeding authority that has been granted,*
*regardless of whether the computer is owned by the*
*government, if the conduct involved an interstate or*
*foreign communication. The CFAA also makes it a crime*
*to knowingly, and with the intent to defraud, access a*
*protected computer without authorization or beyond the*
*scope of authorization, if the person furthers a fraud*
*and an item of any value is obtained (as long as the*
*value is over $5,000 in any one year period).*

208

1

2 *Courts have held that confidential data can constitute*

3 *a thing of value under the CFAA.  Furthermore, it is*

4 *unlawful under the CFAA for a person to (1) knowingly*

5 *cause the transmission of a program, information, code,*

6 *or command, and as a result of such conduct,*

7 *intentionally cause damage to a protected computer; (2)*

8 *intentionally access a protected computer without*

9 *authorisation, and as a result of such conduct,*

10 *recklessly cause damage; or (3) intentionally access a*

11 *protected computer without authorization, and as a*

12 *result of such conduct, cause damage and loss.*

13

14 *The CFAA provides for criminal penalties as well as*

15 *private causes of action, although some courts have*

16 *held that federal government agencies and officials are*

17 *immune from suits involving this statute.  Under the*

18 *CFAA, any person who suffers 'damage or loss' due to a*

19 *violation of the statute may bring a civil action to*

20 *obtain compensatory damages and injunctive relief.*

21

22 *Injunctions, including temporary restraining orders,*

23 *are often the most immediate and effective relief.*

24 *Courts are split as to whether plaintiffs must allege*

25 *both damage and loss to state a claim under the CFAA.*

26 *However, some courts have concluded that a plaintiff*

27 *can satisfy the CFAA's definition of 'loss' by alleging*

28 *costs reasonably incurred in responding to an alleged*

29 *CFAA offense, even if the alleged offense ultimately is*

1    *found to have caused no damage as defined by the CFAA."*

2

3    Then he turns to the Right to Financial Privacy Act:

4

5    "*The Right to Financial Privacy Act protects the*

6    *confidentiality of personal financial records.  Except*

7    *as otherwise provided by federal law, 'no Government*

8    *authority may have access to or obtain copies of, or*

9    *the information contained in the financial records of*

10   *any customer from a financial institution unless the*

11   *financial records are reasonably described' and (1) the*

12   *customer has authorised such disclosure; (2) such*

13   *financial records are disclosed in response to an*

14   *administrative subpoena or summons; (3) such financial*

15   *records are disclosed in response to a search warrant;*

16   *(4) such financial records are disclosed in response to*

17   *a judicial subpoena; or (5) such financial records are*

18   *disclosed in response to· a formal written request that*

19   *meets certain requirements.*

20

21   *A financial institution cannot release any of this*

22   *financial information until the governmental authority*

23   *seeking the records certifies in writing to the*

24   *financial institution that it has complied with the*

25   *RFPA.  A customer may object to his or her financial*

26   *information being provided to the governmental*

27   *authority seeking access."*

28

29   And he refers to certain exceptions in the footnote,

1    Judge.

2

3    "*If, after the government files its response, the court*

4    *is unable to make a decision based on the parties'*

5    *initial allegations and response, 'the court may*

6    *conduct such additional proceedings as it deems*

7    *appropriate'.  A governmental authority that has*

8    *obtained financial records pursuant to the RFPA may not*

9    *transfer those records to another department or agency*

10   *unless the transferring authority certifies in writing*

11   *that there is reason to believe that the records are*

12   *relevant to a legitimate law enforcement inquiry, or*

13   *intelligence or counterintelligence activity,*

14   *investigation, or analysis related to international*

15   *terrorism.*"

16

17   Then he turns to the separate question of standing:

18

19   "*Under Article III of the US Constitution, a plaintiff*

20   *must have standing to bring suit before a federal court*

21   *as a precondition to bringing a claim.*"

22

23   And he sets out three conditions, Judge, I don't think

24   I need read them.  He then deals with the <u>Clapper</u> case

25   and he summarises the facts and the holding there, and      15:39

26   again I don't think I need to read that, we've been

27   through it in other contexts.  But on page 14, Judge,

28   after he summarises <u>Clapper</u>, he goes on to say:

29

211

1    "*Clapper* *also implicates a related but separate*
2    *requirement for bringing a lawsuit in the United*
3    *States.  Federal Rule of Civil Procedure 11 requires*
4    *the attorney presenting a pleading to the court to*
5    *certify that 'the factual contentions have evidentiary*
6    *support or, if specifically so identified, will likely*
7    *have evidentiary support after a reasonable opportunity*
8    *for further investigation or discovery...'  The Court*
9    *in* **Clapper** *held that the plaintiffs did not have*
10   *standing due to the speculative nature of their claim.*
11   *This analysis would seemingly apply to a Rule 11*
12   *analysis, as speculative claims that are unlikely to*
13   *have available evidentiary support would not satisfy*
14   *the Rule 11 requirement.  The Rule 11 and standing*
15   *requirements are barriers that both U.S.  and EU*
16   *citizens would face in bringing a lawsuit."*
17
18   He then turns to the **Spokeo -v- Robins** case that I've
19   opened to you and summarises that, Judge, and says at
20   the bottom of page 14:                              15:40
21
22   "*Although a 'bare procedural violation' does not*
23   *satisfy Article III standing, a 'risk of real harm' may*
24   *sometimes satisfy the concrete injury requirement.*
25   *Thus, a fact-specific inquiry into the harm caused by a*
26   *statutory violation is still required after this*
27   *opinion.*"
28
29   They're the two modern current Supreme Court decisions

212

on it, Judge.  But there are, of course, as we know,
lower court opinions, and he turns to deal with them:


"*Lower courts vary in their interpretation of standing
in the data privacy context.  The Ninth Circuit has
found that individuals who had their personal
information stolen, but not misused, suffered a
sufficient injury to confer standing under Article III.
The Ninth Circuit's interpretation of Article III
standing is broader than many other courts that have
found that cases arising out of alleged data breaches
fail for a lack of standing unless there is a showing
of misuse of data.*


*The Seventh Circuit has held that at least at the
motion to dismiss stage, a plaintiff could establish
standing, based upon allegations that the court felt
created an 'objectively reasonable likelihood that
injury would occur as a result of the breach'.*"


And that's reference to a case, <u>Remijas -v- Neiman
Marcus Group</u>, finding standing for class action arising
from breach of payment card data at Neiman Marcus.


"*On the other hand, the First Circuit has found that a*  15:41
*plaintiff's failure to allege that his or her
information was actually acquired by a third-party is
fatal to the plaintiff's claims.  The Ninth Circuit has
also taken a broad view with respect to whether*

213

*standing can he established through statutory rights,*
*where the statutory cause of action does not require*
*proof of actual damages.  In __Jewel -v- National___*
*__Security Agency__, the plaintiffs' allegations of*
*specific violations of ECPA and FISA, as well as the*
*First and Fourteenth Amendments, coupled with the*
*allegation that their communications were part of the*
*alleged warrantless wiretapping, were sufficient for*
*the Ninth Circuit to find standing under Article III,*
*since Article III standing can exist in certain cases*
*based upon the violation of a statutorily created*
*right. The Supreme Court's recent decision in __Spokeo__*
*may alter the lower courts' analysis on this issue.*

*Based on this ruling, a plaintiff must allege that*
*statutory violations caused a concrete and*
*particularised harm in order to satisfy the Article III*
*standing requirement.  However, a 'risk of real harm'*
*may be sufficient to establish standing in some*
*circumstances, and it is yet to be seen whether lower*
*courts will alter their analysis in light of this*
*decision."*

Then he talks about standing by reference to the
Judicial Redress Act:

*"There is also an unlitigated issue regarding standing*
*and the need to prove actual damages for claims brought*
*under the Judicial Redress Act.  Two Supreme Court*

1    *cases on the Privacy Act shed light on this issue.  In*
2    *__Doe -v- Chao__, the Court held that a party seeking to*
3    *recover the minimum statutory award of $1,000 under the*
4    *Privacy Act must still prove 'actual damages' as a*
5    *prerequisite*" - and I think I opened that case to you,    15:42
6    Judge, briefly - "*In __Federal Aviation Administration__*
7    *__-v- Cooper__*" - which I also opened - "*the Court narrowed*
8    *recovery even further by holding that, under the*
9    *Privacy Act, pecuniary damages are a prerequisite to*
10   *any attempt to recover civil damages, including*
11   *statutory damages.  Because the Judicial Redress Act*
12   *incorporates the remedial provisions that were*
13   *addressed in __Cooper__, it is likely that any plaintiff*
14   *proceeding under the Judicial Redress Act will also*
15   *have to prove pecuniary damages before he or she can*
16   *recover.*"
17
18   Then he sets out his conclusion:
19
20   "*If an EU citizen were to sue for a violation of data*
21   *privacy in the context of national security, the most*
22   *likely and effective causes of action are those*
23   *analysed in this memorandum, starting with FISA and the*
24   *Judicial Redress Act.  As noted, however, there are*
25   *open questions regarding potential limitations in*
26   *bringing suit under the Judicial Redress Act.  For*
27   *example, if a court strictly interpreted relevant*
28   *statutory terms, or if it applied, without adjustment,*
29   *existing Privacy Act exemptions designed to protect*

215

1  national security interests, then the remedies

2  available under the Judicial Redress Act could become

3  foreclosed in certain factual circumstances, contrary

4  to an intent to extend those remedies to non-US

5  citizens.

6

7  Regardless of the cause of action asserted, the first

8  hurdle that either a US or EU citizen would face in

9  bringing suit is Federal Rule of Civil Procedure 11,

10  which essentially requires a good faith basis for the

11  claims alleged in a pleading.  Federal agencies have

12  the ability to classify information.  If an agency had

13  gathered a plaintiff's personal information in the

14  context of national security, that fact would likely be

15  classified and difficult to prove to satisfy Rule 11.

16  The challenges to satisfying the Rule 11 requirements

17  thus appear to be greater for claims related to

18  national security.  However, we note that the purpose

19  of the Judicial Redress Act is to afford remedies to

20  non-US citizens that were not available to them before.

21  It remains to be seen how the Rule 11 requirements in

22  conjunction with the Judicial Redress Act will be

23  implemented in light of this purpose.

24

25  The next significant hurdle that a US or EU litigant in

26  US federal court would face is establishing Article III

27  standing, as summarised below: The plaintiff must show

28  an actual or imminent injury that is caused by the

29  challenged action.  For allegations of future harm, a

216

1 *plaintiff must show that injury is 'certainly pending'.*
2 *Speculative allegations that amount only to 'possible*
3 *future injury' do not suffice*" - citing **Clapper**.

5 "*To bring a claim under the Judicial Redress Act, a*
6 *plaintiff must prove pecuniary damages, assuming the*
7 *Supreme Court cases on the Privacy Act apply to the*
8 *JRA.  For statutory causes of action that do not*
9 *require proof of actual damages, plaintiffs still need*
10 *to allege that the statutory violation caused*
11 *plaintiffs a concrete harm*" - citing **Spokeo -v-**
12 **Robbins**.

14 "*These challenges to bringing a lawsuit for a violation*
15 *of data privacy in the context of national security are*
16 *the same for both US and EU citizens.  The remedies*
17 *available under the causes of action discussed herein*
18 *are also largely identical for US and EU citizens, with*
19 *two exceptions.  First, because the minimisation*
20 *procedures of PISA apply only to US citizens, EU*
21 *citizens may not bring a claim for non-compliance with*
22 *these minimisation procedures.  However, EU citizens*
23 *may utilise the remaining remedies available under*
24 *PISA.  Second, an EU citizen may not bring a civil*
25 *action under the Judicial Redress Act where an agency*
26 *fails to adequately maintain any record concerning an*
27 *individual 'as is necessary to assure fairness in any*
28 *determination' etc.*"

1    We've read that statutory requirement a few times.

2

3    "*These two differences in the remedies available to EU*

4    *citizens are likely not material.  This memorandum*

5    *provided an overview of the causes of actions and*

6    *remedies that may be available to EU citizens for*

7    *violations of data privacy, particularly for*

8    *information gathered in the national security context.*

9    *The causes of action most likely to be effective in a*

10    *given case will necessarily depend on the factual*

11    *circumstances.  The Judicial Redress Act continues to*

12    *evolve, and the conclusions of this memorandum*

13    *regarding the Act and the Rule 11 requirements to bring*

14    *claims under the Act may be impacted by future*

15    *developments and implementations of the statute.*"

16

17    And that was what the Commissioner had, Judge, in terms

18    of the legal advice she had on US law when she took the

19    decision.  And if you look at the decision again –

20    you'll recall I opened it to you – there are various        15:46

21    sections where she identifies the bits of US law and

22    you will see that it's based on, not all but certain

23    parts of that memorandum that she clearly considered

24    amounted to deficiencies in terms of the US citizens'

25    rights.                                                      15:46

26

27    It seems to me the next logical thing for me to do,

28    Judge, is to open the reports on behalf of Facebook,

29    Prof. Swire and Prof. Vladeck.

| 1 | **MS. JUSTICE COSTELLO:**  You don't want to open the |
|---|---|
| 2 | supplemental one yet? |
| 3 | **MR. MICHAEL COLLINS:**  No.  The reason is, Judge, it's |
| 4 | responding to what is said by Prof. Swire and Vladeck, |
| 5 | so I think the logic is I would do, I'll probably do    15:47 |
| 6 | Prof. Swire next, then Prof. Vladeck and then do the |
| 7 | reply from Prof. Serwin and, finally, Prof. Richards' |
| 8 | report.  So I might as well start on Prof. Swire, |
| 9 | Judge. |
| 10 | **MS. JUSTICE COSTELLO:**  Yes.    15:47 |
| 11 | **MR. MICHAEL COLLINS:**  If you think that's appropriate |
| 12 | to do that at this point? I'm happy to do that. |
| 13 | **MS. JUSTICE COSTELLO:**  Which booklet is he in? |
| 14 | **MR. GALLAGHER:**    Book three, Judge. |
| 15 | **MS. JUSTICE COSTELLO:**  Book three.  Thank you,    15:47 |
| 16 | Mr. Gallagher. |
| 17 | **MR. MICHAEL COLLINS:**  And it's at tab four, Judge. |
| 18 | Although there's a very short affidavit, Judge, the |
| 19 | actual report is at tab five.  And if you just look at |
| 20 | tab five, Judge, you will see the length of it.  It's    15:48 |
| 21 | page numbered by reference to individual chapters – I |
| 22 | haven't actually counted how many pages there are.  And |
| 23 | you'll recall that I raised an objection... |
| 24 | **MS. JUSTICE COSTELLO:**  Yes. |
| 25 | **MR. MICHAEL COLLINS:**   ... to this report on the basis    15:48 |
| 26 | that it simply was too long, too unmanageable, didn't |
| 27 | meet various criteria in terms of what an expert report |
| 28 | should meet.  However, we need to be practical about |
| 29 | this as well; I understand the need and why Facebook |

219

want to put a full and comprehensive picture of what

they perceive as the relevant background, including

non-judicial remedies, Congressional oversight, other

forms of oversight, all of which are dealt with by

Prof. Swire.                                    15:48

So the way I propose to deal with it, Judge - I've

discussed this with Mr. Gallagher - is there is a

summary section at the start of Prof. Swire's report

which runs to about 40 pages, I'm going to open that to   15:48

you, which hopefully will give you the essential

summary of what he says in his report and then there's

one particular section of his report, chapter seven,

that deals with this question of the individual

remedies in US privacy law and I might, without        15:49

necessarily opening all of it, but at least bring you

through that chapter seven in particular.  And insofar

as Mr. Gallagher feels there are other parts of the

report that he wishes to emphasise, I'm going to leave

it to him to draw your attention to those rather than    15:49

opening the full report, Judge.  Because if I had to

read the full report, we'd be here for days, or weeks.

**MR. GALLAGHER:**          I don't have any objection to

that.  The whole report *is* relevant, but this is a

sensible way of dealing with it for the moment.        15:49

**MS. JUSTICE COSTELLO:**  Thank you.

**MR. MICHAEL COLLINS:**  His grounding affidavit, Judge,

sets out in brief his qualifications.  He elaborates on

that in the report, so I don't need to read that.  He

220

says he's been asked to - at paragraph five - to give
evidence in the proceedings by Gibson Dunn & Crutcher,
that's a US firm *"which I understand is working with*
*Mason Hayes and Curran, the solicitors on record for*
*Facebook."*  He understands his duties as an expert and    15:50
he confirms that he hasn't or any person connected with
him have any financial or economic interest in
Facebook.

So I turn to his report.  He sets out, Judge, in           15:50
chapter two his biographical report.  So rather -- I'm
going to skip the introduction section just for the
moment and go to chapter two.  And because it's not
page numbered, Judge, you have to look at the bottom of
the pages to see -- he has numbered it by reference to     15:50
chapter numbers, so it's one-dash-whatever.

**MS. JUSTICE COSTELLO:**  Yes.

**MR. MICHAEL COLLINS:**  So if you can find chapter two?

**MS. JUSTICE COSTELLO:**  Yes, it has an index, an
internal index.                                            15:50

**MR. MICHAEL COLLINS:**  Yes, there's an internal index
as well.

**MS. JUSTICE COSTELLO:**  With dividers, I mean.  I've
got...

**MR. MICHAEL COLLINS:**  Oh, you have dividers, Judge?     15:50

**MS. JUSTICE COSTELLO:**  I have dividers between the
chapters.

**MR. MICHAEL COLLINS:**  Yes.  Sorry, I don't.

**MR. GALLAGHER:**  And everything is numbered.

1     **MS. JUSTICE COSTELLO:**  Were you discriminating against

2     Mr. Collins?

3     **MR. GALLAGHER:**          Well, Mr. Collins put the book

4     together.  He discriminated against himself, which is

5     very --                                                          15:51

6     **MS. JUSTICE COSTELLO:**  Well, very good.  I'd just like

7     to be clear about that point.

8     **MR. MICHAEL COLLINS:**    There was clearly unauthorised

9     surveillance going on, Judge.

10    **MR. GALLAGHER:**          Of course, if he had used the       15:51

11    electronic, we wouldn't have this.

12    **MR. MICHAEL COLLINS:**    I look forward to seeing

13    Mr. Gallagher grappling with the electronic.

14    **MS. JUSTICE COSTELLO:**  Just so long as you're not

15    looking forward to seeing *me* trying to grapple with it.  15:51

16    **MR. MICHAEL COLLINS:**    Judge, on page 2-1 he says at

17    paragraph two:

18

19    *"My overall expertise in privacy has developed through*

20    *more than 20 years of focusing primarily on privacy and*

21    *cyber security issues, as both a professor and senior*

22    *government official.  I have written six books and*

23    *numerous academic articles, and have testified before a*

24    *dozen committees of the US Congress.  I am lead author*

25    *of the standard textbook used for the US private sector*

26    *privacy examination of the International Association of*

27    *Privacy Professionals (IAPP).  In 2015, the IAPP, among*

28    *its over 20,000 members, awarded me its Privacy*

29    *Leadership Award.*

1

2      *For government service, under President Bill Clinton I*
3      *was Chief Counselor for Privacy in the US Office of*
4      *Management and Budget, the first person to have US*
5      *government-wide responsibility for privacy issues.*
6      *Under President Barack Obama, I was Special Assistant*
7      *to the President for Economic Policy in 2009-10.  In*
8      *2013, after the initial Snowden revelations, President*
9      *Obama named me as one of five members of the Review*
10     *Group on Intelligence and Communications Technology*
11     *(which I refer to as the 'Review Group').*

12

13     *Section I of this Chapter describes my years of*
14     *experience with EU data protection law.  In 1998, I was*
15     *lead author of the book 'None of Your Business: World*
16     *Data Flows, Electronic Commerce, and the EU Privacy*
17     *Directive.'  Under President Clinton, I participated in*
18     *the negotiation of the EU/US Safe Harbor.  Since that*
19     *time, I have continued to work on EU data protection*
20     *issues.  In December 2015, when the Belgian Privacy*
21     *Agency held a forum on the effects of the initial*
22     ***Schrems** *decision, I was the sole American from the*
23     *private sector asked to participate.*

24

25     *Section II of this Chapter describes my years of*
26     *experience in US surveillance law.  Under President*
27     *Clinton, I chaired White House working groups on both*
28     *encryption and wiretap law.  In 2004, I wrote the*
29     *most-cited law review article on foreign intelligence*

1    *law.  As a member of the Review Group, I was co-author*
2    *of our 300-page report, which was re-published as a*
3    *book by the Princeton University Press.  The Review*
4    *Group was told in 2014 by the Obama Administration that*
5    *70 percent of our 46 recommendations have been adopted*
6    *in letter or spirit, and additional recommendations*
7    *have since been adopted.*
8
9    *To the best of my knowledge, I am the only person to*
10   *have authored both a book on EU data protection law as*
11   *well as one on US surveillance law.  This Chapter*
12   *highlights my experiences in both areas, including how*
13   *these experiences have informed and shaped my views on*
14   *these issues over more than two decades."*
15
16   Then, Judge, just to draw your attention to it, he sets
17   out his expertise in EU data protection law, which I
18   don't think I need read in detail, you can cast your
19   eye over to it, it's obviously very extensive
20   experience.                                              15:53
21
22   On page five he sets out his expertise in US
23   surveillance law and provides a chronological account
24   of his experience of US surveillance law, which goes
25   over a number of pages, and that concludes on page 2-8.  15:53
26   And he puts an annex to it consisting of the reforms
27   that were recommended in his 2004 article.
28
29   So if I go back then to chapter one, Judge, which is

| 1 | the introductory chapter.  And that, as I say, runs to |
|---|---|
| 2 | 40 pages.  So I'll deal with that.  After referring to |
| 3 | his biographical summary, he says at three: |
| 4 | |
| 5 | "*Part 2 summarises the system of safeguards in US law* |
| 6 | *and practice that protect all persons, both in and out* |
| 7 | *of the US.  These numerous safeguards are described in* |
| 8 | *detail in Chapters 3 and 4, and include multiple* |
| 9 | *oversight bodies and transparency requirements, as well* |
| 10 | *as judicial review of foreign intelligence* |
| 11 | *investigations.  Intelligence agencies necessarily* |
| 12 | *often need to act in secret, to detect intelligence* |
| 13 | *efforts from other countries and for compelling* |
| 14 | *national security reasons.  The US has developed* |
| 15 | *multiple ways to ensure oversight by persons with* |
| 16 | *access to classified information for the necessarily* |
| 17 | *secret activities, and to create transparency in ways* |
| 18 | *that do not compromise national security.* |
| 19 | |
| 20 | *The systemic safeguards discussed in Part 2 include:* |
| 21 | |
| 22 | *1. Historical background for the system of US foreign* |
| 23 | *intelligence law, as well as the fundamental safeguards* |
| 24 | *built into the US system of constitutional democracy* |
| 25 | *under the rule of law;* |
| 26 | *2. The systemic statutory safeguards governing foreign* |
| 27 | *intelligence surveillance;* |
| 28 | *3. The oversight mechanisms;* |
| 29 | *4. The transparency mechanisms; and* |

225

*5. Administrative safeguards that are significant in practice and supplement the legislative safeguards.*

*In my view, the US system overall provides effective safeguards 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 clearer rules on collection, use, sharing and oversight of data relating to foreign nationals than the laws of almost all EU Member States. In addition, as shown in the analysis of the Foreign Intelligence Surveillance Court in Chapter 5, those rigorous legal standards are effectively implemented in practice, under the supervision of independent judges with access to top-secret information. In addition, these systemic safeguards in the foreign intelligence realm are complemented by safeguards in the criminal procedure realm that in significant respects are stricter than EU Member States.*

*Part 3 describes how individuals (including residents of EU Member States) have access to multiple remedies in the US for violations of privacy. It outlines the paths an aggrieved person in the US or resident of an EU Member State may take in response to concerns regarding US privacy violations:*

*1. I discuss individual judicial remedies against the US government, including the recently-finalised Privacy Shield and Umbrella Agreement, as well as the recently passed Judicial Redress Act.*

*2. I examine the civil and criminal remedies available in the event that 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.*

*3. I highlight three paths of non-judicial remedies any individual in the US or EU can take: The Privacy and Civil Liberties Oversight Board, Congressional committees, and recourse to the US free press and privacy-protective nongovernmental organisations.*

*4. I analyse individual remedies against US companies that improperly disclose information to the US government about customers or other persons.  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.*

*5. I also examine remedies available under state law in the US, including enforcement by state Attorneys General, as well as private rights of action, which are generally far easier to bring in the US than in the EU.*"

Then at seven he sets out an overall summary:

1

2      "*In summary on Parts 2 and 3, the combination of*

3      *systemic safeguards and individual remedies in the US,*

4      *in my view, are effective and 'adequate' in*

5      *safeguarding the personal data of non-US persons.*

6      *Moreover, the Court of Justice of the European Union*

7      *(CJEU) has announced a legal standard of 'essential*

8      *equivalence' for transfers of personal data to third*

9      *countries such as the US.  Based on my comprehensive*

10     *review of US law and practice, and my years of*

11     *experience in EU data protection law, my conclusion is*

12     *that overall intelligence related safeguards for*

13     *personal data held in the US are greater than in EU*

14     *Member States.  Even more clearly, the US safeguards*

15     *are at least 'essentially equivalent' to EU safeguards.*

16     *I therefore do not see a basis in law or fact for a*

17     *conclusion that the US lacks adequate protections, due*

18     *to its intelligence activities, for personal data*

19     *transferred to the US from the EU.*

20

21     *Part 4 discusses the potentially very broad impact were*

22     *the EU to find a lack of 'adequacy' or 'essential*

23     *equivalence'.  The following are key conclusions, which*

24     *I reach based on the analysis in this and accompanying*

25     *chapters:*

26

27     *1. US law defines the term 'electronic communications*

28     *service provider' broadly to include any company*

29     *providing an e-mail or similar communication system.*

228

*A finding of inadequacy would apply to the full set of such providers. The effect of this proceeding on companies doing business in both the US and EU is thus potentially very broad.*

*2. The surveillance safeguards in most or all other countries outside the EU are less extensive than those in the US. The effect of an inadequacy finding would thus logically appear to apply to transfers to all non-EU countries, except any whose safeguards against surveillance are greater than those in the US.*

*3. An inadequacy finding for Standard Contract Clauses may have implications for other lawful bases for data transfers. I make no statement about whether a finding of inadequacy for SCCs would entail a finding of inadequacy for Privacy Shield or Binding Corporate Rules. The discussion here does support the possibility of a 'categorical finding of inadequacy' – a finding of inadequacy that would apply not only to SCCs but also to Privacy Shield and BCRs. A categorical finding of inadequacy would 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."*

I think he's envisaging there, if I understand it, Judge, a categorical finding of inadequacy being one

1     addressed not just to the SCCs, but addressed to all

2     methods of transfer of data from the EU to the US,

3     including the Privacy Shield, the binding corporate

4     rules --

5     **MS. JUSTICE COSTELLO:** Is that within the scope of your   15:59

6     proceedings?

7     **MR. MICHAEL COLLINS:** Well, no, Judge. We're

8     challenging the transfer and the validity of the -- or

9     we're looking for an adjudication, I should say, on the

10     validity of the Standard Contractual Clauses. So I do   15:59

11     draw that distinction.

12

13     "*This Testimony supports the conclusion that an*

14     *inadequacy finding would have large effects on EU*

15     *economic well-being. EU institutions and Member States*

16     *have clearly indicated the economic importance of*

17     *maintaining data flows with the US. In addition, the*

18     *General Agreement of Trade in Services bans*

19     *'discrimination between countries where like conditions*

20     *prevail'. There appears to be a strong case that such*

21     *discrimination would exist if transfers to the US were*

22     *barred, despite less extensive surveillance safeguards*

23     *in most non-EU nations and EU Member States themselves.*

24

25     *5. A finding of inadequacy would also create large*

26     *risks for EU national security and public safety. NATO*

27     *and other treaty obligations emphasize information*

28     *sharing for national security purposes. The EU has*

29     *stated that EU/US information sharing is 'critical to*

```
 1        prevent, investigate, detect and prosecute criminal

 2        offenses, including terrorism'."

 3

 4        Could I just add, Judge - I hope it's clear from what

 5        I've said, but just while I had it a moment ago - I      16:00

 6        drew attention earlier to the interaction between the

 7        Privacy Shield and the SCCs, so that it could be used

 8        for the purpose of challenging it.  And obviously the

 9        European Court presumably has to have account of the

10        entire situation before it, which is one of the reasons  16:01

11        why we have referred to the Privacy Shield.  So there

12        is that element of interaction between the two.

13

14        "In summary, the combination of systemic safeguards and

15        individual remedies in the US, in my view, are

16        effective and 'adequate' in safeguarding the personal

17        data of non-US persons.  These actions are necessary

18        and taken in accordance with law.  In light of those

19        safeguards and individual remedies available to EU

20        citizens in connection with data transferred to the US,

21        I respectfully believe and assert that continued

22        transfers of personal data under Standard Contract

23        Clauses are necessary in a democratic society to

24        protect vital interests of the EU, including national

25        security, public safety, and economic well-being."

26

27        Then he gives a biographical summary which, as I say,

28        I've already dealt with, Judge.

29        MS. JUSTICE COSTELLO:  I think we might leave it at
```

231

| 1 | that point. |
| 2 | **MR. MICHAEL COLLINS:**   I'll leave it at that point, |
| 3 | Judge. |
| 4 | **MS. JUSTICE COSTELLO:**  So it's Ms. Gorski then tomorrow |
| 5 | at 10:30? |
| 6 | **MR. MICHAEL COLLINS:**   Tomorrow at 10:30.  Thank you |
| 7 | very much, Judge. |
| 8 | **MR. GALLAGHER:**        Judge, that Robertson affidavit; |
| 9 | despite his difficulties, he's very kindly approved the |
| 10 | affidavit and I'm going to hand it in in draft form - |
| 11 | it's been circulated to my Friends - so that you have |
| 12 | it.  And it'll be duly sworn when he's in a position to |
| 13 | do so (Same Handed). |
| 14 | **MR. MICHAEL COLLINS:**   Actually, I haven't had an |
| 15 | opportunity to look at it, Judge, but I'm assuming |
| 16 | there is no difficulty. |
| 17 | **MR. GALLAGHER:**        It's just the qualifications. |
| 18 | **MR. MICHAEL COLLINS:**   Yes, I'll just formally reserve |
| 19 | my position, but I don't *anticipate* any difficulty. |
| 20 | **MR. GALLAGHER:**        Thank you. |
| 21 | **MR. MICHAEL COLLINS:**   Thank you, Judge. |
| 22 | |
| 23 | <u>**THE HEARING WAS THEN ADJOURNED UNTIL FRIDAY, 10TH**</u> |
| 24 | <u>**FEBRUARY AT 10:30**</u> |
| 25 | |
| 26 | |
| 27 | |
| 28 | |
| 29 | |

The times noted in the right margin are: 16:01 (line 5), 16:01 (line 10), 16:02 (line 15), 16:02 (line 20), 11:51 (line 25).

232

1

131:24, 165:29, 188:6, 212:3, 212:11, 212:14, 216:9, 216:15, 216:16, 216:21, 218:13

**112** [1] - 73:2
**113** [1] - 73:11
**115** [2] - 74:6, 76:11
**116** [2] - 76:7, 76:17
**117** [1] - 77:1
**117,675** [1] - 138:10
**118** [1] - 78:29
**119** [1] - 79:11
**12** [4] - 48:8, 118:21, 132:12, 196:6
**12(b)(1** [2] - 7:12, 11:13
**12(b)(6** [1] - 11:14
**12,333** [1] - 163:4
**120** [1] - 80:7
**121** [1] - 81:22
**122** [1] - 82:18
**123** [1] - 83:3
**1233** [1] - 149:10
**12333** [63] - 29:14, 65:24, 74:13, 118:2, 129:13, 130:1, 130:10, 130:15, 130:22, 131:1, 140:11, 140:12, 140:18, 140:20, 140:26, 141:5, 141:11, 141:14, 141:21, 142:22, 142:26, 143:5, 143:11, 144:1, 144:5, 144:16, 145:1, 145:17, 148:24, 149:2, 149:8, 150:2, 150:13, 150:20, 151:27, 154:21, 156:17, 158:27, 163:2, 163:3, 163:10, 163:15, 163:21, 163:22, 163:25, 164:3, 164:6, 164:8, 164:17, 164:22, 164:25, 165:14, 166:12, 166:15, 166:18, 166:22, 166:23, 166:28, 166:29, 167:9, 173:25, 175:21, 176:7
**12333's** [1] - 140:29
**127** [1] - 84:3
**128** [1] - 85:5
**12th** [1] - 108:1
**13** [10] - 38:24, 39:20, 47:25, 48:2, 48:12, 48:27, 132:21,

167:14, 181:12, 188:12

**136** [2] - 49:7, 85:22
**136-140** [1] - 49:1
**137** [1] - 86:1
**139** [3] - 86:7, 86:8, 86:25
**14** [12] - 6:11, 14:27, 49:10, 121:18, 122:7, 125:23, 125:27, 133:5, 168:7, 188:18, 211:27, 212:20
**140** [3] - 49:8, 86:17, 88:1
**141** [1] - 88:18
**144** [1] - 88:25
**145** [1] - 93:29
**148** [1] - 95:2
**15** [5] - 49:20, 133:25, 170:9, 182:29, 188:26
**151** [1] - 96:14
**16** [5] - 11:8, 16:11, 134:16, 138:17, 170:28
**169** [4] - 75:10, 75:12, 75:25, 75:26
**16th** [1] - 110:24
**17** [6] - 16:20, 50:5, 98:17, 135:10, 138:17, 171:8
**170** [2] - 74:19, 75:9
**17th** [1] - 65:28
**18** [3] - 50:14, 135:25, 171:19
**1806** [8] - 181:13, 181:15, 182:6, 182:18, 182:23, 182:25, 193:27, 193:29
**1806(a** [1] - 191:12
**1810** [3] - 193:7, 193:9, 193:19
**1825** [1] - 191:18
**1845** [2] - 191:23, 192:24
**1881a(a** [1] - 133:15
**19** [3] - 5:14, 136:5, 172:5
**1978** [2] - 131:10, 131:14
**1990** [1] - 176:28
**1995** [1] - 186:6
**1998** [1] - 223:14
**1st** [2] - 107:26, 118:8
**1ST** [1] - 2:9

## 2

**2** [42] - 2:7, 2:17, 2:23, 2:27, 2:27, 5:13, 6:5, 23:3, 24:19, 24:28, 30:29, 39:3, 39:12, 39:13, 40:15, 41:4, 41:12, 43:24, 44:5, 47:17, 100:5, 101:1, 102:23, 120:22, 126:16, 143:17, 143:24, 151:18, 169:10, 175:3, 182:20, 191:29, 193:17, 206:10, 209:7, 210:12, 225:5, 225:20, 225:26, 227:6, 228:2, 229:6
**2-1** [1] - 222:16
**2-8** [1] - 224:25
**2.2** [1] - 54:1
**2.3** [8] - 55:22, 148:23, 149:2, 149:7, 149:10, 164:17, 175:21, 176:7
**20** [7] - 16:29, 50:27, 61:27, 66:9, 136:22, 173:6, 222:20
**20,000** [1] - 222:28
**2001** [2] - 167:22, 168:4
**2002** [1] - 22:12
**2004** [3] - 98:17, 223:28, 224:27
**2007** [3] - 126:7, 167:20, 168:5
**2008** [2] - 132:14, 132:21
**2009** [1] - 138:28
**2009-10** [1] - 223:7
**2011** [4] - 136:8, 169:23, 170:2, 197:10
**2013** [5] - 48:13, 65:4, 138:10, 152:2, 223:8
**2014** [6] - 43:6, 48:10, 65:28, 130:6, 145:12, 224:4
**2015** [7] - 72:4, 136:12, 152:16, 172:24, 173:13, 222:27, 223:20
**2016** [11] - 33:26, 34:10, 40:17, 107:26, 108:1, 110:23, 110:24, 186:10, 188:4, 189:17, 197:5
**2016..** [1] - 187:20

**2016/4809P** [1] - 1:5
**2017** [8] - 1:18, 5:2, 20:15, 21:26, 23:24, 67:13, 118:13, 125:25
**2018** [2] - 38:1, 94:23
**21** [6] - 18:11, 51:7, 137:2, 140:4, 173:20, 177:27
**215** [2] - 67:8, 68:8
**22** [3] - 51:12, 137:24, 174:4
**23** [4] - 51:19, 138:2, 174:16, 178:13
**231** [1] - 4:5
**24** [7] - 51:26, 129:2, 138:23, 175:12, 180:13, 187:20, 197:5
**24th** [1] - 189:17
**25** [14] - 23:24, 35:22, 39:15, 48:18, 52:3, 59:18, 88:19, 89:26, 92:9, 105:22, 123:21, 125:25, 138:29, 176:9
**25(1** [1] - 44:7
**25(2** [1] - 40:9
**25(6)..** [1] - 88:28
**250** [1] - 136:9
**25th** [4] - 20:14, 38:1, 110:22, 118:13
**26** [7] - 35:22, 53:4, 92:9, 105:23, 123:22, 139:25, 181:12
**26'** [1] - 89:26
**27** [2] - 13:15, 140:12
**2701(a** [1] - 207:20
**2712** [5] - 191:1, 193:4, 193:29, 206:5, 206:21
**2712(a** [2] - 191:6, 206:28
**27l2(e)** [2] - 192:2, 206:21
**28** [8] - 2:31, 18:20, 43:4, 53:20, 65:24, 130:5, 140:29, 182:29
**28(3** [1] - 44:13
**29** [11] - 19:3, 34:14, 34:16, 94:29, 107:16, 107:22, 109:26, 110:5, 111:25, 111:26, 141:11
**2ND** [1] - 2:14

## 3

**3** [31] - 1:18, 6:12, 20:26, 21:21, 24:19, 25:10, 31:24, 43:24,

44:11, 45:17, 47:17, 47:19, 63:12, 120:26, 129:19, 138:28, 143:18, 143:25, 151:19, 169:13, 177:27, 193:18, 209:10, 210:14, 225:8, 225:28, 226:24, 227:12, 228:2, 229:13
**30** [2] - 111:25, 141:21
**300-page** [1] - 224:2
**305(a** [1] - 192:15
**30th** [1] - 188:3
**31** [4] - 46:8, 54:4, 72:18, 141:29
**31(2** [1] - 46:13
**312** [1] - 69:23
**32** [4] - 54:10, 142:14, 147:27, 183:15
**323** [1] - 3:3
**33** [3] - 24:9, 55:4, 143:5
**3331** [1] - 120:27
**34** [2] - 55:5, 143:11
**35** [6] - 28:25, 40:2, 40:6, 55:7, 144:3, 184:9
**36** [2] - 112:11, 144:16
**37** [2] - 144:27, 184:13
**37-42** [1] - 2:22
**38** [2] - 85:21, 145:12
**39** [2] - 56:5, 145:23

## 4

**4** [19] - 2:12, 23:20, 25:21, 44:9, 44:22, 45:26, 85:20, 102:9, 121:8, 129:20, 143:20, 143:25, 161:15, 175:27, 210:16, 225:8, 225:29, 227:17, 228:21
**4(2** [1] - 45:8
**4(e** [1] - 47:1
**40** [4] - 56:13, 145:28, 220:10, 225:2
**405(a** [1] - 192:23
**41** [2] - 56:24, 146:25
**42** [5] - 20:26, 39:4, 39:25, 57:5, 147:2
**43** [9] - 39:8, 39:13, 39:18, 39:19, 39:28,

2

3

acknowledging [1] - 89:12

ACLU [9] - 7:22, 8:1, 20:15, 23:26, 24:1, 129:7, 152:11, 152:26, 155:18

ACLU's [1] - 129:5

acquire [1] - 158:24

acquired [15] - 148:2, 148:5, 148:8, 172:13, 172:29, 174:24, 174:26, 175:9, 175:10, 180:22, 191:14, 191:20, 192:16, 192:26, 213:27

acquires [4] - 94:9, 162:13, 168:16, 169:13

acquisition [9] - 132:15, 132:23, 138:3, 161:11, 168:12, 169:11, 170:21, 172:5, 204:22

acronym [2] - 10:25, 38:21

act [2] - 49:15, 225:12

Act [144] - 5:24, 14:1, 14:13, 19:26, 27:1, 28:9, 34:8, 34:10, 43:18, 52:19, 52:20, 55:18, 59:25, 66:29, 72:4, 72:29, 73:2, 73:19, 73:21, 80:14, 85:17, 85:18, 85:20, 104:17, 118:6, 121:19, 121:25, 122:4, 122:5, 122:7, 124:6, 124:7, 124:9, 124:15, 125:5, 125:6, 125:10, 125:21, 125:23, 126:5, 126:9, 126:13, 126:21, 127:2, 129:11, 131:10, 155:29, 156:1, 173:11, 183:16, 183:25, 183:27, 190:22, 190:23, 191:2, 194:12, 194:14, 194:19, 194:23, 195:14, 195:26, 196:10, 196:14, 196:22, 196:29, 197:2, 197:4, 197:6, 197:12, 197:14, 197:18, 197:26, 198:5, 198:11, 198:13, 199:10,

199:12, 199:22, 199:24, 199:26, 199:27, 199:29, 200:3, 200:5, 200:7, 200:9, 200:10, 200:14, 200:22, 200:27, 201:8, 201:10, 201:28, 202:1, 202:19, 203:12, 203:17, 203:26, 204:6, 204:13, 204:15, 204:18, 204:19, 204:25, 205:1, 205:5, 206:6, 206:14, 207:1, 207:6, 207:7, 207:14, 207:25, 207:27, 208:15, 208:16, 210:3, 210:5, 214:25, 214:29, 215:1, 215:4, 215:9, 215:11, 215:14, 215:24, 215:26, 215:29, 216:2, 216:19, 216:22, 217:5, 217:7, 217:25, 218:11, 218:13, 218:14, 227:5, 227:9, 227:10, 227:11

Act's [1] - 201:9

Act.. [1] - 73:26

acted [1] - 35:2

Acting [1] - 40:26

acting [2] - 14:24, 136:19

Action [1] - 177:26

action [62] - 1:27, 5:21, 6:8, 7:17, 11:22, 15:25, 24:23, 25:6, 25:19, 25:28, 36:19, 42:17, 55:13, 57:2, 59:24, 59:27, 60:14, 60:22, 60:24, 70:28, 71:12, 73:22, 74:17, 74:24, 77:23, 77:27, 104:26, 110:22, 110:23, 113:24, 157:19, 179:18, 179:19, 182:2, 184:20, 190:10, 195:3, 195:6, 197:21, 198:10, 198:23, 198:28, 199:3, 199:10, 199:12, 206:7, 206:12, 206:18, 209:15, 209:19, 213:22, 214:2, 215:22, 216:7, 216:29, 217:8, 217:17, 217:25,

218:9, 227:20, 227:25

action' [1] - 77:21

action.. [1] - 70:29

actionable [3] - 205:25, 206:2, 206:23

actions [10] - 25:13, 88:24, 95:23, 97:12, 110:16, 118:20, 118:21, 126:11, 218:5, 231:17

Actions [1] - 206:15

active [1] - 208:13

actively [1] - 109:27

activities [20] - 18:23, 65:18, 68:16, 76:27, 80:5, 98:24, 114:18, 118:3, 140:27, 146:10, 146:19, 147:5, 147:6, 156:4, 163:4, 165:7, 174:8, 195:17, 225:17, 228:18

activities' [1] - 165:3

activity [4] - 113:5, 134:22, 188:22, 211:13

actors [2] - 114:1, 178:7

Acts [1] - 52:19

acts [4] - 52:20, 62:27, 183:6, 183:10

actual [19] - 15:26, 16:5, 18:21, 24:21, 27:2, 39:8, 39:29, 62:11, 160:2, 173:28, 191:27, 193:14, 198:17, 206:9, 214:3, 214:28, 216:28, 217:9, 219:19

ad [1] - 47:24

add [3] - 94:22, 202:28, 231:4

addition [17] - 34:4, 35:8, 54:12, 82:12, 131:3, 140:24, 141:29, 143:15, 144:27, 166:17, 180:25, 192:1, 193:28, 206:20, 226:14, 226:18, 230:17

additional [11] - 62:24, 69:8, 73:14, 76:9, 76:17, 96:11, 99:12, 169:29, 180:15, 211:6, 224:6

Additionally [1] - 208:11

address [11] - 21:12, 46:26, 60:23, 79:8,

95:29, 96:24, 115:15, 124:14, 142:28, 145:4, 150:4

addressed [16] - 8:27, 60:22, 77:4, 77:12, 79:14, 88:29, 177:3, 177:15, 177:22, 177:23, 187:29, 203:13, 203:21, 215:13, 230:1

addresses [6] - 10:5, 11:2, 14:5, 135:4, 139:15, 174:12

addressing [2] - 153:7, 154:22

adds [1] - 75:1

Adequacy [4] - 95:14, 108:2, 144:21, 163:6

adequacy [12] - 37:4, 38:25, 46:5, 48:16, 88:27, 89:4, 91:2, 94:6, 96:10, 105:19, 108:6, 123:21

adequate [14] - 35:21, 40:10, 44:25, 49:2, 82:29, 83:29, 85:21, 85:25, 89:17, 89:25, 90:9, 96:5, 187:10, 228:17

adequately [2] - 94:25, 217:26

adherence [5] - 49:24, 54:6, 55:11, 63:28, 88:12

adhering [1] - 42:13

ADJOURNED [1] - 232:23

ADJOURNMENT [2] - 127:12, 128:1

adjudicate [1] - 12:17

adjudication [2] - 150:16, 230:9

adjustment [1] - 215:28

adjustments [1] - 104:22

administered [1] - 50:14

Administration [5] - 54:2, 126:29, 196:24, 215:6, 224:4

administration [3] - 117:25, 123:26, 173:14

Administrative [5] - 73:26, 183:16, 183:24, 183:27, 226:1

administrative [10] -

42:16, 61:16, 63:21, 85:10, 126:9, 127:2, 192:1, 206:20, 210:14, 227:22

admissibility [3] - 110:26, 111:22, 165:17

admitted [1] - 186:7

adopt [5] - 54:28, 92:7, 122:11, 123:14

adopted [13] - 27:23, 33:15, 35:12, 39:29, 49:21, 88:27, 108:1, 109:25, 124:4, 176:18, 203:15, 224:5, 224:7

adopting [1] - 122:22

adoption [1] - 94:4

adopts [1] - 97:18

advance [2] - 171:5, 171:16

advanced [1] - 89:6

advancing [1] - 178:3

adversarial [1] - 182:21

adverse [7] - 52:16, 76:5, 196:16, 198:3, 198:6, 198:15, 199:19

adverted [1] - 90:16

advice [13] - 58:24, 59:8, 59:14, 59:18, 60:1, 60:9, 60:11, 62:18, 185:13, 185:15, 185:20, 186:17, 218:18

Advice [1] - 59:11

advices [1] - 187:7

advisable [1] - 57:16

advised [1] - 178:6

advising [1] - 186:26

advocates [1] - 136:16

affairs [2] - 65:12, 133:23

Affairs [1] - 43:13

affairs' [1] - 25:14

affect [3] - 44:5, 50:1, 192:7

affected [4] - 47:8, 55:28, 150:12, 193:9

affecting [3] - 52:14, 53:1, 229:24

affects [1] - 202:13

affidavit [11] - 15:19, 26:24, 128:26, 128:27, 178:27, 186:3, 188:4, 219:18, 220:27, 232:8, 232:10

affiliates [2] - 189:3,

4

189:10

**afford** [1] - 216:19
**afforded** [4] - 77:24, 94:3, 197:17, 200:15
**aforementioned** [1] - 71:17
**afraid** [1] - 179:12
**AFTER** [1] - 128:1
**afternoon** [2] - 128:4, 128:5
**Agencies** [1] - 121:21
**agencies** [30] - 42:16, 66:27, 70:15, 70:20, 91:16, 101:17, 105:15, 107:3, 114:28, 120:18, 121:8, 122:11, 124:9, 126:4, 127:1, 131:16, 140:22, 148:27, 175:16, 175:25, 186:25, 194:16, 194:17, 195:27, 195:29, 201:11, 209:16, 216:11, 225:11, 227:22
**agencies'** [1] - 158:3
**agency** [58] - 35:2, 41:26, 58:22, 66:14, 71:5, 71:13, 74:3, 80:27, 114:13, 114:20, 114:29, 115:21, 126:12, 140:5, 140:24, 140:26, 142:21, 157:12, 157:25, 170:13, 170:25, 171:10, 171:16, 194:19, 194:21, 194:27, 194:29, 195:2, 195:11, 196:10, 196:12, 196:17, 196:19, 196:27, 197:22, 198:11, 198:24, 198:28, 199:4, 199:12, 200:17, 200:20, 200:21, 201:4, 201:7, 201:9, 202:3, 202:9, 202:22, 203:20, 206:14, 206:17, 206:19, 211:9, 216:12, 217:25
**Agency** [12] - 5:23, 21:25, 31:2, 102:25, 105:15, 153:29, 154:4, 194:29, 195:13, 206:26, 214:4, 223:21
**Agency's** [1] - 13:23

**agency's** [1] - 199:2
**agency/component** [1] - 200:22
**agent** [4] - 17:27, 132:6, 132:9, 193:10
**agents** [2] - 49:13, 134:21
**aggrieved** [3] - 191:6, 206:5, 226:27
**ago** [4] - 23:22, 42:8, 100:11, 231:5
**agree** [24] - 9:9, 24:15, 30:1, 30:7, 126:28, 166:7, 166:27, 167:9, 169:7, 169:10, 169:13, 170:24, 171:4, 171:15, 171:29, 173:16, 175:7, 176:3, 177:22, 179:2, 180:8, 182:18, 182:23, 226:6
**agreed** [12] - 21:10, 21:29, 114:4, 116:28, 123:3, 124:25, 128:11, 153:5, 159:7, 183:13, 184:6, 188:23
**agreement** [18] - 21:6, 24:12, 33:24, 33:25, 33:29, 34:5, 35:13, 45:1, 45:2, 117:4, 126:26, 128:23, 150:6, 157:2, 158:9, 184:26, 201:20, 201:25
**Agreement** [3] - 197:8, 227:4, 230:18
**agreement')** [1] - 197:9
**agreements** [2] - 115:16, 200:28
**agrees** [3] - 113:26, 177:14, 179:27
**AHERN** [1] - 2:16
**AI** [1] - 193:24
**AI-Haramain** [1] - 193:24
**albeit** [2] - 90:2, 92:22
**alia** [1] - 19:15
**aliens** [10] - 119:24, 119:28, 120:4, 120:6, 120:8, 120:11, 120:26, 121:3, 121:6, 121:11
**alike** [1] - 140:15
**allegation** [4] - 12:25, 16:3, 78:1, 214:7
**allegations** [25] - 6:16, 6:18, 8:5, 8:7,

9:5, 15:8, 15:18, 15:25, 16:17, 16:21, 16:22, 22:16, 22:21, 22:23, 23:7, 26:24, 31:10, 32:14, 151:15, 153:2, 211:5, 213:17, 214:4, 216:29, 217:2
**allege** [12] - 13:25, 17:1, 18:21, 26:2, 26:11, 26:13, 28:3, 151:16, 209:24, 213:26, 214:15, 217:10
**alleged** [14] - 6:28, 9:9, 9:12, 15:27, 23:10, 152:23, 180:22, 186:21, 189:23, 209:28, 209:29, 213:11, 214:8, 216:11
**alleged'** [1] - 32:11
**allegedly** [5] - 6:2, 9:21, 17:6, 182:16, 183:28
**alleging** [6] - 5:21, 12:22, 104:27, 110:17, 161:22, 209:27
**Alliance** [1] - 2:25
**allied** [2] - 147:14
**allies** [1] - 146:9
**allow** [4] - 28:10, 30:25, 80:28, 142:15
**allowed** [1] - 49:26
**allowing** [2] - 12:16, 109:10
**allows** [5] - 59:15, 133:5, 135:20, 153:9, 194:14
**almost** [1] - 226:13
**alone** [2] - 9:8, 68:19
**alongside** [1] - 37:17
**alter** [4] - 30:26, 205:10, 214:13, 214:21
**Alternative** [2] - 56:20, 113:9
**alternative** [8] - 35:10, 51:5, 54:21, 54:25, 59:24, 59:28, 112:25, 203:16
**alternatively** [1] - 60:17
**Alternatively** [1] - 96:8
**alternatives** [1] - 56:19
**ambiguities** [1] - 200:13
**ambiguous** [1] -

202:6

**amend** [3] - 96:9, 198:25, 199:7
**Amended** [1] - 23:10
**amended** [2] - 13:1, 122:4
**amending** [1] - 46:13
**amendment** [2] - 20:18, 97:6
**Amendment** [19] - 5:24, 13:3, 23:25, 84:2, 84:6, 84:19, 154:5, 154:14, 155:3, 155:6, 157:29, 176:9, 176:11, 176:22, 177:2, 177:4, 177:10, 177:15, 177:20
**Amendment'** [1] - 19:17
**Amendment's** [2] - 155:15, 176:19
**amendments** [1] - 132:15
**Amendments** [2] - 13:29, 214:6
**amends** [1] - 177:21
**AMERICA** [1] - 2:19
**American** [4] - 6:7, 10:14, 129:5, 223:22
**amici** [2] - 90:12, 187:29
**amicus** [1] - 19:27
**Amnesty** [3] - 14:20, 24:26, 152:3
**amount** [8] - 11:22, 12:23, 21:5, 69:9, 89:25, 191:28, 206:10, 217:2
**amounted** [1] - 218:24
**amounts** [1] - 143:2
**analogous** [1] - 7:3
**analogue** [1] - 17:27
**analogy** [1] - 18:1
**analyse** [2] - 136:28, 227:17
**analysed** [4] - 48:3, 48:27, 73:8, 215:23
**analysing** [1] - 105:20
**analysis** [16] - 31:25, 64:26, 69:2, 90:27, 105:24, 139:19, 145:7, 155:19, 157:28, 211:14, 212:11, 212:12, 214:13, 214:21, 226:14, 228:24
**analysts** [2] - 137:21, 171:10

**analysts'** [3] - 170:13, 170:26, 171:17
**analyze** [1] - 137:8
**analyzed** [1] - 158:17
**AND** [2] - 1:13, 150:8
**Annex** [17] - 40:17, 40:23, 41:4, 41:12, 41:22, 44:17, 45:12, 47:1, 48:22, 50:17, 50:20, 50:21, 57:10, 63:27, 64:21, 76:22, 98:26
**annex** [6] - 40:25, 42:25, 77:10, 81:28, 85:3, 224:26
**annexed** [3] - 46:19, 48:19, 96:19
**annexes** [4] - 35:19, 54:4, 61:29, 97:20
**Annexes** [2] - 40:19, 48:24
**announced** [2] - 98:17, 228:7
**annual** [3] - 46:2, 95:1, 109:2
**annually** [1] - 170:19
**another'** [1] - 34:29
**answer** [2] - 89:15, 177:7
**Anthony** [2] - 26:18, 42:26
**anti** [1] - 208:17
**anti-hacking** [1] - 208:17
**anticipate** [1] - 232:19
**anticipating** [1] - 87:17
**anticipation** [2] - 13:7, 195:6
**anyway** [1] - 87:28
**APA** [2] - 183:15, 184:1
**apart** [1] - 35:3
**apparatus** [1] - 106:21
**appeal** [5] - 13:19, 31:14, 119:10, 126:12, 158:19
**appealed** [2] - 5:29, 152:26
**Appeals** [3] - 6:1, 27:6, 118:18
**appear** [4] - 93:11, 144:5, 216:17, 229:9
**APPEARANCES** [1] - 2:3
**appeared** [1] - 30:25
**appellant** [1] - 3:10

5

appendix [1] - 129:1
APPLICABILITY [1] -
154:25
applicability [1] -
179:25
applicable [10] -
15:3, 64:22, 72:25,
83:27, 100:22,
102:19, 104:1,
121:22, 122:9, 124:10
application [19] -
6:17, 20:15, 20:19,
27:12, 44:6, 50:2,
53:26, 94:18, 119:10,
134:19, 153:26,
167:20, 174:22,
175:1, 176:9, 180:17,
181:5, 186:26, 208:17
applications [1] -
131:21
applied [12] - 19:6,
30:22, 103:27,
126:10, 126:13,
127:1, 167:23, 168:3,
169:24, 200:5, 200:6,
215:28
applies [14] - 29:6,
49:13, 65:21, 77:28,
113:14, 163:10,
166:29, 176:11,
176:22, 177:20,
195:4, 204:19,
204:25, 204:27
apply [39] - 49:27,
50:5, 91:25, 104:9,
108:19, 119:12,
140:17, 148:7,
148:28, 155:15,
163:13, 164:11,
164:12, 166:22,
166:23, 167:2, 167:6,
175:9, 175:16,
175:18, 175:25,
175:26, 177:4,
177:15, 179:29,
180:5, 192:29,
195:28, 199:25,
199:26, 200:10,
205:4, 212:11, 217:7,
217:20, 229:1, 229:9,
229:20
applying [1] - 177:10
appointed [3] -
19:27, 71:7, 100:1
appointee [2] -
116:6, 116:7
appreciable [1] -
30:27
approach [9] - 25:18,
59:11, 106:8, 176:18,

187:13, 190:5,
203:14, 203:24, 204:4
appropriate [18] -
46:28, 51:5, 95:28,
97:3, 97:15, 99:13,
99:16, 102:17,
104:28, 123:1,
146:20, 178:28,
185:19, 188:28,
190:10, 206:13,
206:16, 219:11
appropriate' [2] -
51:27, 211:7
approval [4] - 71:8,
134:8, 181:29, 194:9
approve [4] - 170:13,
170:19, 170:25,
171:16
approved [7] - 67:29,
134:6, 136:24,
140:22, 169:29,
171:13, 232:9
approving [2] -
170:9, 171:10
April [2] - 138:9,
186:9
arbitral [2] - 41:5,
57:10
arbitration [8] -
35:11, 41:8, 41:9,
54:26, 57:8, 61:22,
62:1, 62:13
arbitrators [1] -
61:27
area [4] - 24:11,
53:2, 122:28, 185:18
areas [5] - 19:24,
52:12, 65:21, 72:26,
224:12
argue [3] - 15:1,
16:11, 18:11
argued [1] - 173:8
argues [3] - 6:16,
151:29, 155:21
argument [4] - 15:7,
90:11, 152:3, 155:10
arguments [5] -
6:14, 12:8, 14:27,
19:1, 19:3
arise [5] - 86:21,
86:22, 104:16,
186:11, 190:3
arises [1] - 15:5
arising [5] - 186:23,
189:24, 204:8,
213:11, 213:22
arm [1] - 85:6
arms [1] - 147:14
Army [1] - 203:28
arose [1] - 22:28

arrangement [9] -
33:7, 34:20, 42:12,
92:18, 107:18,
107:19, 107:27,
117:6, 124:5
arrangements [4] -
33:22, 34:17, 63:16,
94:28
array [1] - 142:24
Article [65] - 6:27,
14:4, 14:18, 16:21,
23:11, 24:15, 24:18,
24:20, 24:29, 25:21,
26:8, 27:4, 27:9,
27:19, 27:29, 28:5,
28:14, 29:22, 30:10,
30:12, 30:23, 32:3,
34:14, 34:16, 39:12,
39:13, 39:15, 39:19,
40:7, 40:9, 43:24,
44:5, 44:7, 44:9,
44:11, 44:13, 44:22,
45:8, 45:29, 46:8,
46:13, 47:7, 48:17,
65:14, 88:19, 88:28,
89:26, 92:9, 94:29,
107:16, 107:22,
110:5, 111:25,
111:26, 120:26,
190:8, 211:19,
212:23, 213:8, 213:9,
214:9, 214:10,
214:17, 216:26
article [2] - 223:29,
224:27
Articles [5] - 35:22,
69:16, 105:22,
110:19, 123:21
articles [1] - 222:23
articulated [1] -
145:28
articulates [1] -
145:13
AS [2] - 5:1, 128:1
aside [1] - 90:25
aspect [2] - 100:6,
117:5
aspects [6] - 6:19,
91:13, 91:14, 95:6,
108:11, 108:15
assert [2] - 14:4,
231:21
asserted [2] -
151:21, 216:7
assertions [1] -
22:22
assess [5] - 82:10,
94:17, 109:15,
157:28, 206:9
assessed [2] - 69:26,

109:4
assesses [1] - 29:7
assessing [1] -
44:24
assessment [7] -
69:12, 83:13, 83:28,
94:24, 97:8, 184:2,
200:2
assist [6] - 19:21,
49:16, 77:16, 99:13,
109:27, 188:13
assistance [1] -
128:10
Assistant [2] - 43:11,
223:6
associated [6] -
10:5, 11:2, 118:1,
139:12, 140:26,
142:27
Association [1] -
222:26
assume [1] - 22:20
assumed [1] - 200:4
assuming [5] -
35:15, 87:18, 92:28,
217:6, 232:15
assumption [1] -
177:6
assurance [2] -
67:16, 83:27
assurances [3] -
35:17, 68:12, 108:28
assure [2] - 199:15,
217:27
AT [1] - 232:24
AT&T [1] - 139:5
ate [1] - 206:15
attached [1] - 117:22
attaches [1] - 11:28
attachment [1] -
42:19
attachments [1] -
43:22
attack [1] - 178:7
attempt [4] - 120:4,
180:1, 180:9, 215:10
attention [14] -
21:19, 37:25, 39:10,
100:8, 106:18,
118:11, 121:17,
123:27, 185:20,
196:6, 201:2, 220:20,
224:16, 231:6
attesting [1] - 134:6
Attorney [6] - 5:21,
43:12, 68:1, 126:22,
140:23, 200:23
attorney [5] - 5:28,
6:2, 129:10, 185:17,
212:4

attorney's [1] - 6:5
Attorney-General [1]
- 68:1
Attorneys [1] -
227:24
attorneys [1] -
156:19
attorneys' [3] -
193:17, 198:19, 199:8
audiences [1] -
129:14
auditing [1] - 70:7
audits [1] - 71:13
auth01izes [1] -
134:17
authentic [1] - 11:28
author [3] - 222:24,
223:15, 224:1
authored [1] -
224:10
authorisation [8] -
72:6, 84:14, 85:5,
168:1, 181:28, 194:9,
205:14, 209:9
authorise [2] - 72:12,
171:4
authorised [6] -
51:24, 53:16, 68:6,
69:7, 205:11, 210:12
authorises [5] -
69:18, 72:13, 168:25,
198:23, 198:27
authoritative [1] -
41:15
Authorities [4] -
24:6, 38:6, 110:7,
110:11
authorities [60] -
12:2, 12:3, 16:8,
20:22, 38:7, 43:15,
44:11, 45:19, 46:17,
46:21, 48:11, 48:24,
55:15, 56:16, 61:6,
63:14, 64:6, 64:23,
69:28, 71:20, 74:13,
79:15, 79:17, 79:22,
80:12, 83:6, 83:23,
84:13, 84:18, 84:24,
88:7, 89:1, 95:23,
96:3, 96:17, 96:21,
97:13, 98:13, 101:25,
101:27, 108:8,
108:12, 108:20,
109:12, 109:19,
111:28, 111:29,
117:8, 117:9, 117:13,
117:14, 117:15,
129:23, 130:4,
130:12, 130:13,
156:7, 165:1, 178:27,

6

202:29

**Authority** [3] - 163:18, 166:28, 167:2

**authority** [48] - 10:2, 13:29, 57:1, 59:6, 59:22, 60:6, 60:12, 62:4, 62:14, 65:10, 79:27, 79:28, 89:2, 111:28, 114:10, 114:28, 115:7, 115:11, 115:17, 115:24, 118:4, 134:1, 137:7, 140:12, 140:29, 145:2, 157:4, 157:22, 158:24, 159:13, 164:23, 166:14, 166:22, 167:6, 178:21, 181:1, 181:21, 202:2, 202:23, 207:16, 207:19, 208:21, 210:8, 210:22, 210:27, 211:7, 211:10

**Authority'** [1] - 166:15

**authorization** [5] - 133:27, 205:16, 208:26, 208:27, 209:11

**authorize** [2] - 169:11, 199:10

**authorized** [6] - 8:28, 68:20, 130:27, 139:2, 146:7, 147:29

**authorizes** [8] - 129:28, 130:1, 133:8, 141:23, 143:7, 149:11, 167:10, 190:23

**authorizing** [5] - 132:3, 132:23, 133:28, 168:12, 171:1

**automated** [3] - 52:13, 52:28, 108:16

**availability** [3] - 113:10, 146:12, 155:19

**AVAILABLE** [1] - 190:21

**available** [46] - 34:8, 44:2, 45:29, 54:5, 54:12, 54:16, 56:8, 61:20, 62:25, 63:19, 64:4, 66:22, 70:1, 72:21, 73:3, 73:22, 74:16, 74:23, 86:17, 88:3, 95:17, 111:20, 113:12, 147:3, 160:2, 173:18, 186:20, 187:2, 187:3, 187:9,

189:21, 190:27, 192:2, 199:26, 206:21, 212:13, 216:2, 216:20, 217:17, 217:23, 218:3, 218:6, 227:6, 227:23, 231:19

**availed** [2] - 93:12, 93:17

**availing** [1] - 93:22

**avenue** [6] - 76:9, 76:18, 93:14, 100:25, 100:27, 158:28

**avenues** [8] - 61:20, 62:24, 70:1, 72:21, 73:14, 74:9, 100:20, 100:21

**averments** [1] - 12:13

**Aviation** [2] - 196:24, 215:6

**avoid** [2] - 7:11, 191:11

**award** [3] - 62:8, 191:27, 215:3

**Award** [1] - 222:29

**awarded** [1] - 222:28

**awards** [1] - 36:15

**aware** [4] - 38:3, 110:28, 126:25, 156:13

## B

**backbone** [1] - 139:7

**background** [9] - 5:19, 14:13, 37:23, 47:17, 118:27, 138:19, 186:13, 220:2, 225:22

**bags** [2] - 100:7, 100:11

**ban** [1] - 44:14

**BANK** [1] - 2:11

**bans** [1] - 230:18

**Bar** [1] - 178:13

**bar** [7] - 94:22, 178:18, 178:23, 179:3, 179:5, 179:10, 179:16

**bar'** [1] - 178:29

**Barack** [3] - 130:5, 145:12, 223:6

**bare** [2] - 22:22, 28:3

**barred** [2] - 206:15, 230:22

**barrier** [1] - 205:24

**barriers** [4] - 130:18, 150:16, 190:13,

212:15

**barring** [1] - 203:6

**BARRINGTON** [1] - 2:19

**BARROW** [1] - 2:12

**based** [20] - 11:29, 12:1, 47:21, 49:10, 50:15, 59:24, 67:1, 67:29, 78:26, 101:6, 104:13, 123:23, 146:3, 153:19, 172:10, 211:4, 213:17, 214:11, 218:22, 228:24

**Based** [4] - 48:29, 139:25, 214:15, 228:9

**baseline** [1] - 226:9

**bases** [4] - 67:2, 74:12, 155:10, 229:14

**basic** [4] - 63:7, 80:1, 86:5, 132:12

**basis** [26] - 15:29, 16:23, 19:18, 32:25, 35:20, 36:2, 45:28, 45:29, 52:29, 53:23, 63:10, 68:22, 69:19, 71:2, 83:3, 86:17, 88:3, 95:13, 95:16, 97:18, 139:18, 142:11, 199:18, 216:10, 219:25, 228:16

**basis'** [1] - 66:20

**Bates** [1] - 170:3

**Bay** [1] - 156:21

**BCRs** [1] - 229:21

**bearing** [2] - 133:22, 141:2

**bears** [2] - 15:15, 134:13

**become** [1] - 216:2

**BEFORE** [1] - 1:17

**beg** [3] - 48:8, 117:15, 184:22

**began** [1] - 138:27

**beginning** [1] - 91:24

**begins** [1] - 14:18

**begun** [1] - 206:18

**behalf** [3] - 98:14, 112:29, 218:28

**behind** [2] - 115:24, 122:22

**Belgian** [1] - 223:20

**believes** [4] - 30:16, 30:22, 31:11, 32:12

**belonging** [1] - 155:17

**belongs** [1] - 201:5

**below** [13] - 57:17, 65:6, 101:4, 129:22,

132:13, 132:17, 140:25, 141:6, 142:5, 146:26, 149:29, 190:14, 216:27

**benefit** [3] - 79:26, 84:10, 84:19

**benefits** [1] - 199:17

**best** [5] - 21:17, 60:28, 126:19, 162:5, 224:9

**better** [3] - 47:15, 93:21, 162:23

**between** [33] - 7:6, 15:7, 17:15, 21:6, 24:12, 28:18, 33:25, 35:13, 36:7, 45:1, 63:23, 90:4, 91:10, 99:27, 100:9, 112:20, 112:26, 116:16, 133:7, 135:29, 144:13, 151:18, 156:29, 159:9, 168:4, 184:26, 197:7, 197:11, 204:24, 221:26, 230:19, 231:6, 231:12

**beyond** [9] - 8:4, 27:2, 45:22, 76:27, 114:14, 114:22, 115:2, 123:16, 208:26

**bids** [1] - 19:7

**Bill** [1] - 223:2

**billions** [1] - 144:8

**bind** [1] - 66:12

**binding** [14] - 33:18, 57:8, 61:22, 70:28, 88:28, 89:13, 90:17, 100:19, 109:21, 114:18, 115:11, 115:22, 158:7, 230:3

**Binding** [1] - 229:17

**biographical** [4] - 189:14, 221:11, 225:3, 231:27

**bipartisan** [1] - 71:6

**bit** [5] - 36:22, 39:6, 41:29, 54:19, 184:6

**bits** [3] - 159:8, 184:8, 218:21

**BL** [7] - 2:5, 2:10, 2:15, 2:20, 2:25, 2:30, 3:2

**blanket** [2] - 195:2, 195:10

**block** [1] - 153:9

**blocking** [1] - 156:18

**Blue** [1] - 203:28

**Board** [9] - 10:26, 70:11, 70:12, 71:5, 71:7, 101:19, 115:6,

158:5, 227:14

**Board..** [1] - 71:18

**bodies** [15] - 45:10, 47:4, 78:11, 78:22, 79:3, 80:17, 80:23, 82:22, 101:6, 101:10, 104:29, 105:1, 112:1, 115:7, 225:9

**Body** [5] - 102:1, 102:6, 102:10, 102:18, 104:3

**body** [13] - 17:21, 53:16, 56:28, 58:2, 58:7, 79:18, 80:22, 85:9, 101:29, 102:22, 104:28, 128:29, 162:12

**Book** [8] - 5:13, 20:26, 24:6, 34:1, 38:6, 38:10, 128:26

**book** [15] - 13:16, 117:7, 117:12, 117:13, 117:14, 117:16, 129:1, 138:17, 185:10, 219:14, 219:15, 222:3, 223:15, 224:3, 224:10

**booklet** [1] - 219:13

**booklets** [1] - 21:9

**books** [4] - 34:1, 107:21, 145:4, 222:22

**Border** [1] - 126:16

**bottom** [4] - 52:27, 55:8, 212:20, 221:14

**bound** [2] - 49:15, 66:17

**boundaries** [1] - 65:18

**branch** [12] - 70:6, 71:6, 114:13, 115:12, 115:22, 117:27, 120:21, 134:11, 145:13, 157:25, 158:8, 173:8

**branch's** [1] - 157:2

**branches** [3] - 25:3, 25:7, 25:13

**breach** [4] - 62:28, 78:2, 198:5, 213:23

**breach'** [1] - 213:19

**breached** [1] - 59:23

**breaches** [1] - 213:11

**breadth** [1] - 141:11

**break** [1] - 127:7

**breaking** [1] - 93:4

**BRIAN** [1] - 2:4

**brief** [1] - 220:28

**briefly** [5] - 5:10,

8

232:18, 232:21
**Collins** [6] - 106:17, 122:26, 124:20, 124:23, 222:2, 222:3
**Collins'** [1] - 123:1
**COLM** [1] - 3:1
**colours** [1] - 184:2
**Columbia** [2] - 186:7, 204:7
**column** [2] - 6:11, 28:27
**COM** [1] - 48:13
**combination** [2] - 228:2, 231:14
**coming** [4] - 33:6, 38:4, 89:29, 95:12
**command** [1] - 209:6
**Commander** [1] - 65:10
**commence** [1] - 206:7
**commenced** [2] - 197:10, 206:12
**commends** [1] - 108:7
**comment** [3] - 31:5, 59:13, 114:2
**comments** [3] - 123:1, 123:4, 178:10
**Commerce** [24] - 40:16, 40:24, 41:14, 44:3, 49:25, 50:15, 50:17, 51:4, 54:5, 54:10, 55:6, 55:18, 55:20, 58:16, 58:20, 59:29, 60:27, 61:28, 63:3, 86:2, 95:5, 95:8, 95:27, 223:16
**COMMERCIAL** [1] - 1:3
**commercial** [4] - 50:9, 108:11, 108:15, 146:6
**Commission** [84] - 32:27, 32:29, 35:12, 35:14, 35:15, 35:19, 35:20, 37:13, 38:24, 39:2, 42:6, 42:8, 42:15, 44:20, 44:22, 45:9, 45:17, 45:28, 46:7, 46:11, 47:3, 47:6, 47:21, 47:25, 48:3, 48:10, 48:27, 49:1, 50:19, 60:13, 61:7, 61:28, 63:2, 64:3, 65:4, 67:16, 68:22, 69:26, 73:13, 74:6, 75:18, 76:21, 82:29, 83:3, 85:24, 86:1, 87:18, 88:5,

88:18, 88:23, 88:27, 89:3, 89:13, 89:17, 89:23, 89:24, 90:16, 90:17, 94:4, 94:9, 94:15, 94:17, 95:4, 95:11, 95:17, 96:6, 96:9, 96:14, 96:25, 104:13, 104:21, 106:1, 108:1, 108:8, 110:17, 110:22, 110:25, 111:5, 112:2, 117:11, 117:21, 144:20, 163:5
**Commission's** [5] - 64:26, 69:12, 83:13, 83:18, 83:28
**Commissioner** [16] - 5:6, 36:25, 40:25, 42:26, 89:28, 92:16, 98:9, 128:6, 185:14, 185:29, 186:9, 186:13, 187:7, 187:20, 187:25, 218:17
**COMMISSIONER** [1] - 1:7
**Commissioner's** [5] - 90:26, 92:20, 112:18, 185:8, 189:4
**commit** [4] - 35:25, 49:12, 56:15, 109:26
**commitment** [6] - 50:16, 59:22, 62:23, 79:7, 96:29, 108:26
**commitments** [19] - 40:18, 45:3, 46:18, 48:5, 48:23, 48:29, 77:1, 86:19, 88:5, 96:18, 102:9, 104:9, 104:12, 104:15, 104:20, 105:29, 106:3, 130:14, 146:25
**commits** [1] - 80:7
**committed** [10] - 45:5, 49:26, 60:28, 62:20, 64:11, 82:12, 94:15, 121:6, 121:13, 143:21
**Committee** [4] - 46:8, 129:15, 141:17, 164:25
**committees** [2] - 222:24, 227:15
**Committees** [1] - 71:29
**committing** [1] - 117:26
**common** [1] - 104:13
**communicate** [7] - 13:25, 102:9, 104:2,

168:10, 169:8, 172:17, 172:21
**communicated** [1] - 52:8
**communicates** [1] - 81:6
**communicating** [1] - 104:4
**Communication** [2] - 43:18, 48:13
**communication** [13] - 17:17, 18:6, 133:10, 135:28, 135:29, 168:18, 168:19, 169:19, 205:7, 205:12, 205:15, 208:24, 228:29
**communications** [108] - 9:7, 10:8, 13:27, 17:7, 17:9, 17:15, 18:14, 19:20, 22:11, 23:4, 29:13, 65:5, 130:23, 131:3, 131:6, 132:1, 132:16, 132:24, 133:6, 133:9, 134:11, 135:3, 135:7, 135:17, 135:21, 136:7, 136:9, 136:11, 136:13, 136:15, 136:19, 136:29, 137:9, 137:13, 137:20, 138:4, 138:8, 138:9, 139:3, 139:8, 139:11, 139:21, 140:5, 140:6, 141:28, 142:5, 142:9, 142:17, 142:20, 142:23, 144:19, 144:28, 145:1, 145:16, 145:18, 145:20, 147:27, 148:15, 151:1, 152:6, 152:24, 156:11, 156:16, 156:22, 158:25, 159:23, 161:26, 162:1, 162:8, 162:12, 162:13, 162:28, 163:23, 166:16, 166:18, 167:11, 167:17, 167:24, 167:25, 168:2, 168:7, 168:13, 168:16, 168:17, 168:26, 169:12, 169:14, 169:18, 169:26, 169:27, 171:15, 172:5, 172:13, 172:29, 174:22, 175:10, 175:20, 176:4, 176:7, 181:21,

204:16, 204:17, 204:23, 204:28, 205:3, 205:5, 214:7, 228:27
**Communications** [10] - 73:19, 85:18, 85:20, 139:16, 191:2, 204:12, 204:15, 204:19, 223:10, 227:9
**communications'** [2] - 142:12, 168:22
**communities** [1] - 120:9
**community** [7] - 64:14, 70:22, 116:3, 116:11, 122:16, 141:1, 158:13
**Community** [21] - 65:19, 66:13, 67:17, 71:12, 72:24, 78:13, 80:24, 80:25, 81:24, 99:4, 99:19, 99:26, 99:28, 105:11, 105:13, 106:22, 106:28, 107:2, 112:1, 116:18, 116:25
**companies** [29] - 10:3, 33:16, 35:3, 35:27, 41:9, 42:10, 52:12, 54:23, 56:1, 58:17, 63:22, 84:12, 84:18, 91:10, 96:29, 113:2, 113:4, 113:12, 114:19, 132:25, 138:5, 139:5, 161:20, 161:25, 166:24, 227:17, 227:20, 229:3
**companies'** [2] - 144:13, 173:24
**company** [16] - 9:18, 35:9, 42:17, 54:24, 56:27, 57:3, 57:21, 57:23, 62:16, 63:24, 87:10, 93:4, 112:21, 161:22, 189:2, 228:28
**Company** [1] - 161:15
**company's** [1] - 9:23
**comparable** [3] - 148:22, 149:6, 164:16
**Compare** [1] - 7:22
**compared** [2] - 167:14, 187:3
**comparing** [1] - 226:7
**compatibility** [3] - 78:20, 80:16, 101:8
**compatible** [1] - 51:13
**compel** [1] - 10:2

**compelled** [3] - 113:2, 138:26, 162:1
**compelling** [1] - 225:13
**compensatory** [2] - 196:22, 209:20
**competence** [1] - 109:5
**competent** [6] - 44:11, 59:21, 78:11, 79:15, 101:25, 203:13
**competing** [1] - 125:11
**compiled** [2] - 195:5, 208:11
**complainant** [4] - 60:23, 157:8, 157:18, 196:18
**complained** [2] - 81:12, 151:19
**complains** [1] - 158:15
**Complaint** [2] - 23:10, 102:5
**complaint** [57] - 11:15, 11:26, 11:27, 13:1, 32:15, 35:1, 35:5, 35:6, 35:8, 36:17, 54:15, 55:22, 56:26, 58:1, 59:1, 59:11, 59:17, 60:10, 60:21, 60:23, 61:21, 63:20, 77:12, 77:13, 77:26, 79:8, 79:22, 79:23, 82:3, 82:11, 87:9, 87:11, 89:2, 90:3, 90:19, 91:15, 93:1, 93:2, 93:6, 93:7, 97:10, 100:26, 100:28, 102:3, 102:22, 102:23, 103:19, 103:22, 111:22, 113:22, 151:15, 157:7, 157:9, 157:28, 158:17, 184:18, 185:15
**complaint'** [1] - 103:3
**complaints** [22] - 34:27, 34:29, 41:8, 46:26, 54:17, 55:29, 56:2, 56:9, 57:5, 58:5, 58:21, 58:29, 60:29, 61:11, 77:3, 78:14, 79:14, 82:19, 82:26, 96:24, 101:6
**Complaints** [4] - 102:1, 102:10, 102:18, 104:3
**complaint—**

10

accordingly [1] - 12:5

complemented [2] - 71:18, 226:20

complete [4] - 9:17, 96:7, 102:6, 157:27

complete' [1] - 80:2

completed [1] - 102:14

completely [3] - 90:7, 122:1, 123:4

completeness [2] - 189:6, 199:14

compliance [44] - 32:28, 45:11, 49:20, 53:6, 53:17, 55:28, 56:1, 57:20, 58:8, 58:11, 58:14, 58:19, 61:1, 61:7, 61:16, 62:5, 70:14, 71:19, 71:26, 77:7, 79:5, 79:6, 80:10, 80:22, 80:28, 81:1, 82:6, 87:16, 89:3, 90:9, 95:9, 95:21, 95:29, 96:5, 97:9, 105:21, 114:22, 115:2, 157:14, 157:15, 158:17, 166:3, 193:4, 217:21

compliant [1] - 53:8

complied [13] - 72:25, 77:6, 77:18, 77:20, 82:5, 102:28, 103:5, 103:6, 114:15, 157:14, 158:2, 192:25, 210:24

complies [1] - 66:28

comply [15] - 41:17, 46:17, 49:26, 55:5, 59:17, 60:1, 60:2, 62:17, 62:22, 96:17, 130:13, 182:24, 196:12, 196:14, 198:28

complying [3] - 60:18, 93:2, 93:5

component [8] - 25:1, 199:5, 200:21, 201:4, 202:3, 202:9, 202:22, 203:20

component' [2] - 200:17, 200:20

components [2] - 126:14, 126:15

comport [1] - 19:16

composed [2] - 71:6, 111:27

comprehensive [3] - 95:5, 220:1, 228:9

comprised [1] -

110:5

compromise [1] - 225:18

compromised [1] - 18:26

compulsory [1] - 113:14

Computer [3] - 73:18, 208:15, 208:16

computer [6] - 208:20, 208:22, 208:26, 209:7, 209:8, 209:11

conceded [2] - 141:18, 164:25

conceivably [1] - 90:6

concept [2] - 76:28, 123:21

concern [3] - 19:8, 91:5, 122:28

concerned [15] - 28:7, 36:5, 41:9, 44:19, 58:29, 63:15, 63:24, 68:14, 75:6, 76:4, 80:27, 81:7, 91:8, 105:16, 199:29

concerning [17] - 7:21, 12:13, 18:14, 55:11, 91:20, 108:15, 108:19, 108:22, 139:25, 148:22, 149:6, 149:12, 156:22, 192:16, 192:27, 199:13, 217:26

concerns [16] - 29:21, 33:2, 33:4, 72:22, 76:26, 90:22, 91:3, 91:4, 98:23, 107:17, 107:20, 108:6, 108:11, 174:12, 180:25, 226:28

conclude [2] - 51:29, 59:22

concluded [5] - 6:25, 23:29, 207:21, 209:26, 226:8

concludes [9] - 23:8, 29:22, 49:1, 68:23, 83:4, 88:18, 95:17, 135:22, 224:25

conclusion [7] - 31:15, 31:28, 177:10, 215:18, 228:11, 228:17, 230:13

CONCLUSION [1] - 158:21

conclusions [5] -

22:22, 31:12, 31:26, 218:12, 228:23

conclusively [1] - 9:10

concrete [7] - 24:21, 28:4, 30:24, 108:28, 212:24, 214:16, 217:11

concurrence [1] - 201:3

concurs [1] - 177:9

conditions [6] - 46:20, 73:23, 96:12, 96:20, 211:23, 230:19

conduct [19] - 15:22, 34:23, 65:11, 108:26, 119:29, 137:25, 137:28, 140:14, 141:24, 151:19, 157:27, 192:7, 204:20, 204:21, 208:23, 209:6, 209:9, 209:12, 211:6

conducted [14] - 62:1, 130:3, 130:10, 131:17, 132:27, 133:1, 133:18, 133:19, 140:17, 140:19, 151:28, 163:16, 163:17, 176:17

conducting [1] - 131:26

conducts [3] - 130:29, 139:5, 164:23

confer [1] - 213:8

confidential [1] - 209:2

confidentiality [2] - 18:25, 210:6

confined [4] - 123:2, 123:6, 123:9, 124:27

confirm [11] - 79:5, 103:13, 103:26, 113:22, 114:6, 157:17, 184:17, 188:20, 189:6, 189:8, 195:16

confirmation [3] - 52:6, 77:5, 82:8

confirmed [2] - 14:24, 83:13

confirming [2] - 102:22, 113:28

confirms [2] - 188:6, 221:6

conflict [1] - 189:5

conform [1] - 53:12

conformity [3] - 181:28, 194:8, 198:26

conforms [1] - 69:12

confusion [1] - 191:11

Congress [13] - 65:16, 66:17, 71:1, 72:1, 131:9, 131:16, 132:21, 141:13, 141:19, 156:2, 164:27, 165:1, 222:24

congressional [1] - 131:14

Congressional [6] - 65:22, 164:19, 165:4, 165:6, 220:3, 227:14

conjectural [1] - 151:23

conjunction [2] - 37:17, 216:22

connected [3] - 134:22, 188:20, 221:6

connection [8] - 36:7, 99:27, 100:9, 116:16, 139:14, 151:18, 186:10, 231:20

connection' [1] - 177:18

connections [1] - 177:1

connections' [1] - 177:12

consequence [3] - 76:5, 97:12, 97:13

consequences [4] - 48:2, 58:18, 198:3, 198:6

Consequently [1] - 88:27

consequently [1] - 199:19

consider [13] - 11:11, 12:10, 24:1, 35:20, 37:17, 59:29, 90:25, 91:17, 97:5, 146:12, 187:7, 188:28, 200:1

considerably [1] - 138:19

consideration [5] - 25:17, 80:21, 101:19, 108:9, 200:19

considerations [1] - 148:2

considered [11] - 37:15, 68:17, 80:2, 135:23, 187:10, 201:23, 202:11, 202:17, 203:21, 203:29, 218:23

considering [1] -

185:14

considers [9] - 60:9, 63:2, 85:25, 86:1, 86:8, 88:6, 89:6, 90:21, 176:19

consistent [8] - 9:19, 30:16, 120:26, 121:21, 122:9, 124:10, 148:29, 173:16

consisting [1] - 224:26

consists [4] - 10:28, 134:1, 170:15, 204:18

constant [1] - 16:6

constitute [3] - 48:25, 113:5, 209:2

constituted [1] - 40:15

constitutes [2] - 149:13, 181:17

CONSTITUTION [1] - 154:25

Constitution [7] - 65:8, 65:14, 71:20, 120:27, 130:13, 155:1, 211:19

constitutional [10] - 6:21, 7:4, 13:22, 20:7, 25:18, 151:10, 155:23, 165:20, 181:9, 225:24

constitutionality [2] - 130:15, 165:27

constraint [1] - 160:8

constraints [8] - 104:16, 104:19, 131:8, 145:16, 146:26, 148:17, 159:27, 186:28

construction [1] - 203:3

construe [1] - 202:20

consumer [1] - 112:20

contact [4] - 76:25, 98:22, 145:3, 145:5

Contact [1] - 47:23

contacts [1] - 57:21

contain [5] - 74:3, 126:6, 135:22, 137:10, 160:14

contained [12] - 40:18, 46:18, 48:13, 48:24, 50:20, 64:21, 76:21, 96:18, 160:12, 168:28, 199:2, 210:9

containing [4] - 139:16, 145:18,

11

13

declarations [1] - 111:4

declared [2] - 33:11, 76:14

declassification [1] - 173:6

declassified [1] - 173:17

declassify [2] - 173:9, 173:15

declined [1] - 155:14

decrypt [1] - 140:3

deems [1] - 211:6

deeply [2] - 130:15, 180:29

default [2] - 137:16, 149:18

defence [1] - 195:23

defendant [2] - 11:28, 181:3

Defendant [1] - 189:2

DEFENDANT [2] - 2:9, 2:14

defendant's [1] - 26:4

defendants [6] - 19:17, 180:27, 180:28, 181:2, 181:18, 187:28

DEFENDANTS [1] - 1:13

defendants' [2] - 14:3, 181:6

defendant's [1] - 15:21

defense [3] - 141:2, 194:26, 208:3

DEFENSE [1] - 154:25

DEFENSES [1] - 150:8

deficiencies [1] - 218:24

defined [9] - 80:26, 109:6, 141:25, 142:8, 143:9, 159:28, 176:5, 193:1, 210:1

defines [4] - 133:20, 147:28, 174:23, 228:27

definition [8] - 148:4, 200:16, 201:22, 202:5, 202:15, 205:22, 207:6, 209:27

definitions [1] - 200:14

definitive [1] - 44:14

defraud [1] - 208:25

defunct [1] - 8:28

defy [1] - 22:23

degree [3] - 15:16, 27:10, 32:6

delay [2] - 44:20, 59:19

deletion [1] - 58:13

deliver [1] - 59:14

delivered [4] - 58:25, 59:8, 187:19, 188:3

delivery [1] - 59:18

democracy [1] - 225:24

democratic [1] - 231:23

demonstrate [8] - 8:12, 28:14, 32:9, 80:3, 82:26, 83:29, 96:3, 134:20

demonstrates [2] - 172:12, 172:28

denial [1] - 206:19

denied [2] - 22:7, 167:20

deny [5] - 103:13, 113:22, 114:7, 157:17, 184:18

denying [1] - 113:28

departed [1] - 106:3

department [3] - 78:17, 206:14, 211:9

Department [44] - 40:16, 41:13, 41:16, 42:27, 43:11, 43:13, 44:3, 49:25, 50:15, 50:19, 51:4, 53:15, 54:4, 54:10, 55:6, 55:13, 55:17, 55:19, 58:16, 58:20, 59:29, 60:27, 61:27, 63:3, 64:20, 76:25, 83:26, 84:24, 86:2, 95:4, 95:8, 95:27, 99:13, 99:28, 105:4, 116:1, 116:9, 116:19, 116:24, 126:8, 126:11, 126:14, 158:12, 203:28

departments [5] - 70:19, 101:16, 120:18, 148:27, 208:18

Departments [1] - 99:17

deployed [1] - 200:14

derived [3] - 151:6, 180:28, 181:17

derogations [2] - 100:20, 100:21

describe [3] - 61:26, 94:13, 145:7

described [10] - 65:6, 101:4, 102:14, 102:26, 132:17, 147:27, 154:19, 157:13, 201:13, 225:7

described' [1] - 210:11

describes [9] - 14:15, 64:22, 70:23, 74:28, 100:14, 129:7, 223:13, 223:25, 226:24

describing [3] - 9:28, 130:3, 130:9

description [5] - 27:12, 39:5, 81:27, 169:21, 190:17

deserved [1] - 91:1

design [1] - 136:27

designate [1] - 99:12

designated [16] - 56:29, 58:4, 61:27, 98:19, 111:28, 197:19, 199:4, 200:21, 200:23, 201:3, 201:12, 201:19, 202:3, 202:9, 202:22, 203:19

designation [4] - 76:23, 125:20, 126:23, 202:13

designations [2] - 118:5, 118:8

designed [3] - 33:22, 68:24, 215:29

despite [5] - 141:11, 146:25, 181:20, 230:22, 232:9

destination [4] - 167:5, 167:6, 167:7, 167:8

destruction [2] - 141:5, 147:12

detail [18] - 16:26, 33:29, 34:19, 36:20, 41:29, 50:24, 61:1, 73:20, 77:9, 77:21, 78:16, 87:14, 93:27, 110:12, 110:15, 140:25, 224:18, 225:8

detailed [5] - 99:14, 131:28, 167:23, 168:27, 173:18

details [6] - 18:16, 47:29, 72:3, 178:8, 186:17, 187:17

detainees [1] - 156:20

detect [2] - 225:12, 231:1

detecting [2] - 147:4, 202:4

detection [2] - 45:13, 95:25

determination [3] - 198:24, 199:15, 199:19

determination' [1] - 217:28

determinations [1] - 165:19

determine [3] - 17:29, 27:6, 60:8

determined [1] - 110:27

determines [4] - 31:28, 143:22, 149:23, 200:24

determining [2] - 47:7, 146:11

deterrent [1] - 178:2

developed [4] - 48:29, 56:21, 222:19, 225:14

development [1] - 147:11

developments [3] - 94:16, 125:18, 218:15

devices [3] - 43:19, 191:24, 192:27

devote [1] - 99:6

dictate [1] - 134:9

dictionary [1] - 205:22

Diego [1] - 185:17

difference [4] - 15:7, 75:19, 183:14, 204:24

difference(s [1] - 187:1

differences [3] - 75:21, 125:3, 218:3

different [16] - 8:26, 15:3, 15:29, 17:3, 18:12, 23:1, 25:17, 51:13, 78:12, 93:14, 123:26, 154:7, 154:10, 163:12, 190:3, 191:3

differently [2] - 26:10, 79:11

difficult [9] - 20:3, 27:13, 29:16, 30:9, 150:22, 178:28, 183:5, 183:23, 216:15

difficulties [3] - 31:8, 152:29, 232:9

difficulty [4] - 20:4, 33:12, 232:16, 232:19

digital [1] - 53:1

DIGITAL [1] - 2:29

Digital [1] - 110:25

dignity [2] - 67:25, 146:15

dimension [1] - 123:8

Diplomacy [1] - 98:21

diplomatic [1] - 146:13

direct [7] - 36:15, 57:20, 65:18, 114:27, 120:17, 135:1, 161:19

directed [9] - 19:20, 98:29, 99:6, 100:7, 122:11, 131:11, 132:8, 134:29, 147:6

direction [1] - 136:20

directions [1] - 66:16

directive [8] - 37:27, 66:11, 130:5, 145:13, 145:24, 148:20, 161:25, 171:13

Directive [16] - 34:16, 37:25, 40:9, 43:4, 44:6, 44:13, 46:9, 48:18, 49:21, 63:7, 65:24, 88:19, 93:15, 130:4, 140:24, 223:17

Directive] [1] - 86:5

Directives [5] - 19:22, 65:20, 102:25, 103:4, 117:23

directives [5] - 72:6, 140:21, 157:11, 161:24, 161:29

directly [16] - 56:26, 58:2, 61:11, 99:4, 99:20, 102:4, 104:2, 109:8, 113:14, 121:16, 138:4, 139:6, 144:17, 177:23, 187:14, 202:23

Director [5] - 14:22, 43:2, 70:8, 74:20, 102:27

director [1] - 14:24

directs [1] - 121:8

disadvantaging [1] - 146:3

disagree [14] - 6:18, 24:13, 30:15, 30:29, 31:25, 123:11, 160:8, 160:29, 162:27, 165:5, 166:9, 173:3, 174:12, 182:26

disagreed [1] - 8:15

disagreeing [1] - 12:8

14

15

223:21, 230:14

**efficiency** [1] - 109:3

**effort** [1] - 173:14

**efforts** [4] - 13:23, 60:29, 194:29, 225:13

**eight** [1] - 181:18

**either** [18] - 17:20, 32:12, 56:14, 58:3, 59:20, 60:14, 62:17, 74:24, 77:18, 137:12, 141:12, 150:20, 151:10, 156:16, 165:16, 199:3, 208:6, 216:8

**elaborates** [1] - 220:28

**electronic** [34] - 5:22, 9:6, 9:18, 19:19, 22:11, 73:4, 74:10, 130:1, 131:26, 132:5, 132:8, 141:24, 142:4, 142:9, 142:12, 142:17, 145:16, 163:23, 168:2, 171:14, 181:25, 190:24, 191:14, 193:11, 193:12, 194:2, 194:6, 204:16, 205:2, 205:11, 205:12, 205:14, 222:11, 222:13

**ELECTRONIC** [1] - 3:1

**Electronic** [8] - 43:18, 73:19, 85:17, 85:19, 140:18, 204:12, 204:15, 223:16

**element** [7] - 6:27, 15:13, 26:8, 34:11, 70:23, 80:24, 231:12

**elements** [13] - 15:12, 16:4, 22:22, 24:18, 25:21, 26:3, 27:11, 50:29, 72:24, 78:12, 109:10, 151:16, 151:24

**eliminated** [1] - 131:12

**else'** [1] - 162:22

**elsewhere** [2] - 163:19, 169:2

**emails** [1] - 7:1

**embroil** [1] - 123:7

**eminently** [1] - 31:29

**emphasis** [1] - 141:3

**emphasise** [1] - 220:19

**emphasises** [1] - 181:15

**emphasize** [1] - 230:27

**emphasizing** [1] - 183:29

**employ** [4] - 120:18, 121:8, 171:11, 171:17

**employed** [1] - 69:3

**employee** [1] - 205:29

**employees** [4] - 191:13, 191:19, 205:23, 227:8

**employment** [2] - 52:15, 62:19

**empowered** [2] - 131:20, 157:27

**enable** [1] - 86:11

**enables** [1] - 198:29

**enabling** [1] - 45:13

**enacted** [11] - 6:22, 19:26, 37:28, 124:6, 131:16, 131:24, 132:21, 156:2, 167:19, 200:8, 201:10

**enactment** [3] - 167:15, 173:10, 197:6

**encompass** [1] - 17:17

**encrypted** [5] - 137:10, 140:2, 140:5, 143:17, 149:21

**encryption** [2] - 140:8, 223:28

**end** [13] - 43:9, 53:13, 61:10, 70:25, 75:27, 76:11, 86:24, 88:25, 95:12, 120:15, 166:19, 167:11, 167:18

**energetic** [1] - 173:14

**enforce** [5] - 45:11, 61:16, 120:19, 158:19, 181:9

**enforceable** [1] - 55:17

**enforced** [1] - 96:28

**enforcement** [37] - 42:16, 43:14, 43:16, 45:20, 46:21, 50:18, 53:14, 53:28, 55:13, 55:14, 55:23, 57:6, 59:21, 59:24, 60:16, 61:5, 63:25, 64:1, 64:7, 64:24, 68:6, 83:23, 84:12, 84:25, 88:10, 96:21, 119:22, 168:1, 195:1, 196:2, 197:12, 197:16, 200:29, 208:12,

208:13, 211:12, 227:24

**Enforcement** [4] - 53:4, 55:26, 56:7, 126:16

**engage** [4] - 67:17, 119:29, 130:27, 142:3

**engaged** [5] - 42:10, 62:10, 134:21, 188:16, 194:29

**enhancements** [1] - 40:28

**enhancing** [1] - 118:14

**enjoin** [1] - 196:17

**enormous** [1] - 122:18

**ensuing** [1] - 88:11

**Ensure** [2] - 120:24, 121:3

**ensure** [23] - 19:15, 44:25, 53:6, 53:16, 58:8, 59:10, 61:7, 63:4, 66:18, 77:3, 78:25, 80:7, 81:19, 82:13, 86:3, 95:26, 99:20, 101:4, 101:17, 121:9, 121:22, 122:12, 225:15

**ensured** [2] - 94:6, 95:23

**ensures** [9] - 40:10, 49:2, 69:2, 78:24, 79:3, 82:18, 83:4, 85:25, 102:6

**ensuring** [2] - 47:5, 65:8

**entail** [1] - 229:16

**enter** [2] - 119:25, 201:25

**entered** [3] - 7:7, 21:8, 48:10

**entering** [1] - 201:19

**entire** [5] - 66:12, 153:19, 166:1, 179:18, 231:10

**entirely** [2] - 10:29, 158:12

**entirety** [1] - 118:24

**entities** [8] - 186:22, 189:23, 207:5, 207:8, 207:13, 207:15, 207:17, 207:21

**entitled** [6] - 10:11, 20:17, 73:27, 125:3, 155:23, 203:4

**entity** [5] - 202:2, 202:8, 202:10, 202:23, 202:25

**entrusted** [1] - 71:8

**entry** [1] - 94:18

**enunciated** [1] - 78:4

**envisaging** [1] - 229:28

**EO** [22] - 29:14, 74:13, 130:15, 141:14, 142:22, 142:26, 143:5, 143:11, 144:5, 144:16, 145:1, 145:17, 149:7, 150:2, 156:17, 163:10, 163:22, 164:8, 164:22, 164:25, 166:15, 166:17

**Equal** [1] - 52:18

**equally** [2] - 74:12, 90:14

**equitable** [1] - 62:5

**equivalence'** [2] - 228:8, 228:23

**equivalent** [5] - 7:16, 63:6, 84:26, 86:4, 95:19

**equivalent'** [1] - 228:15

**erasure** [5] - 86:15, 86:21, 86:27, 86:29, 87:12

**especially** [4] - 24:28, 30:19, 30:23, 31:13

**espionage** [2] - 141:4, 147:6

**essence** [1] - 34:18

**essential** [4] - 20:7, 106:13, 178:3, 220:11

**essentially** [7] - 63:6, 63:16, 72:26, 86:4, 91:9, 95:19, 216:10

**establish** [20] - 7:27, 8:2, 9:10, 16:21, 23:15, 24:20, 26:5, 29:16, 30:10, 75:4, 76:2, 150:22, 151:13, 151:24, 152:1, 156:15, 183:6, 183:24, 213:16, 214:19

**established** [11] - 20:6, 32:13, 46:8, 59:9, 98:24, 100:21, 112:1, 132:12, 202:11, 202:25, 214:1

**establishes** [1] - 16:3

**establishing** [4] - 20:2, 31:8, 153:1, 216:26

**entry** [1] - 94:18

**estimate** [1] - 126:19

**etc** [2] - 69:21, 217:28

**etc.')** [1] - 148:4

**ethnicity** [1] - 146:4

**EU** [144] - 29:22, 31:28, 32:27, 33:1, 33:5, 33:13, 33:25, 34:8, 35:1, 35:13, 35:22, 37:29, 38:26, 39:11, 40:12, 40:15, 41:12, 41:22, 42:20, 43:28, 44:23, 45:2, 45:4, 46:23, 46:26, 46:29, 47:5, 47:22, 47:24, 49:3, 49:16, 53:7, 54:3, 55:25, 55:29, 56:16, 57:19, 58:26, 58:28, 58:29, 61:22, 63:14, 64:5, 64:29, 66:26, 67:4, 67:5, 68:27, 70:1, 72:21, 73:14, 74:8, 76:10, 76:18, 79:8, 79:18, 79:26, 83:8, 84:20, 85:22, 85:28, 93:1, 94:7, 94:21, 95:6, 96:4, 96:24, 96:27, 98:12, 98:13, 98:14, 100:17, 101:5, 101:29, 102:3, 102:5, 102:10, 102:17, 102:21, 103:21, 104:2, 104:10, 108:2, 108:5, 108:13, 109:17, 125:20, 163:7, 163:8, 164:12, 166:23, 180:5, 186:21, 186:24, 187:2, 187:8, 189:21, 190:21, 192:12, 193:2, 197:7, 197:12, 197:13, 212:15, 215:20, 216:8, 216:25, 217:16, 217:18, 217:20, 217:22, 217:24, 218:3, 218:6, 223:14, 223:16, 223:19, 224:10, 224:17, 226:13, 226:22, 226:25, 226:28, 227:13, 227:27, 228:11, 228:13, 228:15, 228:19, 228:22, 229:3, 229:7, 229:10, 229:26, 230:2, 230:14, 230:15, 230:23, 230:26, 230:28,

16

231:19, 231:24

**EU-U.S** [7] - 41:22, 44:23, 46:23, 47:5, 47:24, 49:3, 64:5

**EU-US** [26] - 38:26, 39:11, 40:12, 40:15, 41:12, 42:20, 43:28, 47:22, 54:3, 55:25, 63:14, 64:29, 66:26, 67:5, 68:27, 83:8, 85:22, 85:28, 94:7, 95:6, 96:4, 98:12, 104:10, 108:2, 108:5, 109:17

**EU/US** [3] - 223:18, 229:23, 230:29

**EUROPE** [1] - 2:29

**Europe** [2] - 94:21, 110:8

**European** [29] - 37:16, 38:6, 38:13, 48:15, 67:16, 67:19, 69:21, 75:18, 89:21, 90:10, 90:20, 91:2, 104:11, 106:1, 108:1, 110:17, 111:2, 117:8, 117:9, 117:13, 126:23, 144:20, 157:1, 163:5, 172:27, 190:9, 228:6, 231:9

**evaluate** [1] - 45:28

**evaluated** [1] - 165:14

**evaluating** [3] - 11:11, 123:20, 155:19

**evaluation** [2] - 37:4, 109:10

**evasion** [1] - 147:17

**event** [8] - 32:12, 82:6, 84:13, 94:9, 102:28, 157:14, 179:6, 227:7

**events** [1] - 93:10

**eventually** [2] - 86:14, 151:24

**evidence** [36] - 12:16, 15:16, 15:19, 16:4, 23:15, 26:6, 26:25, 29:10, 47:21, 59:14, 123:2, 123:9, 123:10, 128:16, 151:25, 161:24, 172:10, 172:26, 173:27, 179:19, 180:20, 180:27, 181:10, 181:17, 181:24, 181:25, 182:14, 182:15, 185:6, 187:15, 187:22, 194:2, 194:3,

194:5, 221:2

**evidence'** [1] - 8:3

**evidentiary** [6] - 7:10, 8:6, 15:29, 212:5, 212:7, 212:13

**evolve** [1] - 218:12

**ex** [1] - 95:8

**exact** [1] - 28:19

**exactly** [10] - 31:16, 36:18, 87:10, 87:27, 92:29, 93:19, 106:26, 110:13, 122:19, 124:28

**examination** [1] - 222:26

**examine** [2] - 227:6, 227:23

**examining** [4] - 18:5, 140:3, 158:1, 203:24

**example** [19] - 9:16, 9:29, 11:2, 25:29, 33:18, 36:14, 42:13, 78:4, 87:13, 144:8, 145:2, 149:13, 149:21, 174:11, 195:28, 202:10, 203:18, 208:2, 215:27

**examples** [2] - 20:1, 190:1

**exceed** [1] - 104:19

**exceeding** [1] - 208:21

**exceedingly** [4] - 29:16, 150:22, 183:5, 183:23

**exceeds** [2] - 13:29, 205:16

**excellent** [1] - 38:15

**except** [4] - 191:13, 191:19, 191:23, 229:10

**Except** [2] - 57:10, 210:6

**exception** [6] - 50:6, 135:20, 151:3, 163:17, 166:28, 180:17

**exceptionally** [1] - 69:7

**exceptions** [9] - 136:27, 160:15, 161:1, 175:22, 195:28, 196:6, 205:4, 210:29, 217:19

**excessive** [1] - 52:5

**exclude** [5] - 89:27, 121:23, 122:13, 182:14, 194:5

**excluded** [1] - 180:23

**excludes** [2] - 148:4, 174:25

**excluding** [1] - 181:9

**exclusionary** [1] - 194:1

**Exclusionary** [1] - 180:13

**exclusive** [2] - 189:20, 204:7

**execution** [2] - 120:24, 121:9

**Executive** [40] - 65:10, 65:20, 65:23, 66:12, 102:24, 106:6, 117:22, 118:2, 118:12, 118:21, 118:24, 119:3, 119:19, 121:29, 122:8, 123:24, 123:27, 123:28, 125:22, 125:26, 125:27, 126:4, 126:20, 126:25, 129:12, 129:29, 130:10, 130:21, 140:11, 140:12, 143:29, 148:24, 154:20, 163:2, 163:25, 164:17, 166:22, 175:21, 194:25, 195:21

**executive** [17] - 70:6, 71:6, 114:13, 115:12, 115:22, 117:27, 120:17, 120:21, 134:11, 143:6, 145:13, 157:2, 157:11, 157:25, 158:7, 173:8, 195:22

**executive-branch** [2] - 145:13, 157:25

**exempt** [6] - 194:18, 194:20, 194:27, 195:19, 196:28, 208:4

**exempted** [2] - 195:15, 208:5

**exemption** [5] - 194:22, 195:4, 195:5, 195:10, 199:27

**exemptions** [5] - 195:2, 195:13, 200:9, 208:2, 215:29

**exempts** [3] - 194:24, 208:5, 208:11

**exercise** [4] - 44:12, 71:2, 109:28, 187:13

**exercising** [1] - 49:17

**exhausted** [1] - 57:11

**exhibit** [2] - 168:29, 169:1

**exhibits** [3] - 128:29, 129:26, 159:3

**exist** [6] - 67:3, 69:27, 70:19, 74:15, 214:10, 230:21

**existed** [1] - 167:17

**existence** [4] - 74:24, 75:4, 76:2, 161:4

**existing** [10] - 30:22, 37:18, 50:9, 74:2, 80:11, 142:6, 169:23, 199:24, 199:29, 215:29

**exists** [3] - 65:22, 88:15, 160:9

**expand** [1] - 175:1

**expanded** [2] - 127:1, 208:18

**expected** [1] - 108:21

**expeditiously** [1] - 56:10

**experience** [5] - 223:14, 223:26, 224:20, 224:24, 228:11

**experiences** [2] - 224:12, 224:13

**expert** [15] - 28:7, 29:1, 125:19, 128:10, 129:14, 159:16, 166:27, 185:27, 186:10, 186:19, 187:16, 187:27, 188:12, 219:27, 221:5

**expert's** [2] - 27:26, 167:1

**expertise** [8] - 79:4, 82:22, 128:28, 185:18, 188:14, 222:19, 224:17, 224:22

**experts** [50] - 21:2, 21:22, 21:28, 24:9, 24:12, 24:15, 30:1, 30:7, 30:13, 32:18, 112:5, 112:18, 117:3, 122:29, 123:2, 123:6, 123:10, 123:22, 124:13, 124:18, 124:25, 126:28, 127:3, 128:11, 128:21, 159:7, 159:10, 160:8, 160:29, 162:27, 165:5, 166:7, 167:9, 169:7, 169:10,

169:13, 170:24, 171:4, 171:15, 171:29, 173:3, 173:16, 174:12, 175:7, 176:3, 177:22, 179:2, 180:8, 182:18, 182:23

**experts'** [2] - 112:13, 125:15

**experts'** [1] - 162:5

**expiration** [1] - 96:2

**explain** [5] - 93:21, 100:10, 125:2, 125:3, 168:22

**explained** [8] - 10:13, 22:14, 70:17, 70:22, 88:20, 93:26, 103:27, 142:5

**explains** [3] - 39:28, 100:9, 129:1

**explanation** [1] - 59:19

**explanations** [1] - 74:23

**explicit** [1] - 67:16

**explicitly** [4] - 11:26, 12:4, 126:22, 148:4

**exploitation** [1] - 114:1

**exposes** [1] - 135:28

**express** [3] - 51:16, 103:9, 116:28

**expressed** [4] - 107:17, 107:20, 108:6, 116:27

**expressly** [6] - 37:1, 37:3, 90:16, 124:6, 175:7, 203:2

**extend** [5] - 84:6, 124:6, 124:11, 147:25, 216:4

**extended** [1] - 72:2

**extending** [3] - 122:6, 122:24, 199:22

**extends** [1] - 197:17

**extensive** [5] - 71:25, 160:20, 224:19, 229:7, 230:22

**extent** [24] - 11:5, 15:7, 28:19, 53:27, 63:28, 81:13, 93:10, 103:8, 121:21, 122:9, 122:11, 123:16, 124:9, 124:14, 135:12, 162:27, 173:15, 177:19, 184:26, 187:2, 187:29, 195:20, 195:26, 197:23

**external** [1] - 160:23

17

18

196:3, 208:4, 208:11

**follow** [4] - 57:15, 57:16, 70:29, 100:15

**follow-up** [1] - 70:29

**followed** [2] - 25:18, 43:16

**following** [10] - 1:23, 13:8, 24:16, 30:13, 94:4, 94:18, 145:29, 191:8, 197:25, 228:23

**follows** [3] - 63:27, 66:22, 112:9

**FOLLOWS** [2] - 5:1, 128:2

**Foods** [1] - 205:28

**foot** [1] - 81:8

**footnote** [14] - 52:18, 68:7, 74:19, 75:9, 75:24, 75:27, 137:17, 148:26, 150:26, 192:20, 205:18, 206:26, 207:10, 210:29

**FOR** [4] - 2:19, 2:25, 2:29, 3:1

**force** [9] - 8:25, 25:5, 37:3, 37:29, 38:1, 93:12, 93:13, 94:23, 107:27

**forces** [1] - 147:14

**forcing** [1] - 18:23

**foreclose** [1] - 31:17

**foreclosed** [1] - 216:3

**Foreign** [13] - 5:23, 14:1, 20:13, 20:25, 23:21, 66:28, 73:2, 131:19, 169:22, 190:22, 190:23, 226:14, 227:10

**foreign** [71] - 10:4, 10:6, 11:1, 11:3, 25:14, 25:16, 27:17, 34:24, 65:11, 65:12, 68:6, 68:16, 68:17, 68:20, 69:4, 76:25, 98:22, 131:17, 131:21, 132:6, 132:9, 132:10, 133:22, 134:21, 134:25, 137:10, 139:13, 140:13, 141:9, 143:18, 146:6, 147:7, 149:15, 149:22, 150:28, 156:7, 159:20, 159:28, 164:23, 165:3, 165:6, 167:3, 167:5, 170:22, 176:14, 176:16, 178:6, 183:21,

190:26, 190:28, 191:15, 191:25, 193:10, 194:26, 195:24, 202:7, 202:24, 203:18, 208:24, 223:29, 225:10, 225:22, 225:26, 226:9, 226:10, 226:12, 226:19, 229:24

**foreign-intelligence** [5] - 10:4, 11:1, 143:18, 149:22, 150:28

**foreign-relations** [1] - 25:16

**Forester** [2] - 185:17, 186:4

**forget** [4] - 10:24, 10:25, 37:24, 169:3

**form** [22] - 34:29, 42:17, 47:29, 51:21, 51:22, 54:15, 55:12, 91:9, 107:20, 110:18, 119:4, 129:26, 129:27, 133:2, 135:13, 139:14, 140:16, 143:17, 156:1, 169:23, 187:8, 232:10

**formal** [2] - 45:2, 210:18

**formally** [1] - 232:18

**format** [1] - 27:22

**former** [3] - 138:23, 141:16, 164:24

**forms** [5] - 34:22, 35:28, 142:1, 143:5, 220:4

**forms..** [1] - 98:18

**formulate** [1] - 7:2

**formulated** [1] - 47:25

**forth** [13] - 14:10, 14:16, 26:24, 34:25, 43:8, 43:20, 75:1, 85:18, 110:2, 164:4, 190:18, 195:12, 201:1

**forth'** [1] - 15:19

**forum** [1] - 223:21

**forward** [3] - 6:10, 222:12, 222:15

**forwarded** [1] - 167:8

**foundation** [1] - 185:8

**Foundation** [2] - 13:17, 193:25

**founded** [1] - 89:6

**four** [4] - 11:14,

11:25, 197:29, 219:17

**Fourteenth** [1] - 214:6

**fourth** [1] - 60:27

**Fourth** [22] - 5:24, 13:3, 13:28, 19:17, 84:2, 84:6, 84:19, 154:5, 154:13, 155:3, 155:6, 155:15, 157:29, 176:9, 176:11, 176:18, 176:22, 177:2, 177:4, 177:10, 177:15, 177:20

**Fox** [1] - 203:28

**Foxx** [1] - 42:26

**fraction** [2] - 160:4, 172:27

**framework** [6] - 41:13, 42:20, 65:5, 83:18, 132:12, 226:10

**Fraud** [3] - 73:18, 208:15, 208:16

**fraud** [1] - 208:27

**fraudulent** [1] - 62:27

**free** [8] - 13:3, 13:6, 57:12, 81:23, 82:15, 82:24, 99:22, 227:15

**Freedom** [13] - 72:4, 72:29, 80:14, 85:17, 103:28, 104:17, 129:10, 155:29, 156:1, 173:11, 194:23, 207:25, 207:27

**FREEDOM** [1] - 19:26

**French** [1] - 110:20

**FRIDAY** [1] - 232:23

**friendly** [1] - 60:6

**Friends** [2] - 123:15, 232:11

**frivolous)** [1] - 58:6

**from'** [1] - 181:18

**FRY** [1] - 2:26

**FTC** [8] - 53:15, 55:13, 57:1, 59:21, 59:25, 61:10, 63:20, 63:25

**fulfillment** [1] - 104:20

**fulfilment** [1] - 45:6

**full** [7] - 39:4, 111:7, 188:26, 220:1, 220:21, 220:22, 229:1

**fully** [2] - 12:17, 125:2

**function** [4] - 71:2, 82:14, 99:1, 99:21

**functional** [1] - 176:18

**functioning** [3] - 44:23, 47:5, 95:6

**functions** [8] - 63:21, 63:22, 70:14, 71:24, 80:8, 82:24, 104:19, 195:17

**Fundamental** [1] - 190:9

**fundamental** [8] - 68:25, 69:15, 75:5, 76:3, 83:6, 88:7, 89:5, 225:23

**fundamentally** [2] - 17:3, 91:7

**furnished** [1] - 185:22

**Furthermore** [4] - 71:4, 189:8, 195:18, 209:3

**furthers** [1] - 208:27

**future** [10] - 6:23, 26:9, 26:13, 26:21, 32:11, 34:25, 100:21, 216:29, 217:3, 218:14

## G

**g)(1)(A)-(C** [1] - 198:14

**gain** [2] - 86:13, 199:1

**gained** [4] - 38:2, 181:25, 194:2, 194:6

**Gallagher** [10] - 17:16, 17:18, 40:5, 90:11, 93:20, 179:22, 219:16, 220:8, 220:18, 222:13

**GALLAGHER** [23] - 2:9, 40:2, 75:10, 75:12, 75:20, 97:27, 106:16, 106:26, 107:7, 107:9, 119:4, 119:12, 122:25, 124:16, 179:17, 219:14, 220:23, 221:29, 222:3, 222:10, 232:8, 232:17, 232:20

**Gallagher's** [2] - 17:20, 75:14

**gather** [1] - 141:1

**gathered** [5] - 22:10, 47:21, 156:6, 216:13, 218:8

**gathering** [6] - 13:23, 25:14, 25:15,

43:8, 189:24, 190:26

**gathers** [1] - 140:13

**GDPR** [5] - 38:21, 94:19, 94:20, 94:23, 94:26

**gender** [1] - 146:4

**general** [23] - 19:14, 25:18, 30:19, 31:11, 31:27, 34:5, 37:23, 42:22, 55:10, 59:16, 66:15, 73:25, 104:10, 108:17, 111:9, 111:10, 111:11, 134:2, 158:9, 165:15, 166:29, 170:15, 203:1

**General** [20] - 37:27, 38:20, 43:1, 43:12, 68:1, 70:23, 70:27, 105:2, 115:6, 115:11, 115:17, 115:21, 115:23, 126:23, 140:23, 158:4, 158:6, 200:23, 227:25, 230:18

**generalised** [2] - 66:20, 69:19

**generality** [1] - 134:10

**generalized** [3] - 139:20, 142:11, 162:16

**generally** [10] - 22:14, 34:4, 131:24, 143:14, 149:19, 150:27, 155:3, 163:16, 190:27, 227:26

**Generals** [3] - 70:8, 78:23, 80:18

**genuinely** [1] - 122:26

**German** [1] - 129:15

**Gibson** [1] - 221:2

**GILMORE** [1] - 3:2

**given** [18] - 22:1, 45:4, 52:28, 67:16, 68:12, 75:14, 81:27, 82:1, 84:11, 87:14, 104:14, 105:29, 121:11, 128:15, 172:14, 185:12, 205:25, 218:10

**Given** [1] - 137:27

**global** [3] - 142:20, 172:27, 186:5

**goal** [1] - 140:29

**GOODBODY** [1] - 2:31

**Google** [3] - 138:5, 144:12, 161:20

19

20

21

22

*Gwen Malone Stenography Services Ltd.*

24

140:14

**latter** [2] - 49:16, 84:10

**law** [99] - 5:13, 32:9, 33:1, 37:14, 38:13, 43:14, 43:16, 45:20, 46:21, 48:3, 48:27, 52:15, 53:28, 62:25, 62:26, 63:25, 64:1, 64:4, 64:7, 64:23, 64:27, 68:6, 69:2, 72:21, 72:25, 78:20, 80:11, 80:16, 82:4, 83:23, 84:12, 84:25, 88:10, 89:7, 94:16, 96:21, 101:8, 102:24, 104:27, 105:27, 105:28, 120:4, 121:22, 122:9, 124:10, 125:6, 125:7, 125:18, 130:7, 131:7, 152:7, 156:3, 157:10, 165:13, 167:14, 168:1, 185:2, 185:15, 186:11, 186:20, 187:8, 188:7, 189:22, 190:2, 193:14, 196:2, 197:12, 197:16, 200:29, 204:15, 208:11, 208:13, 208:16, 208:17, 210:7, 211:12, 218:18, 218:21, 220:15, 223:14, 223:26, 223:28, 223:29, 224:1, 224:10, 224:11, 224:17, 224:23, 224:24, 225:5, 225:23, 225:25, 227:23, 228:10, 228:11, 228:16, 228:27, 231:18

**Law** [1] - 129:3

**LAW** [1] - 190:21

**law'** [2] - 11:23, 87:16

**lawful** [15] - 33:1, 92:8, 92:9, 92:11, 92:13, 93:15, 120:18, 121:9, 121:24, 149:15, 191:13, 191:19, 193:1, 197:18, 229:14

**lawfully** [3] - 32:26, 33:13, 122:14

**Lawfulness** [1] - 165:9

**lawfulness** [6] - 129:9, 130:18,

150:16, 153:8, 154:22, 165:14

**laws** [17] - 77:5, 77:6, 77:18, 77:20, 78:2, 100:22, 102:19, 103:3, 119:22, 120:19, 120:24, 121:10, 158:10, 190:4, 195:1, 226:13, 227:9

**lawsuit** [9] - 22:9, 25:24, 129:11, 153:10, 154:20, 196:9, 212:2, 212:16, 217:14

**lawsuits** [2] - 24:29, 31:22

**lawyer** [1] - 186:6

**lawyers** [2] - 122:17, 188:29

**layers** [1] - 70:7

**lead** [6] - 59:24, 60:3, 129:10, 170:21, 222:24, 223:15

**Leadership** [1] - 222:29

**leading** [3] - 44:13, 96:7, 97:6

**leaked** [1] - 9:14

**learn** [2] - 158:16, 178:8

**least** [16] - 34:9, 35:28, 74:12, 82:20, 84:14, 84:20, 84:27, 111:21, 133:9, 137:25, 138:10, 142:1, 144:11, 213:15, 220:16, 228:15

**leave** [6] - 32:21, 128:14, 208:8, 220:19, 231:29, 232:2

**leaving** [1] - 90:25

**led** [3] - 157:2, 170:6, 226:6

**Lee** [1] - 187:24

**LEE** [1] - 2:6

**left** [1] - 6:11

**left-hand** [1] - 6:11

**legal** [46] - 10:2, 12:12, 15:2, 15:3, 22:21, 45:23, 62:14, 62:26, 65:5, 65:23, 67:2, 69:24, 73:15, 73:27, 74:12, 83:5, 83:14, 86:13, 86:18, 88:4, 88:15, 89:7, 94:3, 105:20, 105:21, 123:14, 123:17, 126:3, 126:20,

126:25, 129:11, 135:25, 152:12, 157:4, 157:27, 167:16, 167:23, 167:28, 182:9, 184:2, 189:1, 197:24, 218:18, 226:10, 226:16, 228:7

**legality** [2] - 182:10, 182:21

**legally** [2] - 94:8, 113:16

**legislation** [9] - 10:10, 14:14, 43:17, 50:1, 50:2, 69:14, 80:26, 85:15, 196:7

**legislative** [1] - 226:2

**legitimate** [5] - 68:29, 69:5, 88:14, 146:17, 211:12

**lending** [1] - 52:14

**length** [1] - 219:20

**less** [7] - 167:29, 191:28, 193:15, 198:18, 206:9, 229:7, 230:22

**letter** [17] - 40:23, 40:26, 41:21, 42:1, 42:5, 42:25, 43:1, 43:11, 64:10, 76:20, 97:24, 98:6, 98:7, 102:27, 103:2, 157:13, 224:6

**Letter** [1] - 67:2

**letters** [2] - 34:22, 35:18

**level** [28] - 23:1, 40:10, 44:25, 49:2, 52:1, 53:24, 59:10, 63:5, 76:24, 83:29, 85:21, 85:26, 86:3, 87:14, 94:2, 94:6, 94:17, 94:21, 95:18, 95:26, 96:5, 97:11, 102:3, 102:4, 114:20, 115:1, 134:9, 163:27

**Liability** [3] - 53:4, 55:26, 56:7

**liable** [8] - 82:15, 94:3, 99:23, 193:21, 207:5, 207:15, 207:17, 207:21

**liberties** [2] - 70:17, 71:11

**Liberties** [10] - 70:9, 70:11, 71:4, 101:19, 105:2, 105:3, 115:6, 129:6, 158:5, 227:14

**liberties)** [1] - 84:29

**Liberty** [1] - 10:26

**light** [12] - 29:27, 63:1, 82:28, 85:24, 88:20, 90:7, 94:2, 203:17, 214:21, 215:1, 216:23, 231:18

**lighter** [1] - 7:14

**likelihood** [9] - 7:29, 8:13, 18:26, 139:27, 151:19, 172:13, 172:28, 182:26, 213:18

**likelihood'** [2] - 7:26, 29:11

**likely** [13] - 29:27, 52:12, 143:1, 167:6, 172:19, 189:26, 192:7, 212:6, 215:13, 215:22, 216:14, 218:4, 218:9

**Likewise** [1] - 12:7

**limit** [9] - 68:24, 84:25, 174:18, 175:7, 175:28, 190:13, 200:15, 203:10, 206:28

**Limitation** [2] - 51:8, 51:20

**limitation** [1] - 192:12

**limitations** [26] - 43:7, 46:20, 64:3, 64:22, 64:27, 65:16, 65:29, 72:24, 82:5, 83:27, 96:20, 102:26, 140:16, 147:24, 157:12, 173:20, 174:16, 174:21, 175:12, 186:28, 190:2, 197:24, 199:25, 199:29, 200:4, 215:25

**limited** [16] - 8:6, 11:14, 11:25, 51:9, 53:22, 53:27, 63:28, 68:3, 69:17, 74:17, 85:10, 88:13, 97:15, 133:2, 157:5, 171:24

**limiting** [2] - 46:14, 96:10

**limits** [7] - 174:19, 175:8, 175:19, 176:3, 176:5, 179:12, 195:26

**line** [2] - 48:12, 132:2

**lines** [1] - 135:4

**linking** [2] - 172:11, 172:26

**links** [2] - 51:3, 110:2

**liquidated** [1] - 193:15

**List** [1] - 44:16

**list** [12] - 26:18, 35:27, 41:15, 41:18, 54:5, 54:8, 54:11, 55:5, 55:7, 60:4, 60:19, 195:14

**list'** [1] - 44:2

**listed** [2] - 40:19, 198:13

**lists** [3] - 118:19, 145:3, 145:5

**litigant** [3] - 178:18, 179:3, 216:25

**litigate** [1] - 151:9

**litigated** [1] - 165:17

**litigating** [1] - 129:8

**litigation** [12] - 12:7, 15:17, 26:22, 32:4, 130:19, 150:3, 154:9, 173:8, 182:8, 185:12, 191:29, 206:11

**Litt** [1] - 43:2

**loaned** [1] - 3:9

**local** [3] - 59:5, 60:6, 120:12

**locally** [1] - 79:22

**locate** [1] - 131:3

**located** [12] - 66:25, 131:2, 131:11, 134:24, 135:11, 144:14, 154:29, 155:16, 158:25, 159:19, 177:5, 177:17

**location** [1] - 144:9

**lodge** [1] - 55:29

**logic** [2] - 84:21, 219:5

**logical** [2] - 57:16, 218:27

**logically** [1] - 229:9

**logistical** [1] - 21:13

**long-term** [2] - 139:18, 162:14

**look** [30] - 5:13, 5:18, 15:25, 15:26, 17:15, 38:28, 39:11, 41:28, 47:14, 49:7, 64:16, 81:27, 89:18, 90:14, 90:24, 90:28, 91:18, 103:23, 112:6, 117:7, 117:16, 138:20, 148:26, 159:6, 205:18, 218:19, 219:19, 221:14, 222:12, 232:15

**looked** [9] - 27:22, 34:10, 74:29, 85:16, 99:26, 112:5, 117:28, 179:9, 200:26

**looking** [7] - 34:17,

25

105:19, 107:16, 112:10, 117:10, 222:15, 230:9

**looks** [2] - 106:4, 142:21

**loose** [1] - 107:23

**loosely** [1] - 34:6

**loss** [2] - 209:12, 209:25

**loss'** [1] - 209:18

**low** [4] - 131:3, 135:26, 172:12, 172:28

**lower** [9] - 21:27, 22:7, 27:16, 30:24, 31:16, 165:25, 213:2, 214:13, 214:20

**Lower** [1] - 213:4

**lower-court** [2] - 22:7, 27:16

**lowering** [1] - 97:11

**LTD** [1] - 1:12

**Ltd** [2] - 5:6, 128:7

**lunch** [2] - 107:12, 110:12

**LUNCHEON** [2] - 127:12, 128:1

## M

**magistrate** [1] - 85:7

**mail** [17] - 9:9, 10:5, 10:14, 11:2, 17:21, 17:28, 135:4, 139:15, 142:28, 145:4, 167:3, 167:7, 167:8, 169:17, 205:3, 228:29

**mails** [7] - 5:26, 6:7, 12:24, 17:15, 17:18, 17:19, 205:23

**maintain** [3] - 41:14, 199:13, 217:26

**maintained** [3] - 44:2, 194:28, 195:19

**maintaining** [2] - 29:25, 230:17

**maintains** [2] - 130:26, 155:18

**major** [1] - 135:1

**majority** [5] - 19:12, 150:11, 158:26, 183:3, 183:20

**Malone** [3] - 1:21, 3:8, 3:10

**MALONE** [1] - 1:31

**Management** [1] - 223:4

**mandatory** [1] - 56:19

**manner** [11] - 3:9, 15:15, 53:9, 102:16, 148:28, 186:26, 197:23, 200:2, 200:8, 201:12, 208:8

**Marcus** [2] - 213:22, 213:23

**marked** [1] - 98:5

**marshal** [1] - 29:23

**MARY'S** [1] - 3:4

**Maryland** [1] - 13:19

**Mason** [1] - 221:4

**MASON** [1] - 2:11

**mass** [6] - 108:26, 139:2, 141:4, 147:12, 147:26, 162:24

**material** [4] - 7:9, 9:26, 94:15, 218:4

**materially** [2] - 25:17, 51:13

**materials** [3] - 5:14, 9:14, 11:10

**matter** [29] - 5:5, 10:16, 15:14, 20:24, 37:8, 37:15, 37:21, 41:10, 59:21, 60:12, 64:18, 75:6, 76:4, 81:8, 89:29, 93:13, 105:27, 105:28, 106:22, 118:19, 122:28, 123:3, 153:20, 179:13, 179:28, 180:9, 187:8, 189:7

**matters** [16] - 35:12, 80:21, 101:16, 101:18, 106:9, 122:27, 158:4, 186:11, 188:1, 188:9, 188:13, 189:1, 194:24, 203:12, 208:7, 208:10

**MAURICE** [1] - 2:25

**MAXIMILLIAN** [1] - 1:14

**McCANN** [1] - 2:21

**McCULLOUGH** [1] - 2:14

**McGRANE** [1] - 3:3

**McGRATH** [1] - 3:3

**MCTs** [2] - 169:24, 169:25

**mean** [13] - 9:16, 9:24, 10:1, 11:18, 11:20, 13:4, 39:11, 86:25, 87:8, 89:14, 91:27, 122:19, 221:23

**meaning** [5] - 25:26, 35:21, 89:26, 171:19, 201:29

**meaningful** [7] - 141:12, 141:18, 145:24, 146:26, 157:5, 158:28, 164:26

**meanings** [1] - 123:21

**means** [13] - 16:2, 35:23, 74:2, 78:25, 81:18, 84:17, 120:18, 121:9, 122:10, 162:3, 182:19, 193:20, 200:20

**meant** [3] - 87:1, 118:28, 136:25

**meantime** [1] - 109:24

**measure** [1] - 117:3

**measures** [8] - 18:24, 46:11, 47:3, 51:27, 69:3, 72:13, 95:28, 184:26

**mechanism** [42] - 35:4, 41:23, 41:27, 42:1, 54:3, 54:16, 54:20, 54:28, 55:2, 57:13, 57:14, 58:18, 61:19, 64:12, 76:22, 79:6, 79:12, 82:18, 83:16, 91:3, 91:7, 91:17, 92:7, 93:3, 93:7, 93:11, 94:25, 97:24, 98:13, 98:25, 100:10, 100:14, 100:28, 104:15, 105:27, 106:13, 108:4, 108:23, 109:4, 109:29, 156:9

**Mechanism** [4] - 76:20, 77:2, 78:9, 79:1

**mechanisms** [25] - 33:14, 33:17, 34:27, 35:10, 45:13, 53:6, 55:22, 56:9, 56:14, 57:7, 63:18, 65:1, 69:27, 71:17, 80:10, 91:8, 91:9, 101:3, 101:15, 105:6, 105:21, 123:18, 150:4, 225:28, 225:29

**MECHANISMS** [1] - 155:26

**mechanisms..** [1] - 86:11

**media** [7] - 129:13, 138:2, 138:24, 138:29, 144:16, 144:29, 152:12

**mediation** [1] - 54:27

**meet** [8] - 28:8,

48:17, 53:27, 63:29, 92:8, 201:18, 219:27, 219:28

**meeting** [3] - 21:3, 21:5

**meets** [3] - 88:18, 94:25, 210:19

**member** [4] - 71:6, 129:5, 170:4, 224:1

**Member** [26] - 44:8, 44:12, 44:19, 45:8, 45:17, 45:27, 47:10, 50:3, 59:6, 79:15, 79:23, 88:24, 88:29, 101:25, 110:11, 111:28, 125:20, 126:24, 226:13, 226:22, 226:25, 226:28, 228:14, 229:25, 230:15, 230:23

**members** [4] - 55:7, 109:7, 222:28, 223:9

**memo** [1] - 32:2

**memoranda** [2] - 188:5, 188:8

**memorandum** [19] - 13:21, 14:5, 99:15, 100:14, 102:15, 104:9, 104:12, 186:16, 187:6, 187:19, 188:3, 189:15, 189:17, 189:20, 190:7, 215:23, 218:4, 218:12, 218:23

**Memorandum** [2] - 187:26, 188:1

**Memorandum..** [1] - 188:24

**memory** [1] - 170:3

**mention** [3] - 19:5, 20:11, 21:20

**mentioned** [4] - 5:9, 23:22, 24:7, 42:7

**mentions** [1] - 17:29

**mere** [3] - 8:4, 26:23, 152:1

**merely** [4] - 10:2, 31:10, 153:2, 153:18

**merits** [7] - 8:13, 19:5, 25:5, 29:9, 151:10, 165:19, 165:26

**messaging** [1] - 145:5

**metadata** [3] - 138:4, 139:10, 139:23

**methods** [3] - 84:28, 182:10, 230:2

**Mexican** [2] - 155:13, 155:17

**Mexico** [1] - 155:17

**MICHAEL** [106] - 2:4, 2:29, 4:5, 5:7, 11:20, 21:10, 21:12, 21:16, 21:24, 22:3, 22:5, 27:25, 28:25, 28:27, 29:1, 36:29, 38:9, 38:14, 38:16, 38:19, 39:17, 39:19, 39:22, 39:25, 39:28, 40:4, 40:7, 41:2, 41:7, 57:26, 58:28, 59:4, 75:9, 75:11, 75:16, 75:22, 75:26, 76:7, 78:1, 86:22, 86:27, 87:4, 87:7, 87:21, 87:24, 87:27, 88:1, 91:22, 91:27, 92:3, 93:19, 97:28, 98:4, 106:29, 107:8, 107:11, 107:26, 110:6, 111:2, 111:8, 111:11, 111:14, 111:16, 112:13, 112:16, 117:12, 117:19, 119:2, 119:7, 119:13, 119:18, 123:11, 124:28, 127:9, 128:5, 128:8, 152:22, 154:8, 159:6, 159:15, 169:27, 177:29, 178:16, 179:11, 179:15, 179:21, 182:14, 184:13, 219:3, 219:11, 219:17, 219:25, 220:27, 221:18, 221:21, 221:25, 221:28, 222:8, 222:12, 222:16, 230:7, 232:2, 232:6, 232:14, 232:18, 232:21

**Microsoft** [1] - 138:5

**might** [19] - 17:14, 20:29, 21:1, 24:10, 26:14, 54:19, 77:11, 95:22, 112:6, 127:7, 146:17, 177:4, 178:15, 185:6, 185:9, 192:6, 219:8, 220:15, 231:29

**million** [1] - 136:9

**millions** [5] - 135:3, 137:13, 139:9, 145:3, 181:21

**mind** [2] - 21:12, 109:26

26

**minimisation** [7] - 135:26, 160:12, 160:29, 175:25, 192:18, 217:19, 217:22

**minimise** [1] - 69:9

**minimization** [13] - 19:14, 19:16, 135:14, 136:23, 137:5, 160:13, 160:16, 160:21, 163:27, 175:2, 175:17, 192:28, 193:4

**minimize** [1] - 18:24

**minimized** [1] - 8:25

**minimum** [1] - 215:3

**minute** [1] - 185:9

**mis** [1] - 116:27

**mis-expressed** [1] - 116:27

**misconduct** [1] - 104:27

**misleading** [1] - 55:12

**misplaced** [3] - 8:9, 19:9, 97:26

**misrepresentation** [2] - 55:10, 62:27

**missed** [1] - 106:25

**missions** [1] - 18:23

**misspoke** [2] - 107:1, 124:1

**mistake** [1] - 186:1

**misunderstood** [1] - 91:29

**misuse** [2] - 206:1, 213:13

**misused** [1] - 213:7

**mixed** [3] - 126:9, 127:2, 192:23

**mode** [1] - 17:8

**model** [2] - 41:5, 41:7

**modern** [2] - 53:1, 212:29

**modest** [1] - 130:6

**modifications** [5] - 165:29, 166:2, 166:4, 166:8, 166:10

**modified** [1] - 145:25

**Mohamed** [1] - 153:22

**Mohamud** [1] - 155:8

**moment** [15] - 23:22, 25:24, 36:21, 39:20, 40:22, 64:16, 91:18, 92:13, 99:27, 100:11, 109:3, 117:18, 220:25, 221:13, 231:5

**monetary** [1] - 62:4

**money** [3] - 111:15, 191:8, 206:8

**money/new** [1] - 111:15

**monitor** [4] - 44:23, 45:5, 133:6, 138:7

**monitored** [6] - 6:6, 22:10, 50:15, 53:2, 132:2, 204:17

**monitoring** [7] - 5:25, 55:5, 55:19, 83:19, 94:13, 95:1, 138:10

**months** [1] - 206:18

**moreover** [3] - 71:1, 71:24, 147:24

**Moreover** [11] - 19:26, 66:16, 67:15, 74:14, 79:2, 82:25, 141:15, 158:8, 168:11, 174:20, 228:6

**morning** [6] - 5:4, 22:2, 152:20, 168:22, 184:7, 184:23

**Morrison** [3] - 185:17, 186:4, 188:29

**mortgage** [1] - 52:14

**Most** [1] - 157:23

**most** [18] - 9:5, 9:6, 9:8, 20:12, 20:23, 27:9, 31:24, 52:12, 129:22, 148:14, 152:14, 189:26, 209:23, 215:21, 218:9, 223:29, 229:6, 230:23

**most-cited** [1] - 223:29

**most-visited** [1] - 152:14

**motion** [24] - 5:28, 7:23, 8:5, 11:12, 15:5, 15:6, 15:20, 15:24, 22:8, 22:15, 22:19, 22:29, 25:27, 26:1, 26:4, 26:10, 32:13, 181:25, 181:29, 182:7, 182:13, 194:4, 213:16

**motion-to-dismiss** [1] - 32:13

**motions** [1] - 11:13

**move** [10] - 11:8, 32:22, 41:20, 54:1, 72:9, 128:9, 179:14, 184:10, 184:13, 185:6

**moves** [1] - 194:11

**moving** [1] - 5:11

**MR** [136] - 2:4, 2:4, 2:9, 2:10, 2:14, 2:15,

2:15, 2:25, 2:29, 3:1, 4:5, 5:7, 11:20, 21:10, 21:12, 21:16, 21:24, 22:3, 22:5, 27:25, 28:25, 28:27, 29:1, 36:29, 38:9, 38:14, 38:16, 38:19, 39:17, 39:19, 39:22, 39:25, 39:28, 40:2, 40:4, 40:7, 41:2, 41:7, 57:26, 58:28, 59:4, 75:9, 75:10, 75:11, 75:12, 75:16, 75:20, 75:22, 75:26, 76:7, 78:1, 86:22, 86:27, 87:4, 87:7, 87:21, 87:24, 87:27, 88:1, 91:22, 91:27, 92:3, 93:19, 97:27, 97:28, 98:4, 106:16, 106:26, 106:29, 107:7, 107:8, 107:9, 107:11, 107:26, 110:6, 111:2, 111:8, 111:11, 111:14, 111:16, 112:13, 112:16, 117:12, 117:19, 119:2, 119:4, 119:7, 119:12, 119:13, 119:18, 122:25, 123:11, 124:16, 124:28, 127:9, 128:5, 128:8, 152:22, 154:8, 159:6, 159:15, 169:27, 177:29, 178:16, 179:11, 179:15, 179:17, 179:21, 182:14, 184:13, 219:3, 219:11, 219:14, 219:17, 219:25, 220:23, 220:27, 221:18, 221:21, 221:25, 221:28, 221:29, 222:3, 222:8, 222:10, 222:12, 222:16, 230:7, 232:2, 232:6, 232:8, 232:14, 232:17, 232:18, 232:20, 232:21

**MS** [99] - 1:17, 2:5, 2:9, 2:19, 2:20, 2:25, 2:30, 3:2, 5:4, 11:18, 21:7, 21:11, 21:14, 21:23, 22:1, 22:4, 27:24, 28:24, 28:26, 28:29, 36:28, 38:8, 38:12, 38:15, 38:18, 39:16, 39:18, 39:20, 39:24, 39:27, 40:3, 40:6, 41:1, 41:6,

57:25, 58:26, 59:3, 75:7, 75:13, 75:24, 76:6, 77:28, 86:20, 86:24, 86:28, 87:5, 87:18, 87:22, 87:26, 87:29, 91:19, 91:23, 91:29, 93:16, 98:1, 106:24, 107:25, 110:4, 110:29, 111:6, 111:10, 111:13, 111:15, 112:12, 112:15, 117:9, 117:18, 118:25, 119:16, 124:13, 127:7, 128:4, 152:21, 154:7, 159:5, 159:14, 169:25, 177:28, 178:15, 179:9, 179:14, 182:12, 184:12, 219:1, 219:10, 219:13, 219:15, 219:24, 220:26, 221:17, 221:19, 221:23, 221:26, 222:1, 222:6, 222:14, 230:5, 231:29, 232:4

**multi** [4] - 168:19, 169:14, 169:26, 169:27

**multi-communication** [1] - 168:19

**multi-communications** [3] - 169:14, 169:26, 169:27

**multiple** [5] - 159:27, 190:28, 225:8, 225:15, 226:25

**Murphy** [2] - 179:20, 179:21

**MURRAY** [1] - 2:4

**must** [58] - 3:9, 12:5, 15:13, 15:18, 22:20, 24:21, 25:22, 26:5, 26:11, 26:24, 28:2, 28:8, 28:13, 29:10, 30:3, 31:10, 49:14, 51:8, 51:26, 51:28, 53:5, 53:12, 54:13, 56:6, 57:26, 58:7, 58:19, 61:4, 61:23, 62:9, 62:10, 62:11, 69:16, 72:4, 75:26, 89:7, 89:9, 123:8, 129:27, 134:5, 146:20, 151:15, 151:21, 151:23, 153:2, 164:15,

170:19, 192:25, 195:2, 201:18, 206:13, 209:24, 211:20, 214:15, 215:4, 216:27, 217:1, 217:6

## N

**name** [3] - 17:14, 17:20

**Named** [1] - 189:2

**named** [2] - 1:26, 223:9

**namely** [1] - 62:16

**names** [1] - 143:2

**narrow** [7] - 12:29, 13:12, 128:12, 128:24, 201:8, 203:2, 203:9

**narrowed** [2] - 28:19, 215:7

**narrower** [2] - 30:17, 205:21

**Nation's** [1] - 119:22

**national** [54] - 7:21, 45:19, 46:21, 49:20, 53:28, 56:29, 60:25, 63:29, 64:6, 64:12, 64:29, 65:9, 68:24, 74:11, 79:16, 79:27, 80:12, 88:9, 89:7, 89:8, 95:24, 96:21, 97:12, 100:16, 101:16, 101:26, 109:14, 119:23, 119:27, 146:8, 153:12, 155:17, 173:16, 173:26, 173:28, 176:1, 186:25, 189:25, 194:26, 195:23, 199:28, 208:2, 215:21, 216:1, 216:14, 216:18, 217:15, 218:8, 225:14, 225:18, 229:24, 230:26, 230:28, 231:24

**National** [19] - 5:22, 13:23, 14:22, 21:25, 31:1, 43:2, 58:22, 67:2, 70:9, 74:21, 102:27, 105:14, 129:6, 137:6, 153:29, 154:4, 195:13, 206:26, 214:3

**nationality** [2] - 146:16, 146:22

**nationals** [2] -

27

28

29

88:4, 94:3, 101:4, 113:14, 113:16, 118:13, 118:22, 120:17, 131:3, 131:25, 131:27, 132:2, 134:4, 135:7, 136:14, 141:23, 141:29, 142:14, 143:7, 173:15, 181:28, 194:9, 196:18, 199:6, 214:17

**ordered** [1] - 121:3
**orders** [9] - 43:19, 61:17, 62:8, 72:5, 115:22, 123:24, 157:11, 195:22, 209:22
**Orders** [5] - 65:20, 102:24, 106:6, 117:22, 123:24
**ordinary** [5] - 67:19, 103:21, 172:6, 172:14, 172:29
**organisation** [21] - 44:15, 49:28, 50:8, 52:6, 54:29, 55:11, 56:26, 56:29, 57:26, 58:4, 58:10, 59:17, 60:9, 60:17, 61:4, 62:16, 62:22, 63:17, 81:6, 110:21
**organisation's** [3] - 60:1, 60:3, 60:29
**organisations** [29] - 14:8, 14:10, 40:12, 41:15, 43:29, 44:27, 49:4, 49:12, 49:23, 49:29, 50:28, 51:26, 51:28, 53:5, 53:12, 54:6, 54:13, 55:6, 55:27, 56:5, 56:13, 56:17, 58:8, 66:25, 85:27, 88:12, 171:25, 172:2, 227:16
**Organisations** [1] - 61:23
**organization** [2] - 143:20, 201:18
**organizations** [3] - 13:24, 136:14, 152:12
**organs** [1] - 88:28
**orientation** [1] - 146:4
**origin** [1] - 167:3
**original** [4] - 9:27, 51:14, 76:28, 129:26
**originally** [2] - 131:24, 185:21
**originated** [1] - 203:18

**originating** [1] - 202:7
**origins** [1] - 197:6
**ostensibly** [1] - 136:25
**OTHER** [1] - 155:26
**otherwise** [8] - 22:16, 27:14, 68:19, 103:17, 119:26, 123:13, 190:13, 210:7
**outcome** [1] - 81:17
**outlets** [1] - 129:14
**outline** [1] - 50:25
**outlined** [1] - 106:14
**outlines** [2] - 192:20, 226:26
**outright** [1] - 8:16
**outset** [4] - 22:25, 29:7, 31:9, 153:1
**outside** [15] - 105:13, 105:14, 118:3, 122:28, 134:24, 140:19, 155:4, 159:19, 163:11, 163:16, 167:1, 167:9, 176:17, 176:26, 229:7
**outstanding** [2] - 37:18, 118:20
**Overall** [1] - 82:18
**overall** [6] - 177:25, 222:19, 226:4, 227:29, 228:12, 229:23
**overarching** [1] - 189:28
**overcome** [1] - 23:12
**overlooked** [1] - 179:21
**overrides** [2] - 188:12, 188:14
**overseas** [2] - 131:2, 144:18
**oversee** [1] - 78:12
**overseeing** [1] - 101:15
**overseen** [2] - 141:18, 164:26
**oversees** [1] - 71:19
**overside** [1] - 113:16
**oversight** [41] - 64:12, 65:1, 69:26, 70:4, 70:5, 70:7, 70:14, 70:18, 71:2, 71:17, 71:24, 72:1, 78:11, 78:22, 79:1, 79:3, 79:16, 80:10, 80:17, 80:22, 80:23, 82:21, 86:10, 101:10, 101:26, 104:29,

105:1, 115:7, 123:18, 133:3, 141:12, 160:23, 165:2, 165:5, 165:6, 220:3, 220:4, 225:9, 225:15, 225:28, 226:12
**Oversight** [11] - 10:26, 54:2, 70:11, 70:12, 71:5, 71:18, 101:19, 115:6, 158:5, 164:19, 227:14
**overstates'** [1] - 32:6
**overstay** [1] - 119:26
**overtaken** [1] - 93:10
**overturned** [1] - 152:28
**overview** [4] - 42:21, 189:20, 189:26, 218:5
**overwhelming** [3] - 150:11, 183:3, 183:20
**owe** [2] - 188:15, 188:27
**owed** [1] - 187:16
**own** [11] - 22:24, 24:4, 59:6, 60:15, 61:12, 63:21, 70:23, 79:28, 124:8, 188:9, 199:1
**owned** [1] - 208:22
**Oxford** [1] - 226:6

## P

**package** [1] - 34:6
**packaged** [1] - 169:18
**page** [78] - 6:11, 11:8, 11:9, 14:18, 14:19, 14:27, 16:11, 16:29, 18:11, 18:20, 19:3, 21:21, 23:20, 24:9, 28:24, 28:25, 28:26, 39:3, 39:4, 39:8, 39:9, 39:13, 39:16, 39:19, 39:28, 40:21, 41:3, 41:4, 41:12, 41:20, 42:5, 42:19, 42:25, 43:1, 43:11, 47:19, 48:1, 52:27, 55:8, 56:24, 66:9, 67:11, 72:18, 85:21, 88:25, 97:27, 97:29, 98:5, 99:9, 102:12, 104:25, 107:24, 112:11, 124:26, 129:2, 129:19, 159:12, 177:27, 178:13, 180:13, 181:12, 182:29, 183:15,

184:9, 184:13, 191:25, 201:1, 205:19, 206:2, 211:27, 212:20, 219:21, 221:14, 222:16, 224:22, 224:25
**PAGE** [1] - 4:3
**pages** [9] - 39:25, 47:17, 66:5, 169:4, 219:22, 220:10, 221:15, 224:25, 225:2
**panel** [8] - 8:14, 57:10, 59:9, 59:14, 59:19, 59:28, 60:2, 62:3
**Panel** [1] - 57:8
**Panel'** [1] - 61:23
**paragraph** [25] - 12:26, 16:29, 23:20, 39:12, 43:24, 43:27, 47:18, 52:10, 53:19, 61:10, 66:6, 72:11, 75:7, 86:24, 99:9, 100:8, 102:12, 129:20, 140:4, 147:27, 184:14, 186:17, 188:12, 221:1, 222:17
**parameters** [2] - 130:9, 137:27
**pardon** [3] - 48:8, 117:15, 184:22
**parent** [1] - 189:2
**part** [23] - 15:12, 34:5, 34:9, 39:23, 46:1, 56:5, 61:13, 81:16, 106:20, 116:1, 116:10, 116:18, 116:23, 116:24, 122:4, 124:2, 124:5, 130:17, 138:15, 154:8, 158:11, 189:7, 214:7
**Part** [4] - 225:5, 225:20, 226:24, 228:21
**partial** [1] - 96:7
**partially** [1] - 137:4
**participate** [2] - 138:26, 223:23
**participated** [1] - 223:17
**participates** [1] - 129:13
**participating** [5] - 9:18, 10:3, 53:5, 109:14, 138:28
**particular** [58] - 17:9, 17:14, 17:29, 29:18,

35:2, 42:9, 44:8, 54:29, 59:11, 61:6, 61:13, 65:19, 69:6, 77:1, 77:23, 77:24, 78:19, 80:12, 82:4, 82:24, 86:1, 88:21, 96:14, 96:28, 97:13, 103:9, 106:7, 109:6, 117:25, 117:29, 118:21, 122:16, 139:14, 141:3, 142:27, 152:22, 153:10, 153:18, 155:2, 156:10, 157:25, 170:21, 171:11, 171:17, 172:11, 174:1, 178:19, 179:3, 182:10, 190:11, 192:9, 195:11, 195:16, 201:11, 208:9, 208:10, 220:13, 220:17
**particularised** [1] - 214:17
**particularity** [2] - 135:5, 159:22
**particularized** [1] - 24:21
**particularized'** [1] - 151:22
**particularly** [5] - 49:7, 80:15, 119:28, 187:27, 218:7
**parties** [8] - 17:19, 18:17, 21:6, 50:10, 60:10, 112:26, 184:27, 187:27
**parties'** [2] - 12:18, 211:4
**partner** [1] - 186:4
**partners** [1] - 146:9
**parts** [3] - 116:24, 218:23, 220:18
**Parts** [1] - 228:2
**party** [5] - 3:10, 133:10, 188:15, 213:27, 215:2
**Party** [7] - 94:29, 97:16, 107:22, 110:5, 111:24, 111:26, 112:3
**pass** [1] - 22:15
**passed** [1] - 227:5
**past** [1] - 182:24
**paths** [2] - 226:27, 227:12
**pause** [5] - 44:29, 54:19, 63:15, 77:9, 86:20
**Pause)** [1] - 185:10

30

pausing [1] - 81:4
payment [1] - 213:23
PBD28 [1] - 117:29
PCLOB [12] - 10:25,
70:10, 80:21, 115:10,
115:14, 115:21,
158:6, 160:1, 160:24,
161:9, 161:10, 168:28
PCLOB) [1] - 78:23
pecuniary [3] -
215:9, 215:15, 217:6
pen [3] - 43:19,
191:23, 192:26
penalties [1] -
209:14
pending [1] - 119:10
pending' [1] - 217:1
Pennsylvania [1] -
5:27
Penny [1] - 40:24
people [7] - 34:27,
41:8, 55:4, 67:25,
110:9, 133:7, 135:3
per [3] - 152:25,
156:2, 193:16
perceive [1] - 220:2
percent [1] - 224:5
perform [1] - 98:29
performance [2] -
99:14, 109:9
perhaps [13] - 14:13,
20:24, 27:9, 28:18,
31:24, 38:2, 77:25,
84:8, 90:24, 93:26,
97:10, 127:7, 138:14
period [2] - 137:16,
148:8
period) [1] - 208:29
periodic [1] - 70:6
periodically [1] -
94:5
permanent [4] -
121:24, 122:14,
176:26, 197:24
permanently [3] -
68:18, 143:16, 149:21
permission [1] - 3:10
permissive [5] -
131:7, 135:27, 143:6,
149:11, 158:23
permit [8] - 132:15,
141:26, 142:1, 142:2,
142:9, 142:26,
160:17, 164:8
permits [7] - 134:23,
143:11, 156:5,
159:18, 159:22,
163:22, 191:6
permitted [5] -
148:23, 149:7,

163:21, 205:29,
207:13
persistent [1] - 60:2
person [52] - 17:22,
36:16, 68:15, 68:16,
73:27, 75:6, 76:4,
77:13, 87:23, 87:25,
105:7, 107:1, 126:7,
131:2, 133:11,
134:24, 135:17,
141:22, 141:27,
143:12, 143:19,
143:26, 144:7,
155:13, 159:19,
164:11, 164:12,
170:21, 175:3,
175:20, 176:4, 176:6,
181:23, 182:2,
188:20, 191:6,
192:17, 193:9,
193:13, 194:1, 194:3,
198:4, 205:5, 205:13,
206:5, 208:27, 209:4,
209:18, 221:6, 223:4,
224:9, 226:27
person' [1] - 151:4
person.. [1] - 198:18
personal [68] - 6:3,
40:11, 43:27, 44:8,
44:19, 44:26, 45:22,
46:22, 49:3, 49:27,
50:3, 51:1, 51:8,
51:20, 51:22, 52:7,
52:13, 53:8, 58:12,
63:5, 63:13, 64:5,
64:28, 66:19, 66:27,
67:4, 67:24, 68:13,
68:26, 69:19, 69:29,
72:23, 72:27, 74:4,
79:17, 80:4, 84:11,
85:26, 86:3, 86:14,
96:22, 97:14, 101:27,
108:25, 108:27,
139:23, 144:22,
145:4, 145:18,
145:20, 146:18,
146:21, 148:21,
149:4, 163:7, 164:10,
174:19, 186:24,
189:24, 210:6, 213:6,
216:13, 228:5, 228:8,
228:13, 228:18,
231:16, 231:22
personally [1] -
121:25
personnel [1] -
147:15
persons [72] - 10:29,
67:28, 67:29, 68:26,
69:20, 73:4, 74:2,

74:15, 76:14, 83:7,
84:7, 88:7, 112:3,
121:23, 122:7,
122:13, 122:24,
124:7, 124:12,
126:11, 130:24,
131:11, 133:8,
135:11, 135:21,
135:26, 136:26,
138:9, 139:9, 140:15,
141:8, 141:28, 143:8,
145:19, 145:21,
145:24, 146:3,
146:15, 146:17,
148:16, 148:21,
148:23, 148:29,
149:5, 149:7, 149:12,
154:29, 155:4,
155:20, 155:22,
158:25, 159:27,
164:15, 164:16,
175:18, 175:26,
175:29, 176:16,
176:25, 189:8,
192:28, 192:29,
199:23, 205:1, 225:6,
225:15, 227:19,
228:5, 231:17
PERSONS [1] -
154:26
persons' [2] -
132:24, 136:29
perspective [3] -
42:22, 103:21, 103:24
persuasive [2] -
8:25, 12:5
pertain [1] - 44:7
pertaining [4] -
194:15, 195:1,
195:17, 199:2
pertains [1] - 146:23
pertinent [1] - 46:7
phase [1] - 23:14
phenomenon [1] -
27:15
Philip [1] - 187:24
PHILIP [1] - 2:6
phone [5] - 133:10,
139:16, 142:28,
144:8, 144:10
photocopied [1] -
3:9
phrase [4] - 18:1,
80:25, 80:26, 122:10
physical [4] - 139:7,
155:16, 177:13,
191:20
picture [1] - 220:1
piece [3] - 17:28,
169:19, 180:20

pieces [1] - 21:29
PISA [2] - 217:20,
217:24
place [22] - 21:17,
53:21, 58:18, 68:23,
94:14, 102:8, 108:29,
122:3, 123:18,
123:19, 125:10,
129:29, 130:2, 131:9,
132:28, 141:21,
160:25, 167:22,
176:12, 176:23,
176:26, 200:28
placed [2] - 106:6,
123:15
places [3] - 132:7,
134:28, 163:3
plain [1] - 206:28
plainly [2] - 20:3,
142:10
Plaintiff [1] - 188:22
plaintiff [27] - 12:16,
15:14, 15:18, 16:3,
26:11, 27:2, 27:6,
28:2, 28:8, 28:13,
29:10, 30:3, 151:9,
151:23, 198:10,
198:16, 199:8,
206:13, 206:16,
209:26, 211:19,
213:16, 214:15,
215:13, 216:27,
217:1, 217:6
PLAINTIFF [2] - 1:7,
2:4
plaintiff's [9] - 11:29,
12:12, 16:20, 32:15,
151:14, 153:2,
213:26, 213:28,
216:13
plaintiffs [34] - 6:20,
7:9, 7:23, 7:24, 8:1,
8:12, 8:18, 8:20,
13:24, 14:4, 15:9,
16:11, 18:3, 18:11,
18:12, 18:13, 18:22,
22:9, 23:3, 23:14,
26:1, 26:5, 26:23,
30:9, 31:8, 31:10,
32:9, 152:4, 152:17,
152:29, 209:24,
212:9, 217:9, 217:11
Plaintiffs [6] - 15:1,
16:29, 17:26, 18:20,
23:9, 199:5
plaintiffs' [7] - 8:14,
13:27, 13:28, 18:1,
26:20, 151:29, 214:4
plaintiff's [1] - 15:13
plausibility [3] -

6:15, 22:16, 29:8
plausible [6] - 6:8,
7:13, 26:2, 29:23,
32:14, 153:3
plausible' [1] - 31:10
plausibly [4] - 18:3,
23:10, 151:16, 152:23
play [1] - 178:3
played [1] - 134:14
plays [1] - 134:12
pleaded [5] - 6:22,
10:12, 10:15, 13:2,
22:20
pleading [4] - 13:2,
13:7, 212:4, 216:11
pleadings [4] - 12:1,
12:21, 29:8, 187:26
pleadings' [1] -
22:17
pleased [1] - 98:11
pleasure [1] - 116:6
pled [1] - 22:16
point [23] - 19:5,
21:13, 26:22, 29:18,
31:18, 39:10, 46:25,
76:25, 89:12, 90:25,
98:22, 112:24,
117:25, 123:13,
127:8, 190:14,
199:24, 201:2,
204:11, 219:12,
222:7, 232:1, 232:2
pointed [1] - 74:1
points [5] - 8:3,
64:18, 68:3, 123:22,
128:22
points' [1] - 144:18
policies [20] - 53:12,
71:10, 102:20, 103:4,
106:4, 118:14,
121:22, 122:13,
123:18, 123:23,
124:11, 125:8,
140:24, 140:26,
142:6, 142:9, 142:10,
143:13, 157:12
Policies [1] - 102:25
policies' [1] - 141:3
Policy [5] - 43:4,
65:24, 117:23, 130:4,
223:7
policy [20] - 45:5,
54:13, 69:5, 100:22,
117:24, 120:21,
121:29, 122:2, 122:8,
122:12, 122:21,
122:23, 123:5, 124:4,
124:8, 126:13,
126:29, 127:4,
146:25, 194:26

31

policy' [1] - 195:24
political [7] - 25:3, 25:13, 82:25, 116:5, 116:7, 123:8, 143:3
pool [1] - 61:27
population [1] - 142:20
portion [2] - 17:7, 18:5
position [39] - 12:3, 27:26, 28:7, 28:23, 30:1, 32:17, 112:8, 113:9, 114:4, 114:25, 115:19, 116:21, 116:29, 127:6, 150:27, 154:28, 157:3, 158:12, 159:16, 159:26, 160:7, 161:9, 161:28, 163:15, 164:2, 164:14, 165:22, 166:7, 166:27, 167:28, 169:7, 170:24, 174:1, 176:13, 177:9, 178:22, 183:14, 232:12, 232:19
positive [2] - 81:10, 81:11
possesses [1] - 9:21
possession [1] - 147:11
possibilities [1] - 74:15
possibilities' [1] - 6:25
possibility [13] - 33:6, 41:17, 42:14, 55:28, 56:15, 60:24, 61:24, 73:25, 96:27, 109:8, 182:7, 192:5, 229:19
possible [4] - 48:16, 69:6, 93:5, 100:20
possibly [2] - 86:25, 169:2
post [3] - 17:28, 27:16, 27:17
post-Clapper [1] - 27:16
post-Snowden [1] - 27:17
postdates [1] - 90:26
posted [1] - 28:11
posture [6] - 7:8, 8:26, 10:16, 22:13, 25:24, 25:26
Potential [1] - 190:3
potential [7] - 95:29, 136:1, 189:26, 190:2,

190:4, 200:13, 215:25
potentially [3] - 202:6, 228:21, 229:4
potions [1] - 191:7
power [9] - 45:11, 60:8, 65:16, 80:19, 132:6, 132:9, 193:10
power' [1] - 132:10
powers [14] - 20:8, 24:4, 25:2, 44:12, 53:14, 61:5, 78:22, 82:23, 83:19, 101:11, 108:22, 134:21, 147:7, 226:5
PPD-28 [46] - 43:6, 65:28, 66:17, 67:21, 67:24, 70:6, 71:28, 76:23, 78:4, 98:18, 106:7, 106:9, 122:3, 123:5, 123:29, 140:25, 145:10, 145:13, 145:23, 145:28, 146:26, 147:2, 147:28, 148:27, 149:19, 160:25, 163:24, 164:4, 164:8, 164:10, 164:14, 174:4, 174:7, 174:16, 174:18, 174:23, 175:1, 175:4, 175:7, 175:12, 175:15, 175:18, 175:24, 175:28, 176:3
PPD-28's [4] - 147:24, 148:14, 174:13, 174:20
PPD28 [1] - 66:6
practical [2] - 197:16, 219:28
practice [17] - 42:13, 45:15, 48:4, 48:28, 60:16, 86:12, 108:29, 125:19, 147:22, 160:9, 161:2, 186:27, 200:3, 225:6, 226:2, 226:17, 228:10
practices [9] - 19:15, 42:11, 55:12, 59:27, 62:28, 98:15, 146:27, 170:5, 170:7
pre [2] - 22:19, 50:9
pre-discovery [1] - 22:19
pre-existing [1] - 50:9
precedent [2] - 119:8, 180:9
precedential [1] - 31:12
precise [2] - 162:3,

200:8
precisely [1] - 41:29
precondition [1] - 211:21
predicated [1] - 134:18
predict [2] - 27:13, 203:26
preempts [1] - 153:26
preferred [1] - 10:17
prejudice [1] - 49:20
preliminary [5] - 7:25, 8:1, 8:11, 8:21, 89:10
premises [2] - 12:9, 134:28
preparation [4] - 186:12, 188:8, 188:23, 189:11
prepare [4] - 81:20, 95:11, 186:16, 187:25
prepared [1] - 108:4
preparing [1] - 187:14
preponderance [4] - 23:15, 26:6, 29:10, 151:25
prerequisite [3] - 32:4, 215:5, 215:9
presence [1] - 177:13
present [11] - 12:8, 15:4, 31:18, 46:11, 47:3, 49:22, 65:22, 105:18, 119:27, 121:17, 206:13
presentation [1] - 9:16
presented [1] - 12:14
presenting [1] - 212:4
presently [1] - 165:16
presents [1] - 206:16
President [20] - 5:16, 43:5, 65:18, 66:11, 71:7, 98:17, 107:1, 118:13, 121:8, 125:25, 130:5, 145:12, 145:26, 197:4, 223:2, 223:6, 223:7, 223:8, 223:17, 223:26
President's [2] - 65:9, 70:11
presidential [3] - 118:4, 123:24, 157:11
Presidential [9] - 43:4, 65:20, 65:24,

102:24, 103:4, 106:6, 117:22, 121:28, 130:4
presiding [1] - 23:24
Press [1] - 224:3
press [2] - 161:21, 227:15
presumably [5] - 23:13, 46:4, 78:3, 100:6, 231:9
presume [2] - 93:5, 124:13
prevail' [1] - 230:20
prevailed [1] - 156:17
prevailed' [1] - 199:9
prevailing [1] - 177:6
prevent [4] - 140:2, 150:1, 205:11, 231:1
preventing [2] - 153:7, 202:4
prevention [1] - 95:24
prevents [1] - 47:6
previous [2] - 100:8, 177:10
previously [3] - 112:10, 167:17, 167:24
primarily [4] - 33:26, 58:29, 110:10, 222:20
primary [3] - 38:13, 140:12, 164:23
Princeton [1] - 224:3
principal [1] - 6:14
principally [2] - 134:1, 170:15
principle [5] - 74:15, 93:14, 108:18, 123:14, 201:7
Principle [10] - 50:7, 50:27, 51:8, 51:14, 51:16, 51:20, 52:3, 53:5, 53:21, 56:7
principles [27] - 34:21, 34:26, 40:16, 40:29, 41:13, 41:17, 42:14, 45:6, 48:22, 49:12, 49:18, 50:23, 53:7, 53:13, 54:7, 57:20, 61:1, 63:7, 66:15, 78:3, 86:5, 91:11, 91:13, 97:9, 145:14, 145:28, 188:6
Principles [24] - 44:17, 45:12, 45:14, 49:25, 49:27, 50:5, 50:18, 51:26, 53:17, 53:25, 53:26, 55:11, 55:26, 56:22, 58:9, 61:8, 62:6, 62:23,

63:3, 63:28, 86:2, 88:13, 95:22, 96:1
Principles.. [1] - 86:11
prioritisation [1] - 121:11
Prism [2] - 67:11, 72:14
PRISM [23] - 6:15, 9:11, 9:19, 9:28, 10:8, 10:13, 10:19, 14:15, 137:17, 138:3, 138:11, 138:15, 138:26, 138:28, 161:6, 161:7, 161:16, 161:18, 161:23, 171:8, 171:12, 179:6, 179:8
Pritzker [1] - 40:24
privacy [40] - 30:19, 37:19, 42:21, 48:22, 49:12, 50:23, 54:13, 56:21, 61:14, 70:18, 71:11, 75:5, 76:3, 84:29, 89:5, 112:22, 121:22, 122:12, 122:24, 135:11, 136:25, 145:23, 146:18, 156:27, 186:5, 186:22, 189:24, 201:20, 213:5, 215:21, 217:15, 218:7, 220:15, 222:19, 222:20, 222:26, 223:5, 226:26, 226:29, 227:16
PRIVACY [1] - 3:1
Privacy [207] - 5:11, 10:25, 32:22, 34:8, 34:12, 34:17, 35:24, 35:28, 36:6, 36:23, 36:26, 37:11, 38:11, 38:26, 39:11, 40:13, 40:15, 41:12, 41:22, 42:12, 42:20, 43:18, 43:28, 44:16, 44:23, 46:23, 46:27, 47:5, 47:23, 48:25, 49:3, 49:10, 50:1, 50:8, 54:3, 54:7, 54:14, 55:4, 55:25, 56:21, 57:8, 60:3, 60:18, 61:4, 61:12, 62:3, 63:14, 64:6, 64:13, 64:29, 66:26, 67:5, 68:27, 70:9, 70:10, 71:4, 73:19, 73:21, 78:9, 78:13, 78:21, 79:5, 79:12, 79:19,

32

80:1, 80:8, 80:20, 81:16, 81:22, 82:8, 82:14, 83:8, 85:18, 85:20, 85:22, 85:28, 88:9, 90:15, 90:29, 91:11, 91:24, 92:18, 92:25, 93:23, 93:25, 94:7, 94:16, 94:25, 95:7, 95:18, 96:4, 96:23, 97:2, 98:12, 98:25, 99:11, 99:15, 100:18, 101:2, 101:9, 102:15, 102:20, 103:12, 103:26, 104:1, 104:10, 104:18, 105:2, 105:3, 105:27, 106:12, 106:18, 107:18, 107:19, 107:27, 108:2, 108:3, 108:5, 108:10, 108:18, 108:21, 109:3, 109:17, 109:20, 109:24, 109:28, 111:4, 112:5, 112:8, 113:9, 113:15, 114:6, 114:21, 114:27, 115:1, 115:5, 115:16, 116:23, 117:6, 117:20, 121:18, 121:25, 122:2, 122:4, 122:7, 122:22, 124:7, 124:9, 125:5, 125:23, 126:5, 126:9, 126:13, 126:26, 127:2, 144:20, 150:6, 157:1, 157:3, 158:4, 158:9, 163:6, 184:11, 184:16, 184:23, 194:11, 194:14, 194:19, 195:14, 195:26, 196:10, 196:14, 196:22, 196:29, 197:8, 197:14, 197:18, 197:26, 198:13, 199:12, 199:24, 199:26, 199:29, 200:5, 200:9, 201:29, 204:13, 204:15, 210:3, 210:5, 215:1, 215:4, 215:9, 215:29, 217:7, 222:27, 222:28, 223:3, 223:16, 223:20, 227:3, 227:13, 229:17, 229:21, 230:3, 231:7, 231:11
**privacy-protective** [1] - 227:16
**private** [30] - 35:11,

41:8, 41:10, 54:20, 55:1, 56:20, 63:16, 63:18, 63:23, 91:9, 112:21, 112:26, 113:2, 113:3, 113:12, 130:23, 146:6, 173:20, 173:26, 183:28, 189:21, 202:2, 202:8, 202:10, 202:23, 202:25, 209:15, 222:25, 223:23, 227:25
**private-sector** [1] - 56:20
**privilege** [10] - 153:9, 153:17, 153:26, 154:1, 179:7, 179:25, 179:28, 180:1, 180:4, 180:10
**privilege'** [1] - 153:7
**Privy** [1] - 101:18
**pro** [1] - 109:27
**pro-actively** [1] - 109:27
**probable** [4] - 84:3, 132:16, 134:18, 135:6
**problem** [1] - 11:9
**problematic** [1] - 147:25
**problems** [1] - 50:12
**procedural** [8] - 7:8, 8:26, 10:16, 22:13, 26:29, 27:3, 28:3, 212:22
**procedurally** [1] - 25:27
**procedure** [11] - 24:3, 36:10, 36:12, 36:13, 46:12, 81:14, 96:7, 96:15, 97:6, 101:21, 226:21
**Procedure** [6] - 73:26, 183:16, 183:24, 183:27, 212:3, 216:9
**procedures** [32] - 19:14, 19:16, 43:15, 66:14, 67:29, 70:4, 97:10, 117:29, 134:2, 134:9, 136:23, 136:24, 136:26, 137:3, 137:5, 137:6, 142:26, 149:18, 160:12, 160:13, 160:16, 160:21, 160:23, 170:10, 170:16, 175:25, 175:27, 192:18, 192:28, 193:5, 217:20, 217:22

**procedures'** [3] - 134:8, 134:9, 135:13
**proceed** [4] - 23:13, 36:2, 106:12, 187:7
**proceeding** [5] - 151:5, 163:5, 195:7, 215:14, 229:2
**PROCEEDING** [1] - 4:3
**proceedings** [16] - 8:16, 19:28, 42:9, 89:9, 106:15, 110:29, 185:28, 187:12, 187:15, 187:23, 192:6, 192:7, 192:9, 211:6, 221:2, 230:6
**proceeds** [1] - 23:8
**process** [5] - 56:17, 59:15, 67:4, 114:20, 114:29
**processed** [5] - 53:8, 56:27, 59:2, 102:8, 103:29
**processed..** [1] - 72:23
**processing** [22] - 44:7, 44:18, 49:27, 49:28, 50:3, 51:1, 51:10, 51:17, 51:28, 52:7, 52:13, 52:28, 58:12, 62:9, 62:18, 79:17, 99:17, 100:16, 101:27, 103:22, 104:24, 186:23
**processor** [2] - 49:23, 51:29
**processors** [3] - 49:13, 49:14, 108:19
**procure** [1] - 205:2
**produce** [3] - 161:24, 161:26, 199:7
**produced** [1] - 154:21
**production** [1] - 196:18
**productive** [2] - 21:4, 21:5
**Prof** [20] - 29:4, 29:19, 30:17, 30:22, 31:11, 32:2, 112:29, 185:24, 185:27, 218:29, 219:4, 219:6, 219:7, 219:8, 220:5, 220:9
**Professionals** [1] - 222:27
**Professor** [1] - 226:6
**professor** [1] - 222:21
**profiling** [1] - 52:29

**profit** [1] - 14:9
**program** [17] - 5:22, 6:5, 8:28, 10:28, 19:10, 20:5, 20:6, 153:24, 161:18, 166:5, 167:21, 167:26, 168:5, 178:19, 178:20, 179:4, 209:5
**program"** [1] - 170:1
**programme** [3] - 9:29, 138:15, 169:24
**programmes** [3] - 14:15, 67:12, 72:14
**programs** [21] - 14:2, 27:18, 30:9, 47:24, 56:21, 137:29, 141:13, 141:15, 144:4, 144:7, 155:23, 161:4, 161:5, 161:7, 163:4, 163:16, 163:25, 164:6, 164:26, 172:25, 182:10
**prohibit** [1] - 114:21
**prohibited** [2] - 171:3, 195:18
**prohibition** [1] - 51:16
**prohibits** [2] - 191:12, 191:18
**Project** [1] - 129:6
**proliferation** [1] - 147:11
**promptly** [1] - 121:4
**promulgate** [3] - 194:18, 194:20, 194:27
**promulgated** [3] - 140:21, 143:14, 196:15
**promulgating** [1] - 195:3
**prong** [1] - 27:4
**pronunciation** [1] - 5:15
**proof** [3] - 15:15, 214:3, 217:9
**proper** [2] - 109:10, 157:7
**properly** [14] - 48:7, 77:3, 77:12, 82:3, 102:23, 103:2, 103:5, 103:6, 153:8, 156:5, 157:10, 187:9, 194:24, 195:21
**property** [2] - 134:28, 155:16
**proportionality** [3] - 84:26, 109:11, 174:11

**propose** [3] - 96:9, 128:14, 220:7
**proposed** [2] - 34:18, 136:23
**proposes** [2] - 134:2, 170:16
**proposing** [2] - 21:8, 128:9
**proposition** [1] - 18:4
**propositions** [1] - 184:7
**prosecute** [2] - 57:2, 231:1
**prosecuted** [1] - 19:17
**prosecuting** [1] - 202:5
**prosecution** [3] - 33:28, 95:25, 180:21
**prospective** [1] - 6:22
**protect** [10] - 44:18, 71:11, 102:19, 135:15, 136:25, 146:8, 155:4, 215:29, 225:6, 231:24
**protected** [6] - 65:3, 177:2, 208:26, 209:7, 209:8, 209:11
**protecting** [1] - 25:2
**protection** [45] - 31:27, 35:21, 37:4, 38:25, 40:11, 40:28, 44:25, 45:21, 45:24, 49:2, 52:1, 53:24, 56:16, 57:1, 59:5, 60:6, 60:12, 63:5, 69:24, 83:5, 83:29, 84:20, 85:21, 85:26, 86:3, 88:16, 89:4, 89:5, 89:18, 89:25, 94:2, 94:6, 94:18, 94:21, 95:18, 95:27, 96:6, 104:11, 155:23, 158:10, 223:14, 223:19, 224:10, 224:17, 228:11
**PROTECTION** [1] - 1:7
**Protection** [10] - 5:5, 37:27, 38:20, 58:22, 110:7, 110:11, 126:17, 128:6, 185:8, 197:8
**protections** [22] - 34:8, 52:16, 84:11, 84:23, 97:11, 121:24, 122:6, 122:24, 123:16, 124:6,

33

34

20:12, 20:23, 21:20, 27:29, 153:16, 214:12

**Recent** [1] - 144:3

**recently** [9] - 14:22, 19:26, 150:5, 196:20, 200:8, 201:10, 207:20, 227:3, 227:4

**recently-finalised** [1] - 227:3

**recitals** [2] - 49:1, 49:7

**recites** [1] - 67:24

**recklessly** [1] - 209:10

**recognised** [1] - 11:23

**recognises** [1] - 145:23

**recommendations** [11] - 47:26, 48:13, 70:28, 114:19, 114:28, 115:12, 158:7, 160:1, 160:24, 224:5, 224:6

**recommended** [1] - 224:27

**reconciled** [19] - 113:9, 114:25, 115:19, 116:21, 160:7, 161:9, 161:28, 163:15, 164:2, 164:14, 165:22, 166:7, 166:27, 167:28, 169:7, 170:24, 174:1, 177:9

**reconciliation** [2] - 30:1, 178:11

**record** [17] - 7:10, 8:6, 15:9, 16:4, 111:20, 187:24, 198:12, 198:25, 199:13, 199:18, 202:1, 202:7, 202:13, 202:21, 203:18, 217:26, 221:4

**record'** [7] - 200:18, 201:28, 202:12, 202:14, 202:26, 203:10, 203:21

**recording** [1] - 144:9

**records** [43] - 20:16, 24:4, 29:25, 71:13, 74:3, 126:6, 126:10, 127:3, 144:9, 194:15, 194:17, 194:18, 194:20, 194:21, 194:28, 195:4, 195:10, 195:15, 195:17, 195:19, 196:13, 196:17,

196:19, 196:28, 197:20, 198:2, 199:1, 199:7, 199:28, 208:5, 208:11, 210:6, 210:9, 210:11, 210:13, 210:15, 210:16, 210:17, 210:23, 211:8, 211:9, 211:11

**Recourse** [3] - 53:4, 55:25, 56:6

**recourse** [11] - 53:7, 54:16, 55:27, 56:8, 56:13, 57:6, 58:18, 61:19, 73:15, 86:10, 227:15

**recover** [6] - 193:14, 198:17, 206:8, 215:3, 215:10, 215:16

**recovery** [3] - 190:2, 190:13, 215:8

**rectification** [2] - 86:15, 86:29

**rectified'** [1] - 87:3

**rectify** [1] - 62:10

**redacted** [1] - 137:4

**redress** [23] - 36:14, 41:25, 52:25, 55:22, 57:13, 61:20, 62:24, 65:1, 70:2, 73:25, 74:9, 74:14, 76:9, 76:17, 79:2, 124:15, 150:2, 150:4, 155:20, 155:24, 156:2, 157:5, 158:28

**Redress** [38] - 34:10, 118:6, 122:5, 124:5, 124:15, 125:6, 125:10, 125:21, 126:21, 149:27, 197:2, 197:4, 198:11, 199:10, 199:22, 199:27, 200:2, 200:7, 200:10, 200:14, 202:19, 203:11, 203:26, 204:6, 214:25, 214:29, 215:11, 215:14, 215:24, 215:26, 216:2, 216:19, 216:22, 217:5, 217:25, 218:11, 227:5

**Redress"** [1] - 72:19

**redressability** [3] - 16:5, 23:11, 24:20

**redressability]** [1] - 24:24

**redressable** [1] - 24:23

**redressed** [1] - 151:20

**reducing** [1] - 18:26

**refer** [22] - 11:9, 13:15, 23:20, 40:22, 53:11, 67:7, 74:20, 80:20, 83:10, 89:21, 90:20, 101:18, 112:6, 132:13, 138:13, 158:4, 159:4, 172:1, 174:10, 184:24, 191:10, 223:11

**reference** [15] - 10:24, 37:16, 89:9, 90:10, 91:5, 123:29, 170:1, 170:2, 175:20, 190:14, 193:24, 213:21, 214:24, 219:21, 221:15

**referenced** [2] - 189:27, 203:1

**references** [2] - 149:2, 191:3

**referencing** [1] - 153:22

**referrals** [1] - 95:7

**referred** [23] - 17:20, 20:12, 21:21, 33:24, 34:4, 34:12, 38:21, 46:12, 65:26, 66:7, 67:9, 73:13, 91:2, 92:22, 95:1, 104:28, 105:20, 111:25, 120:5, 152:19, 161:12, 197:8, 231:11

**referring** [12] - 9:26, 30:20, 87:5, 87:8, 124:26, 125:15, 138:14, 152:9, 154:11, 155:8, 202:28, 225:2

**refers** [39] - 15:7, 23:29, 37:1, 38:22, 48:1, 50:27, 51:3, 51:7, 52:18, 54:3, 55:7, 58:16, 60:12, 64:10, 67:11, 68:7, 71:28, 72:6, 73:7, 73:18, 85:16, 86:7, 97:16, 105:1, 120:2, 124:8, 133:14, 133:15, 152:19, 186:3, 186:9, 189:14, 192:5, 204:11, 206:25, 207:10, 208:10, 210:29

**refined** [1] - 72:2

**reflect** [1] - 136:10

**reflected** [2] - 7:21, 27:16

**reflection** [1] - 44:29

**reflective** [1] - 31:21

**reflects** [1] - 79:7

**reforms** [8] - 130:7, 145:25, 148:14, 148:17, 160:23, 174:29, 224:26

**refresh** [1] - 110:4

**refusal** [1] - 60:1

**refuse** [1] - 120:10

**refused** [2] - 24:1, 181:16

**refuses** [1] - 196:12

**regard** [14] - 24:15, 25:21, 30:12, 32:19, 44:18, 50:17, 65:23, 67:25, 69:27, 90:1, 94:11, 109:5, 164:29, 188:27

**regarded** [1] - 95:19

**regarding** [15] - 41:23, 55:29, 76:26, 82:10, 98:15, 98:23, 109:19, 121:25, 201:20, 214:27, 215:25, 218:13, 226:29

**Regardless** [1] - 216:7

**regardless** [3] - 146:16, 146:21, 208:22

**regards** [7] - 46:20, 62:18, 64:4, 65:11, 67:22, 96:20, 187:1

**regime** [2] - 132:22, 184:2

**regional** [1] - 201:17

**register** [2] - 43:19, 118:5

**Register** [1] - 48:21

**registers** [2] - 191:24, 192:26

**REGISTRAR** [2] - 5:5, 128:6

**regrets** [2] - 108:15, 108:28

**regularly** [2] - 129:13, 155:21

**regulate** [2] - 131:17, 140:26

**regulating** [1] - 160:21

**regulation** [1] - 195:8

**Regulations** [2] - 37:28, 38:20

**regulations** [16] - 37:28, 38:3, 38:4, 38:20, 104:1, 114:15, 114:23, 115:3,

129:12, 140:21, 141:21, 142:1, 142:15, 158:2, 195:12, 195:16

**rejected** [3] - 19:2, 20:18, 26:20

**rejection** [1] - 52:23

**relate** [3] - 72:26, 80:15, 92:1

**related** [16] - 52:7, 126:15, 138:24, 143:18, 143:20, 147:17, 149:22, 153:27, 156:9, 192:8, 202:10, 202:25, 211:14, 212:1, 216:17, 228:12

**relatedly** [1] - 134:16

**relates** [5] - 50:6, 78:19, 101:7, 190:14, 204:22

**relating** [10] - 29:26, 38:25, 50:29, 86:14, 94:5, 100:16, 197:15, 199:28, 200:13, 226:12

**relation** [21] - 16:9, 16:18, 16:27, 34:28, 35:2, 36:10, 37:19, 42:28, 46:5, 91:13, 94:16, 105:10, 110:15, 115:15, 123:3, 123:14, 125:11, 128:22, 184:9, 186:15, 199:16

**relations** [2] - 25:16, 229:24

**relationship** [1] - 229:24

**relationships** [1] - 50:10

**release** [2] - 24:2, 210:21

**released** [2] - 120:9, 138:27

**relevance** [3] - 163:2, 181:15, 199:14

**relevant** [27] - 37:9, 37:10, 51:9, 55:14, 68:4, 71:13, 82:4, 95:6, 114:15, 114:22, 115:3, 117:6, 121:16, 143:13, 158:2, 161:26, 163:4, 163:12, 176:1, 184:28, 184:29, 190:11, 201:4, 211:12, 215:27, 220:2, 220:24

**reliance** [6] - 8:9,

15:8, 52:24, 106:5, 123:15

**relied** [4] - 6:24, 11:27, 12:4, 187:14

**relief** [6] - 112:21, 189:29, 190:5, 199:6, 209:20, 209:23

**relief'** [1] - 62:5

**relies** [2] - 9:14, 166:17

**religion** [1] - 146:5

**rely** [11] - 18:3, 78:14, 78:21, 80:9, 90:25, 101:15, 106:2, 124:25, 135:6, 137:28, 166:14

**Relying** [1] - 207:19

**relying** [1] - 136:6

**remain** [2] - 16:6, 108:11

**remaining** [2] - 109:16, 217:23

**remains** [9] - 13:5, 33:1, 45:5, 106:14, 108:18, 122:3, 132:13, 203:14, 216:21

**remand** [3] - 8:15, 13:6, 13:9

**remanded** [1] - 27:5

**remanding** [1] - 8:21

**remark** [1] - 106:19

**remedial** [8] - 36:19, 77:21, 77:23, 77:27, 113:24, 157:19, 184:20, 215:12

**remediation** [1] - 79:6

**remedied** [4] - 77:7, 82:7, 102:29, 158:18

**remedied'** [4] - 81:12, 87:12, 103:7, 157:15

**remedied)** [1] - 81:2

**REMEDIES** [1] - 190:21

**remedies** [53] - 36:15, 53:9, 57:11, 58:7, 62:26, 73:3, 83:14, 86:13, 87:19, 112:20, 112:24, 113:3, 114:8, 114:18, 123:19, 177:29, 178:2, 178:5, 183:9, 186:19, 186:27, 186:29, 187:2, 187:9, 189:21, 190:3, 190:8, 191:4, 196:28, 197:17, 197:22, 199:23, 199:25,

200:15, 203:11, 216:1, 216:4, 216:19, 217:16, 217:23, 218:3, 218:6, 220:3, 220:15, 226:25, 227:2, 227:6, 227:12, 227:17, 227:23, 228:3, 231:15, 231:19

**Remedies** [1] - 190:26

**Remedy** [3] - 181:13, 182:29, 183:15

**remedy** [22] - 36:16, 56:3, 60:8, 62:5, 77:15, 77:24, 80:28, 81:8, 89:7, 91:3, 91:9, 93:18, 103:27, 112:26, 113:5, 113:7, 114:13, 157:26, 180:18, 183:20, 183:28, 194:1

**Remijas** [1] - 213:21

**remotely** [1] - 134:22

**removable** [5] - 120:6, 120:8, 120:26, 121:6, 121:10

**removal** [3] - 41:18, 60:3, 120:5

**removed** [2] - 121:3, 121:4

**removes** [1] - 60:18

**removing** [1] - 55:4

**rendering** [1] - 51:21

**rendition** [1] - 153:24

**repatriation** [1] - 120:11

**repeal** [4] - 96:8, 96:15, 97:6, 106:3

**repealing** [1] - 46:14

**repeatedly** [2] - 75:3, 76:1

**replace** [1] - 33:22

**replaced** [1] - 37:26

**reply** [1] - 219:7

**repo1ts** [1] - 144:16

**Report** [2] - 189:11, 189:12

**report** [40] - 46:7, 95:11, 107:4, 128:15, 128:17, 128:20, 128:26, 128:29, 129:2, 129:19, 130:17, 159:8, 161:9, 161:10, 168:28, 168:29, 185:7, 185:9, 185:11, 185:16, 185:23, 185:26, 187:14, 219:8, 219:19, 219:25,

219:27, 220:9, 220:12, 220:13, 220:19, 220:21, 220:22, 220:24, 220:29, 221:10, 221:11, 224:2

**reported** [4] - 106:24, 106:26, 171:23, 171:26

**Reporting** [3] - 27:1, 28:9, 52:19

**reporting** [5] - 71:25, 72:3, 113:18, 116:15, 184:16

**reports** [19] - 70:29, 71:13, 99:4, 99:19, 115:25, 125:19, 128:10, 138:2, 138:24, 138:29, 144:29, 161:21, 171:20, 171:23, 171:27, 172:1, 187:28, 187:29, 218:28

**represent** [3] - 19:28, 117:23, 117:24

**representation** [1] - 64:20

**representations** [16] - 35:17, 40:18, 46:18, 48:4, 48:23, 48:28, 50:16, 50:20, 66:23, 67:15, 74:20, 85:3, 86:18, 88:4, 96:18, 97:20

**representative** [3] - 111:27, 111:29, 112:2

**representatives** [3] - 109:15, 110:7, 110:10

**represented** [1] - 156:20

**representing** [1] - 152:11

**represents** [2] - 28:1, 31:26

**reproduced** [1] - 3:9

**request** [21] - 24:2, 46:29, 66:28, 78:19, 79:29, 80:13, 95:4, 95:28, 101:7, 101:24, 101:28, 102:6, 102:8, 102:14, 104:5, 104:26, 156:19, 196:13, 198:26, 198:29, 210:18

**requested** [4] - 25:12, 187:13, 187:19, 187:22

**requests** [13] - 78:26, 80:15, 98:14,

99:18, 100:16, 100:23, 101:5, 101:22, 103:28, 104:17, 104:24, 104:26, 173:27

**require** [12] - 6:17, 74:24, 115:15, 134:26, 157:24, 159:22, 175:16, 178:10, 195:7, 200:18, 214:2, 217:9

**required** [17] - 7:8, 15:16, 23:11, 46:29, 72:7, 85:9, 94:9, 95:26, 97:11, 131:24, 131:28, 136:22, 151:7, 176:14, 196:2, 196:21, 212:26

**requirement** [21] - 19:6, 20:7, 28:5, 30:23, 53:26, 68:7, 72:3, 133:16, 143:18, 149:22, 155:15, 174:8, 174:13, 176:19, 182:27, 192:11, 212:2, 212:14, 212:24, 214:18, 218:1

**requirement'** [1] - 68:20

**requirement)** [1] - 84:15

**requirements** [24] - 8:19, 16:1, 28:20, 48:17, 56:6, 59:15, 64:1, 66:12, 67:21, 71:25, 74:29, 94:26, 104:12, 135:14, 135:27, 175:2, 200:26, 201:18, 210:19, 212:15, 216:16, 216:21, 218:13, 225:9

**requires** [8] - 7:13, 55:26, 57:11, 135:5, 148:27, 175:24, 212:3, 216:10

**requiring** [7] - 32:9, 84:27, 114:20, 115:1, 161:25, 167:29, 171:13

**Research** [2] - 116:10, 116:17

**resemblance** [1] - 134:13

**reserve** [2] - 106:2, 232:18

**reside** [1] - 146:17

**resident** [3] - 84:7, 197:25, 226:27

**residents** [7] - 121:24, 122:14, 176:26, 193:1, 193:3, 197:18, 226:24

**resides** [1] - 146:23

**Resolution** [3] - 56:20, 113:10, 113:15

**resolution** [9] - 12:18, 34:28, 35:10, 54:21, 54:25, 55:2, 56:28, 58:2, 63:18

**resolutions** [1] - 112:25

**resolve** [5] - 35:12, 58:5, 60:29, 62:14, 79:8

**resolved** [6] - 56:2, 56:10, 57:6, 61:21, 82:20, 200:11

**resort** [1] - 52:12

**resort'** [1] - 61:19

**resource** [2] - 104:15, 104:19

**resources** [3] - 56:18, 62:19, 99:7

**respect** [26] - 62:15, 62:23, 67:25, 67:28, 71:25, 84:14, 88:12, 91:14, 96:25, 104:16, 107:14, 131:10, 131:29, 146:16, 148:14, 165:3, 170:18, 176:5, 176:16, 179:17, 179:18, 186:21, 191:23, 197:20, 198:8, 213:29

**respectfully** [3] - 105:26, 106:11, 231:21

**respective** [2] - 30:2

**respects** [6] - 18:13, 65:17, 94:20, 168:3, 202:6, 226:21

**respond** [4] - 12:16, 79:13, 101:17, 158:8

**respondent** [1] - 3:10

**responding** [3] - 49:16, 209:28, 219:4

**response** [50] - 29:4, 57:27, 78:26, 80:29, 81:10, 81:11, 81:20, 82:11, 82:16, 99:23, 100:22, 101:5, 102:17, 102:21, 114:8, 131:14, 156:19, 157:9, 160:24, 162:10, 164:21, 166:1,

36

37

208:27, 230:5
**scrutiny** [3] - 19:8, 19:10, 23:1
**se** [1] - 156:2
**SEAN** [1] - 2:15
**search** [5] - 9:17, 29:12, 142:23, 155:16, 210:15
**searched** [3] - 136:11, 148:9, 151:1
**searches** [13] - 13:4, 131:5, 139:10, 139:22, 142:16, 162:11, 176:12, 176:23, 176:25, 177:4, 177:11, 177:16, 191:20
**searching** [4] - 9:8, 139:3, 139:28, 147:26
**searching'** [1] - 142:15
**Second** [10] - 9:4, 29:13, 73:13, 80:7, 133:25, 142:14, 153:5, 172:16, 202:12, 217:24
**second** [9] - 13:1, 46:25, 58:1, 59:28, 113:18, 130:17, 154:13, 160:11, 185:22
**secondly** [2] - 28:22, 90:5
**secret** [15] - 30:8, 131:18, 151:28, 154:19, 165:25, 178:8, 180:28, 183:21, 194:25, 195:23, 206:1, 225:12, 225:17, 226:5, 226:18
**Secretary** [30] - 40:24, 40:26, 41:21, 42:2, 42:25, 50:17, 64:10, 76:21, 76:24, 78:10, 78:24, 81:28, 82:12, 82:13, 97:25, 98:19, 98:29, 99:3, 99:20, 99:28, 100:3, 105:8, 105:9, 106:19, 106:20, 106:21, 107:4, 116:7, 116:16
**secrets** [12] - 146:7, 153:6, 153:17, 153:25, 153:26, 154:15, 165:13, 179:25, 179:28, 180:1, 180:4, 180:10
**SECRETS** [1] - 150:8
**secrets'** [1] - 150:15

**Section** [158] - 6:21, 16:13, 19:7, 19:11, 19:12, 19:18, 19:29, 20:2, 20:3, 29:14, 47:1, 59:25, 67:8, 67:12, 68:7, 72:11, 103:28, 120:26, 125:27, 129:9, 129:24, 130:10, 130:15, 130:21, 131:1, 132:19, 132:21, 132:27, 132:29, 133:5, 133:18, 133:27, 133:28, 134:4, 134:13, 134:17, 134:19, 134:23, 134:26, 135:5, 135:27, 136:3, 136:6, 136:8, 136:22, 137:3, 137:4, 137:14, 137:25, 137:27, 139:2, 140:6, 140:17, 142:19, 142:25, 144:27, 148:10, 148:23, 149:7, 150:2, 150:13, 150:20, 151:27, 152:5, 152:15, 154:2, 154:15, 154:20, 155:5, 156:16, 158:27, 159:16, 159:18, 159:21, 159:28, 160:3, 160:4, 160:9, 160:13, 160:15, 160:20, 160:25, 160:27, 161:4, 161:5, 161:7, 161:10, 161:11, 161:18, 161:28, 162:8, 162:14, 165:9, 165:14, 165:15, 165:19, 165:23, 165:27, 165:29, 167:14, 167:16, 167:19, 167:22, 167:29, 168:7, 168:15, 168:25, 168:28, 169:11, 170:9, 170:13, 170:18, 170:25, 171:1, 171:2, 171:6, 171:29, 172:3, 172:5, 172:25, 173:4, 174:23, 174:27, 175:1, 175:10, 175:17, 175:21, 176:7, 180:6, 181:3, 181:13, 181:19, 182:11, 182:18, 182:22, 182:23,

182:25, 191:1, 191:6, 191:12, 191:18, 192:2, 193:4, 193:7, 193:9, 193:19, 193:27, 193:29, 194:22, 197:28, 206:5, 206:21, 206:28, 207:19, 223:13, 223:25
**section** [43] - 21:28, 39:3, 54:1, 63:2, 63:12, 63:27, 69:23, 83:22, 85:20, 93:29, 95:12, 102:15, 112:10, 119:20, 120:15, 120:22, 120:27, 121:8, 121:12, 121:17, 122:7, 125:1, 125:14, 125:21, 125:23, 133:14, 149:2, 149:10, 164:17, 168:12, 173:25, 175:3, 175:27, 184:4, 191:2, 191:10, 192:4, 192:23, 193:22, 204:9, 220:9, 220:13, 221:12
**Sections** [2] - 44:16, 192:15
**sections** [6] - 67:7, 121:15, 190:28, 191:3, 191:11, 218:21
**sector** [6] - 55:1, 56:20, 173:20, 173:26, 222:25, 223:23
**security** [52] - 7:21, 42:21, 45:20, 46:22, 51:27, 53:28, 63:29, 64:7, 64:13, 64:29, 65:9, 67:22, 68:25, 74:11, 79:16, 88:9, 95:24, 96:22, 100:16, 101:16, 101:26, 119:23, 119:27, 141:9, 143:23, 146:8, 147:13, 149:24, 153:12, 173:16, 173:26, 173:28, 176:1, 181:3, 186:6, 186:24, 186:25, 189:25, 199:28, 215:21, 216:1, 216:14, 216:18, 217:15, 218:8, 222:21, 225:14, 225:18, 229:25, 230:26, 230:28, 231:25

**Security** [15] - 5:23, 13:23, 14:22, 21:25, 31:1, 51:26, 67:2, 126:8, 126:14, 129:6, 153:29, 154:4, 195:13, 206:26, 214:4
**see** [24] - 23:7, 30:4, 32:2, 38:19, 38:21, 54:19, 54:23, 57:23, 74:19, 75:22, 77:9, 77:10, 77:15, 78:16, 94:24, 117:15, 117:26, 128:22, 138:14, 154:4, 218:22, 219:20, 221:15, 228:16
**seeing** [2] - 222:12, 222:15
**seek** [11] - 8:21, 23:27, 52:25, 66:27, 70:1, 73:15, 73:27, 74:2, 84:13, 93:7, 197:10
**seeking** [6] - 129:11, 140:3, 155:22, 210:23, 210:27, 215:2
**seeks** [2] - 124:23, 150:1
**seem** [3] - 22:25, 112:3, 183:13
**seemingly** [1] - 212:11
**seize** [2] - 9:6, 29:12
**seized** [2] - 7:1, 151:1
**seized'** [1] - 12:24
**seizing** [1] - 9:8
**seizures** [3] - 13:4, 176:12, 176:23
**selection** [2] - 142:22, 148:3
**Selectors** [1] - 139:13
**selectors** [9] - 139:16, 142:25, 142:27, 142:29, 162:2, 162:4, 171:11, 171:17, 172:19
**selectors'** [1] - 171:14
**self** [16] - 33:4, 34:20, 41:16, 49:4, 49:11, 49:24, 50:8, 54:6, 56:1, 56:5, 57:21, 62:15, 66:26, 85:27, 88:11, 96:29
**self-certification** [4] - 33:4, 34:20, 49:11, 56:5
**self-certified** [11] -

41:16, 49:4, 49:24, 54:6, 56:1, 57:21, 62:15, 66:26, 85:27, 88:11, 96:29
**self-certifying** [1] - 50:8
**Senate** [4] - 71:8, 71:29, 141:17, 164:24
**send** [1] - 162:4
**sends** [1] - 171:12
**senior** [2] - 129:4, 222:21
**Senior** [4] - 76:23, 98:20, 99:11, 100:15
**sense** [9] - 17:14, 20:21, 35:25, 45:2, 60:7, 77:19, 93:11, 99:29, 122:4
**sensible** [1] - 220:25
**sensitive** [2] - 18:25, 18:27
**sent** [4] - 6:7, 10:14, 71:1, 162:1
**separate** [4] - 8:29, 177:25, 211:17, 212:1
**Separately** [1] - 176:16
**separation** [2] - 20:7, 25:2
**September** [1] - 110:24
**sequence** [1] - 57:15
**series** [4] - 13:22, 16:20, 35:18, 105:29
**seriously** [1] - 59:23
**servant** [1] - 100:2
**serve** [2] - 99:11, 178:2
**served** [1] - 120:12
**server** [1] - 167:7
**servers** [1] - 9:23
**Servers** [1] - 161:15
**serves** [6] - 51:23, 98:20, 116:6, 161:29, 192:11, 226:8
**service** [10] - 19:20, 54:26, 54:27, 54:29, 132:26, 138:25, 171:15, 205:15, 223:2, 228:28
**services** [3] - 79:16, 101:26, 147:7
**Services** [4] - 1:22, 3:9, 3:10, 230:18
**SERVICES** [1] - 1:32
**serving** [1] - 161:25
**Serwin** [7] - 30:16, 32:2, 181:23, 181:29, 185:16, 186:3, 219:7
**Serwin's** [2] - 185:7,

38

185:11

**set** [39] - 14:27, 16:17, 26:24, 27:21, 33:21, 34:15, 34:21, 35:4, 35:18, 40:17, 41:4, 41:7, 44:17, 45:3, 45:12, 47:17, 49:12, 50:16, 54:3, 57:17, 61:2, 61:29, 69:13, 76:20, 85:2, 98:26, 102:9, 106:8, 110:2, 120:21, 128:28, 162:13, 164:4, 186:11, 187:17, 188:7, 195:12, 229:1

**sets** [25] - 14:8, 14:12, 39:4, 40:27, 41:22, 43:7, 61:28, 93:17, 94:28, 102:7, 119:20, 129:18, 186:13, 186:15, 188:11, 189:17, 190:17, 200:26, 211:23, 215:18, 220:28, 221:10, 224:16, 224:22, 227:29

**setting** [3] - 118:27, 122:8, 186:19

**settlement** [1] - 51:5

**seven** [3] - 220:13, 220:17, 227:29

**Seventh** [1] - 213:15

**seventh** [1] - 62:22

**several** [5] - 172:19, 175:22, 176:19, 180:16, 208:2

**Several** [1] - 67:2

**severely** [1] - 157:5

**sexual** [1] - 146:4

**shall** [14] - 44:19, 45:9, 45:17, 108:18, 109:7, 111:26, 121:21, 146:1, 146:10, 146:12, 147:4, 174:8, 198:18, 204:7

**shaped** [1] - 224:13

**share** [4] - 18:27, 113:2, 113:12, 195:27

**shared** [2] - 201:21, 208:3

**shares** [1] - 89:20

**sharing** [6] - 113:4, 197:11, 197:15, 226:12, 230:28, 230:29

**Shaw** [1] - 205:28

**shed** [1] - 215:1

**shield** [3] - 37:19, 120:4, 153:18

**Shield** [144] - 5:11, 32:23, 34:12, 34:17, 35:24, 35:28, 36:6, 36:23, 36:26, 37:11, 38:11, 38:26, 39:11, 40:13, 40:15, 41:13, 41:23, 42:12, 42:20, 43:28, 44:1, 44:16, 44:23, 46:23, 46:27, 47:5, 49:4, 49:10, 50:1, 50:9, 54:3, 54:7, 54:14, 55:4, 55:25, 57:8, 60:4, 60:18, 61:4, 61:12, 61:23, 62:3, 63:14, 64:6, 64:13, 64:29, 66:26, 67:5, 68:28, 78:9, 78:13, 78:21, 79:5, 79:12, 79:19, 80:1, 80:8, 80:20, 81:16, 81:22, 82:8, 82:14, 83:8, 85:22, 85:28, 88:9, 90:15, 90:29, 91:11, 91:24, 92:18, 92:25, 93:23, 93:25, 94:7, 94:17, 94:25, 95:7, 95:18, 96:4, 96:23, 97:2, 98:12, 98:25, 99:12, 99:15, 100:18, 101:2, 101:9, 102:15, 102:20, 103:12, 103:26, 104:1, 104:10, 104:18, 105:27, 106:13, 106:18, 107:18, 107:19, 107:27, 108:2, 108:3, 108:5, 108:10, 108:18, 108:21, 109:4, 109:17, 109:20, 109:24, 109:28, 111:4, 112:6, 112:8, 113:9, 113:15, 114:6, 114:21, 114:27, 115:1, 115:16, 116:23, 117:6, 117:21, 122:2, 122:22, 126:26, 144:21, 150:6, 156:27, 157:2, 157:3, 158:9, 163:6, 184:16, 184:23, 227:4, 229:17, 229:21, 230:3, 231:7, 231:11

**Shield"** [1] - 184:11

**Shield'** [1] - 48:25

**short** [9] - 39:9, 107:24, 111:17,

111:18, 128:27, 148:8, 158:15, 185:22, 219:18

**Short** [1] - 185:10

**show** [7] - 28:14, 29:10, 76:15, 137:24, 152:5, 216:27, 217:1

**showing** [5] - 74:25, 84:3, 131:28, 160:2, 213:12

**shown** [5] - 27:11, 69:2, 181:26, 194:6, 226:14

**shows** [1] - 64:26

**sides** [1] - 59:12

**sign** [8] - 35:24, 35:25, 35:29, 36:1, 36:2, 54:24, 91:10, 91:12

**signal** [1] - 98:23

**signals** [11] - 41:23, 76:26, 80:5, 98:15, 146:1, 146:11, 146:19, 147:3, 148:1, 174:13, 175:4

**Signals** [2] - 140:23, 146:10

**signed** [4] - 33:26, 35:27, 45:3, 197:4

**significance** [4] - 166:9, 173:3, 174:13, 203:29

**Significance** [1] - 181:12

**significant** [26] - 21:5, 31:15, 82:1, 105:23, 106:5, 117:3, 119:27, 123:8, 125:9, 129:23, 130:17, 148:14, 155:20, 160:23, 160:26, 163:26, 165:2, 169:4, 173:9, 175:22, 180:16, 190:1, 216:25, 226:1, 226:21, 229:23

**Significantly** [1] - 135:19

**significantly** [6] - 7:14, 31:24, 41:20, 65:6, 76:27, 132:14

**silent** [1] - 115:1

**similar** [5] - 7:18, 23:18, 42:15, 156:18, 228:29

**Similarly** [1] - 148:24

**similarly** [2] - 149:4, 161:23

**simplification** [1] - 84:8

**simply** [10] - 15:18, 22:21, 32:14, 77:17, 87:11, 103:19, 158:1, 166:23, 185:13, 219:26

**single** [3] - 135:6, 136:14, 144:10

**SIR** [1] - 2:22

**sister** [1] - 7:22

**situation** [2] - 189:27, 231:10

**situations** [1] - 196:11

**six** [9] - 22:9, 71:7, 93:29, 104:25, 147:5, 164:4, 175:5, 206:18, 222:22

**six-year** [1] - 71:7

**sixth** [1] - 61:19

**skip** [1] - 221:12

**skipped..** [1] - 76:11

**slide** [1] - 138:27

**slides** [2] - 9:28, 138:15

**slight** [1] - 75:19

**slightly** [2] - 26:10, 129:27

**small** [1] - 160:4

**SMITH** [1] - 2:25

**Snowden** [6] - 9:27, 27:17, 138:16, 138:24, 145:6, 223:8

**so-called** [4] - 67:1, 119:14, 119:16, 130:29

**society** [1] - 231:23

**soft** [1] - 22:1

**Software** [1] - 2:25

**soil** [4] - 129:29, 131:27, 132:28, 166:17

**sole** [3] - 12:11, 151:3, 223:22

**solely** [4] - 29:6, 49:27, 68:14, 120:9

**SOLICITORS** [2] - 2:6, 2:26

**solicitors** [2] - 187:24, 221:4

**solved** [1] - 109:16

**sometimes** [6] - 21:4, 38:1, 38:21, 80:11, 142:3, 212:24

**somewhat** [1] - 47:15

**somewhere** [1] - 80:26

**soon** [1] - 31:13

**sorry** [45] - 10:24, 21:27, 28:25, 39:16,

39:17, 40:4, 41:20, 43:24, 48:7, 75:7, 75:16, 75:22, 76:10, 86:7, 86:22, 97:25, 98:6, 100:5, 100:7, 106:16, 106:29, 107:8, 107:10, 107:12, 111:9, 111:13, 111:17, 117:4, 117:8, 117:12, 117:14, 117:16, 122:25, 124:17, 124:28, 148:26, 161:9, 178:16, 179:9, 184:22, 186:1, 188:13, 189:16, 201:1, 221:28

**Sorry** [1] - 76:11

**sort** [6] - 42:11, 63:19, 77:14, 106:9, 118:28, 169:17

**sought** [4] - 7:11, 153:17, 156:21, 185:14

**source** [1] - 20:22

**sources** [1] - 146:14

**SOUTH** [1] - 2:11

**sovereign** [6] - 193:20, 202:19, 203:1, 203:25, 204:3, 206:29

**speaking** [1] - 118:26

**Special** [1] - 223:6

**special** [2] - 25:16, 84:23

**specific** [27] - 10:29, 26:25, 27:12, 27:14, 31:21, 52:15, 52:22, 57:15, 62:4, 66:15, 85:10, 103:27, 108:16, 113:23, 132:1, 134:27, 142:21, 143:25, 148:3, 153:11, 157:19, 165:22, 175:5, 184:19, 195:14, 212:25, 214:5

**specifically** [6] - 34:15, 43:3, 85:19, 121:18, 208:5, 212:6

**Specifically** [2] - 17:4, 133:8

**specificity** [1] - 49:14

**specified** [3] - 53:22, 96:1, 96:2

**speculate** [1] - 127:3

**speculation** [1] - 16:23

39

**Speculative** [1] - 217:2

**speculative** [2] - 212:10, 212:12

**spend** [1] - 39:6

**spirit** [1] - 224:6

**splintered** [1] - 8:26

**split** [3] - 8:14, 207:12, 209:24

**splits** [1] - 190:1

**spoken** [2] - 118:2, 122:5

**Spokeo** [13] - 26:27, 27:26, 27:29, 28:2, 28:7, 28:13, 28:15, 28:19, 30:15, 30:22, 212:18, 214:12, 217:11

**Spokeo's** [1] - 30:20

**SQUARE** [1] - 2:27

**staff** [3] - 70:15, 78:11, 99:6

**stage** [14] - 10:10, 11:10, 12:6, 15:17, 15:20, 16:2, 22:15, 22:20, 23:9, 25:26, 32:13, 34:2, 165:17, 213:16

**stages** [2] - 15:16, 30:4

**stake** [1] - 58:13

**Standard** [15] - 90:1, 90:27, 91:20, 92:1, 92:5, 92:19, 92:21, 93:3, 100:18, 109:22, 112:17, 113:11, 229:13, 230:10, 231:22

**standard** [9] - 7:20, 15:2, 15:3, 27:15, 69:13, 134:18, 174:6, 222:25, 228:7

**standards** [4] - 30:5, 88:19, 131:1, 226:16

**standards'** [1] - 226:9

**STANDING** [1] - 150:8

**standing** [106] - 5:10, 6:3, 6:8, 7:4, 7:23, 7:25, 8:14, 8:20, 12:25, 13:2, 13:5, 13:13, 14:4, 14:5, 14:19, 15:4, 15:12, 16:1, 16:3, 16:5, 16:21, 18:9, 19:6, 20:2, 20:5, 20:13, 20:19, 20:29, 21:20, 22:8, 23:11, 23:27, 24:1, 24:9, 24:15,

24:18, 24:20, 25:1, 25:11, 25:16, 25:22, 26:5, 26:9, 26:11, 26:21, 27:4, 27:10, 27:19, 28:2, 28:10, 28:15, 28:20, 28:22, 29:16, 29:22, 29:27, 30:5, 30:10, 30:12, 30:18, 30:20, 31:9, 31:17, 31:20, 31:26, 32:3, 32:17, 32:21, 112:10, 151:9, 151:17, 151:24, 152:2, 152:4, 152:17, 153:1, 154:15, 154:18, 165:12, 165:25, 183:6, 183:24, 184:5, 184:8, 189:28, 204:11, 211:17, 211:20, 212:10, 212:14, 212:23, 213:4, 213:8, 213:10, 213:12, 213:17, 213:22, 214:1, 214:9, 214:10, 214:18, 214:19, 214:24, 214:27, 216:27

**standing'** [1] - 8:19

**standing'..** [1] - 76:15

**stands** [1] - 10:25

**start** [6] - 106:14, 125:16, 128:15, 159:12, 219:8, 220:9

**started** [2] - 22:2, 208:16

**starting** [2] - 199:24, 215:23

**starts** [5] - 38:12, 39:1, 39:3, 112:11, 191:1

**state** [23] - 7:13, 18:3, 23:4, 25:15, 26:22, 102:3, 142:6, 153:17, 153:24, 153:26, 154:15, 154:19, 165:12, 165:25, 179:17, 179:28, 180:1, 180:4, 180:10, 196:21, 209:25, 227:23, 227:24

**State** [34] - 41:21, 42:2, 44:19, 59:6, 64:11, 76:21, 76:25, 78:24, 79:23, 82:12, 97:25, 98:19, 99:12, 99:20, 99:28, 99:29, 100:3, 105:8, 105:9,

105:10, 106:19, 106:20, 106:21, 107:4, 111:29, 116:1, 116:7, 116:9, 116:16, 116:19, 116:24, 120:12, 158:11, 226:28

**STATE** [1] - 150:8

**Statement** [1] - 11:17

**statement** [5] - 11:21, 107:22, 107:24, 121:28, 229:15

**Statements** [1] - 55:18

**statements** [2] - 24:16, 55:12

**STATES** [1] - 2:19

**states** [81] - 29:5, 29:19, 30:18, 51:12, 67:24, 74:6, 112:20, 112:29, 113:21, 113:28, 114:12, 114:17, 115:10, 116:1, 116:5, 116:9, 159:18, 159:21, 159:26, 160:1, 160:13, 160:15, 160:20, 160:25, 161:5, 161:6, 161:18, 161:21, 162:10, 162:14, 162:18, 162:23, 163:2, 163:10, 163:22, 163:24, 164:8, 164:10, 164:22, 164:29, 165:12, 165:15, 166:3, 166:21, 166:23, 167:15, 167:19, 167:22, 168:25, 170:18, 171:2, 171:11, 171:26, 172:24, 173:7, 173:13, 173:21, 173:25, 174:5, 174:7, 174:18, 174:29, 175:15, 175:24, 176:11, 176:22, 176:28, 178:4, 178:14, 178:17, 178:26, 179:25, 179:27, 180:4, 180:15, 181:8, 181:23, 183:2, 183:9, 183:18, 184:17

**States** [112] - 5:16, 5:26, 13:18, 34:7, 40:10, 40:12, 44:1,

44:8, 44:12, 44:15, 44:24, 45:8, 45:10, 45:17, 45:27, 47:6, 47:10, 49:2, 49:5, 50:3, 54:22, 56:14, 58:3, 60:13, 66:19, 66:25, 68:24, 68:27, 69:27, 69:29, 79:15, 83:4, 83:8, 83:14, 84:8, 85:25, 85:28, 88:9, 88:24, 88:29, 94:7, 95:22, 101:25, 103:5, 105:28, 110:12, 118:3, 118:15, 118:17, 119:24, 119:25, 119:29, 120:3, 120:5, 120:19, 120:25, 120:27, 121:4, 121:23, 122:13, 125:20, 126:24, 132:26, 133:7, 133:23, 134:25, 136:18, 139:4, 139:7, 140:1, 140:19, 141:3, 143:24, 144:23, 149:25, 155:10, 157:1, 159:20, 166:19, 166:25, 176:29, 177:2, 177:6, 182:24, 186:20, 187:4, 189:22, 190:15, 191:15, 192:17, 192:27, 192:29, 193:21, 197:7, 197:11, 200:29, 201:20, 201:22, 202:16, 202:26, 206:8, 206:12, 206:15, 212:3, 226:13, 226:22, 226:25, 228:14, 229:26, 230:15, 230:23

**States'** [3] - 130:14, 144:25, 155:5

**States..** [1] - 191:21

**statistic** [1] - 172:12

**statistics** [3] - 173:21, 173:22, 173:26

**statute** [20] - 6:22, 27:1, 28:9, 103:29, 131:18, 132:15, 132:22, 133:14, 133:20, 133:29, 135:10, 135:12, 136:6, 137:28, 141:16, 208:6, 209:17, 209:19,

218:15

**statute's** [1] - 135:14

**Statutes** [1] - 102:24

**statutes** [3] - 72:2, 157:11, 203:25

**statutorily** [3] - 70:24, 151:7, 214:11

**statutory** [23] - 45:11, 53:16, 74:28, 80:25, 84:23, 85:16, 151:10, 164:29, 190:28, 202:20, 203:16, 207:4, 212:26, 214:1, 214:2, 214:16, 215:3, 215:11, 215:28, 217:8, 217:10, 218:1, 225:26

**stay** [3] - 89:9, 192:6, 192:8

**Stellar** [3] - 167:21, 167:25, 168:5

**stemming** [1] - 47:22

**stenographers** [1] - 66:3

**stenographic** [1] - 1:25

**Stenography** [3] - 1:21, 3:9, 3:10

**STENOGRAPHY** [1] - 1:31

**step** [1] - 81:7

**steps** [2] - 62:11, 66:18

**stick** [1] - 21:14

**sticky** [1] - 98:2

**still** [22] - 28:13, 51:13, 51:19, 89:15, 89:18, 90:18, 90:21, 91:4, 94:8, 110:26, 110:27, 111:21, 122:3, 125:6, 125:10, 182:27, 202:11, 203:20, 212:26, 215:4, 217:9

**stolen** [1] - 213:7

**stop** [2] - 62:9, 126:4

**storage** [3] - 67:23, 69:19, 205:12

**store** [1] - 9:6

**stored** [8] - 6:6, 9:22, 87:10, 87:14, 136:17, 162:20, 204:23, 204:28

**Stored** [3] - 191:2, 204:18, 227:9

**storing** [2] - 5:25, 13:26

**STREET** [2] - 2:12, 2:17

40

strengthened [1] - 65:6

strengthening [1] - 48:11

strengthens [1] - 94:20

stressed [2] - 75:4, 76:2

strict [2] - 167:29, 202:14

stricter [5] - 28:1, 30:19, 108:21, 168:3, 226:22

strictly [8] - 45:22, 68:28, 69:18, 88:13, 97:15, 118:26, 202:20, 215:27

striking [1] - 7:16

strong [2] - 160:29, 230:20

structure [2] - 38:28, 190:15

structure' [1] - 78:29

sub [2] - 51:28, 51:29

sub-processing [1] - 51:28

sub-processor [1] - 51:29

subject [41] - 29:14, 30:8, 53:14, 55:13, 61:5, 61:22, 70:5, 74:10, 85:11, 86:13, 87:26, 90:3, 96:11, 102:18, 103:18, 113:22, 113:28, 113:29, 114:7, 118:16, 123:25, 133:2, 133:26, 136:18, 141:12, 150:20, 152:25, 153:20, 157:18, 158:26, 159:9, 160:27, 163:25, 183:4, 183:21, 184:18, 186:29, 188:1, 194:21, 197:23, 208:1

subjected [1] - 193:11

subjects [20] - 46:26, 46:29, 50:29, 51:15, 52:3, 53:7, 55:29, 57:19, 67:5, 70:1, 72:22, 73:14, 74:8, 76:10, 76:18, 96:25, 96:27, 109:27, 142:19, 183:10

submission [2] - 54:15, 125:14

SUBMISSION [1] - 4:5

submissions [3] - 21:15, 54:11, 117:20

submit [3] - 59:20, 79:18, 98:14

submits [1] - 134:19

submitted [3] - 101:24, 101:28, 134:7

submitting [7] - 101:5, 101:21, 102:10, 102:17, 102:21, 103:19, 104:5

subpoena [2] - 210:14, 210:17

subpoenas [1] - 85:10

subscribed [1] - 42:12

Subsection [2] - 198:23, 198:27

subsection [3] - 198:27, 200:22, 200:23

subsections [3] - 197:29, 198:13, 199:3

subsequent [2] - 69:10, 107:19

subsequently [6] - 51:24, 67:4, 169:28, 170:7, 185:22, 187:22

substance [2] - 15:26, 119:8

substantial [5] - 8:12, 26:15, 139:27, 166:4, 177:1

substantial' [1] - 166:2

substantially [3] - 5:26, 6:6, 10:14

substantive [2] - 63:7, 182:8

succeeded [2] - 140:8, 156:14

success [1] - 8:13

success' [1] - 7:29

successive [2] - 15:16, 16:2

such' [1] - 63:4

sue [7] - 13:2, 13:5, 29:27, 151:9, 203:2, 203:4, 215:20

suffered [4] - 27:7, 32:10, 76:4, 213:7

suffering [1] - 73:27

suffers [1] - 209:18

suffice [1] - 217:3

suffice' [1] - 15:22

sufficiency [1] - 12:12

sufficient [7] - 12:24, 65:2, 151:18, 152:6, 213:8, 214:8, 214:19

sufficiently [3] - 6:3, 6:7, 58:7

suggested [1] - 31:20

suggests [1] - 175:27

suit [14] - 6:4, 28:8, 30:25, 113:10, 152:16, 190:13, 192:13, 196:12, 197:13, 198:16, 203:6, 211:20, 215:26, 216:9

SUITE [1] - 3:3

suits [4] - 27:17, 153:5, 199:5, 209:17

sum [2] - 130:21, 198:18

summarised [2] - 97:21, 216:27

summarises [7] - 24:11, 50:23, 66:6, 211:25, 211:28, 212:19, 225:5

summary [31] - 7:7, 7:27, 8:2, 14:11, 15:6, 15:17, 15:26, 21:2, 21:22, 22:28, 23:13, 25:29, 26:4, 26:22, 32:17, 32:18, 43:9, 47:29, 50:25, 111:17, 111:18, 127:6, 158:23, 189:15, 220:9, 220:12, 225:3, 227:29, 228:2, 231:14, 231:27

summons [1] - 210:14

supersede [1] - 51:16

supervised [2] - 171:3, 171:13

supervising [2] - 170:28, 171:8

supervision [2] - 45:13, 226:17

supervisory [5] - 24:3, 79:15, 89:1, 101:25, 111:27

supplement [2] - 187:25, 226:2

supplemental [2] - 188:3, 219:2

Supplemental [1] - 189:11

supplied [1] - 3:9

support [11] - 6:3, 6:8, 8:6, 12:2, 18:4, 31:14, 79:29, 212:6, 212:7, 212:13, 229:18

Support [1] - 121:5

supported [5] - 7:10, 10:15, 15:13, 70:14, 71:24

supporting [1] - 12:17

supports [2] - 9:1, 230:13

suppose [3] - 20:23, 138:18, 178:10

supposed [1] - 135:14

supposing [3] - 87:8, 90:28, 93:1

suppositions [1] - 16:22

suppress [5] - 181:25, 182:1, 182:8, 182:13, 194:5

suppressing [1] - 146:2

suppression [1] - 180:17

Suppression [1] - 181:13

Supreme [23] - 6:25, 15:11, 19:2, 22:27, 24:28, 25:10, 26:28, 28:1, 29:28, 152:2, 155:14, 176:17, 176:28, 177:3, 177:14, 177:21, 177:23, 196:20, 203:27, 212:29, 214:12, 214:29, 217:7

surprising [1] - 7:1

surreptitious [1] - 144:11

surveillance [196] - 5:22, 7:22, 8:28, 14:2, 16:13, 16:14, 16:18, 16:24, 17:3, 17:4, 17:5, 17:8, 17:12, 17:17, 17:23, 17:24, 18:22, 19:8, 19:9, 19:11, 19:13, 19:15, 19:18, 19:19, 19:21, 19:29, 27:18, 29:15, 30:8, 32:7, 34:24, 67:18, 69:3, 72:13, 73:5, 74:11, 74:16, 78:20, 80:16, 82:21, 82:28, 101:8, 103:14, 103:18, 113:5, 113:23, 113:29, 114:7, 114:14, 114:18, 129:9, 129:16, 129:23, 129:28, 130:2, 130:3, 130:7, 130:9, 130:11, 130:19, 130:29, 131:7, 131:11, 131:15, 131:17, 131:21, 131:26, 131:29, 132:3, 132:5, 132:8, 132:27, 132:28, 133:1, 133:12, 133:18, 133:25, 133:27, 133:28, 134:3, 134:10, 134:17, 134:20, 134:29, 135:1, 136:1, 136:8, 137:26, 137:27, 137:29, 138:3, 139:1, 139:6, 139:15, 139:20, 139:26, 139:27, 140:15, 140:17, 140:18, 141:5, 141:11, 141:13, 141:24, 141:26, 141:27, 142:2, 142:18, 142:21, 142:26, 143:6, 145:14, 146:27, 147:22, 147:26, 148:10, 150:2, 150:12, 150:17, 150:21, 150:23, 150:29, 151:2, 151:27, 152:15, 152:26, 153:8, 154:2, 154:14, 154:21, 154:23, 155:1, 155:22, 156:10, 156:15, 156:22, 157:18, 157:29, 158:1, 158:23, 158:27, 159:1, 159:13, 162:11, 162:16, 162:18, 162:25, 165:1, 166:9, 170:17, 173:4, 173:24, 176:17, 178:6, 178:19, 178:21, 178:27, 179:4, 180:28, 180:29, 181:2, 181:5, 181:6, 181:19, 181:26, 181:27, 182:20, 182:22, 183:4, 183:22, 183:29, 184:19, 190:24, 190:25, 191:15, 193:11, 193:12, 194:2, 194:6, 194:8, 222:9, 223:26,

41

**topic** [3] - 125:26, 160:11, 177:25
**topical** [1] - 118:12
**tort** [1] - 62:26
**Tort** [1] - 206:14
**torture** [1] - 153:24
**total** [1] - 160:3
**Totten** [8] - 178:13, 178:18, 178:23, 178:29, 179:3, 179:5, 179:10, 179:15
**touchpoint** [1] - 200:1
**to·** [1] - 210:18
**trace** [3] - 43:19, 191:24, 192:27
**traceability** [1] - 6:27
**traceable** [1] - 24:22
**tracks** [1] - 38:4
**Trade** [8] - 40:27, 42:6, 42:8, 42:15, 50:18, 60:13, 61:6, 230:18
**trade** [3] - 42:11, 146:7, 206:1
**traditional** [3] - 133:5, 133:25, 134:16
**traditionally** [2] - 133:1, 134:14
**transactions** [5] - 162:19, 168:19, 169:14, 169:26, 169:28
**transatlantic** [2] - 144:24, 163:8
**transcendent** [1] - 182:9
**transcript** [1] - 1:24
**Transcripts** [1] - 3:8
**transfer** [14] - 33:13, 33:27, 53:21, 91:13, 92:8, 92:10, 93:15, 100:20, 100:26, 100:27, 109:21, 211:9, 230:2, 230:8
**Transfer** [2] - 50:7, 53:20
**transferred** [32] - 32:26, 40:11, 43:28, 43:29, 44:26, 46:23, 49:3, 63:13, 63:17, 64:5, 64:28, 66:24, 67:5, 68:26, 69:20, 69:29, 77:29, 83:7, 85:26, 88:8, 96:23, 108:13, 108:20, 109:12, 109:20, 136:17, 163:13, 176:24, 202:1, 202:21, 228:19,

231:20
**transferring** [2] - 32:28, 211:10
**transfers** [24] - 33:2, 33:19, 35:22, 35:23, 35:29, 36:4, 36:8, 49:22, 53:19, 92:3, 92:11, 92:12, 92:16, 92:17, 93:16, 93:22, 93:24, 96:11, 228:8, 229:9, 229:15, 230:21, 231:22
**Transit** [4] - 163:18, 166:28, 167:2, 167:6
**transit** [4] - 139:18, 144:23, 163:7, 166:16
**transition** [1] - 50:12
**translate** [1] - 182:12
**transmission** [4] - 204:20, 204:23, 204:27, 209:5
**transmit** [1] - 79:23
**transmits** [1] - 162:4
**transmitted** [3] - 100:17, 102:3, 139:29
**transnational** [1] - 147:16
**transparency** [11] - 86:8, 156:3, 160:22, 171:19, 171:23, 171:27, 172:1, 173:20, 225:9, 225:17, 225:29
**Transparency** [1] - 54:2
**Transportation** [5] - 42:26, 42:27, 50:19, 53:15, 55:14
**transpose** [1] - 66:15
**trap** [3] - 43:19, 191:24, 192:27
**travels** [1] - 144:13
**treated** [3] - 67:28, 78:5, 146:15
**treating** [1] - 67:25
**treats** [1] - 26:9
**treaty** [1] - 230:27
**triable** [1] - 7:9
**trial** [5] - 22:14, 151:5, 165:24, 181:8, 185:10
**Trial** [1] - 128:26
**tried** [1] - 168:22
**trigger** [2] - 114:19, 114:29
**trillion** [1] - 152:25
**trivial** [2] - 26:29, 27:2
**true** [4] - 22:26, 26:2, 28:15, 151:16

**Trump** [1] - 125:25
**Trump's** [1] - 118:13
**truth** [1] - 22:20
**try** [2] - 159:8, 191:11
**trying** [3] - 100:10, 116:28, 222:15
**turn** [8] - 10:3, 27:13, 40:21, 79:26, 177:25, 184:4, 189:15, 221:10
**turns** [8] - 194:11, 197:2, 204:12, 207:24, 210:3, 211:17, 212:18, 213:2
**two** [41] - 5:8, 17:19, 25:6, 33:21, 36:21, 39:9, 42:8, 65:4, 65:22, 66:5, 103:2, 110:16, 124:26, 125:22, 129:22, 130:3, 137:17, 137:25, 142:1, 144:11, 150:4, 154:10, 159:3, 161:6, 161:10, 178:10, 184:14, 185:10, 198:1, 202:6, 204:24, 206:17, 212:29, 217:19, 218:3, 221:11, 221:13, 221:18, 222:17, 224:14, 231:12
**Two** [2] - 6:19, 214:29
**two-page** [1] - 39:9
**type** [7] - 17:22, 17:23, 34:20, 35:10, 36:13, 42:15, 183:20
**types** [5] - 137:26, 147:5, 147:25, 161:11, 208:10
**typical** [1] - 14:1
**typically** [3] - 52:20, 182:1, 208:4

## U

**U.S** [135] - 24:28, 27:17, 29:9, 29:24, 32:4, 32:9, 40:16, 41:22, 44:23, 45:19, 46:21, 46:23, 47:5, 47:23, 47:24, 48:20, 48:24, 48:25, 48:27, 49:3, 49:11, 49:24, 49:28, 52:15, 59:21, 64:5, 64:20, 65:8, 65:11, 65:19, 67:17, 79:7, 86:2, 96:21, 129:23, 129:29,

130:22, 130:23, 130:24, 130:26, 131:2, 131:7, 131:9, 131:11, 131:15, 131:26, 132:24, 132:28, 134:24, 135:21, 136:20, 136:25, 138:4, 138:9, 140:15, 140:23, 141:22, 141:28, 142:6, 143:7, 143:12, 143:13, 143:25, 143:26, 144:3, 144:6, 144:21, 144:27, 145:21, 146:1, 146:8, 146:12, 146:19, 147:2, 147:8, 147:9, 147:10, 147:14, 148:16, 148:21, 148:22, 149:5, 149:6, 149:12, 150:3, 150:5, 150:12, 151:13, 151:17, 151:28, 152:2, 152:16, 153:23, 154:21, 154:29, 155:1, 155:2, 155:4, 155:16, 155:20, 155:21, 156:2, 156:3, 156:9, 156:20, 157:2, 157:10, 158:25, 165:3, 166:16, 166:17, 166:19, 167:5, 167:8, 167:11, 167:12, 167:18, 175:3, 175:17, 175:18, 175:20, 175:29, 176:6, 190:1, 190:27, 193:1, 193:2, 212:15
**ultimate** [1] - 184:29
**ultimately** [8] - 12:23, 33:21, 105:10, 107:2, 111:3, 162:13, 185:2, 209:29
**Umbrella** [1] - 227:4
**umbrella** [2] - 33:24, 34:5
**unable** [2] - 7:2, 211:4
**unaccounted** [1] - 27:14
**unauthorised** [1] - 222:8
**unauthorized** [1] - 204:27
**unbelievable** [1] - 22:26
**uncertainty** [3] - 31:16, 31:19, 207:4

**unclear** [3] - 108:18, 122:10, 203:14
**unconstitutional** [3] - 9:22, 25:8, 169:24
**unconstrained** [1] - 11:13
**UNDER** [1] - 190:21
**Under** [20] - 40:26, 76:24, 78:10, 82:13, 98:19, 98:29, 142:22, 143:12, 148:20, 161:28, 175:3, 193:9, 205:1, 205:10, 206:5, 209:17, 211:19, 223:6, 223:17, 223:26
**under** [228] - 5:23, 6:11, 6:27, 7:12, 8:24, 11:12, 11:14, 13:19, 13:28, 13:29, 18:20, 28:8, 33:1, 33:12, 33:19, 34:16, 36:8, 36:22, 40:12, 40:28, 43:16, 43:28, 46:8, 46:23, 49:3, 49:17, 50:27, 51:8, 51:19, 51:26, 52:3, 53:4, 55:18, 57:8, 62:25, 62:26, 63:13, 64:5, 65:8, 65:14, 66:26, 67:3, 67:5, 68:27, 70:5, 72:4, 72:21, 72:26, 72:28, 73:22, 74:16, 76:23, 80:14, 83:8, 85:22, 85:28, 88:9, 92:9, 92:11, 93:15, 94:7, 96:23, 98:18, 99:3, 100:21, 102:19, 103:29, 104:15, 105:22, 108:20, 109:17, 109:20, 109:28, 118:2, 118:4, 118:6, 125:21, 126:12, 126:21, 126:24, 129:9, 130:3, 130:10, 130:21, 131:1, 132:27, 132:29, 133:1, 133:18, 133:25, 133:27, 134:13, 134:14, 136:14, 140:5, 140:13, 140:17, 140:18, 140:20, 141:11, 141:14, 142:18, 142:25, 144:5, 144:16, 145:1, 145:2, 145:17, 148:10, 148:23, 149:7, 149:18, 150:13, 151:17,

43

44

176:24, 176:25,
176:26, 177:11,
177:12, 177:17,
177:18, 180:5, 181:8,
181:20, 182:21,
184:2, 185:1, 185:15,
186:11, 186:24,
187:9, 188:7, 190:3,
190:21, 194:14,
196:20, 197:15,
197:17, 197:24,
200:16, 202:11,
202:22, 203:4,
203:27, 206:7,
208:18, 211:19,
216:4, 216:8, 216:20,
216:25, 216:26,
217:16, 217:18,
217:20, 218:18,
218:21, 218:24,
220:15, 221:3,
222:24, 222:25,
223:3, 223:4, 223:26,
224:11, 224:22,
224:24, 225:5, 225:7,
225:14, 225:22,
225:24, 226:4, 226:7,
226:8, 226:11,
226:26, 226:27,
226:29, 227:3,
227:13, 227:15,
227:17, 227:18,
227:20, 227:21,
227:24, 227:26,
228:3, 228:5, 228:9,
228:10, 228:13,
228:14, 228:17,
228:19, 228:27,
229:3, 229:8, 229:11,
230:2, 230:17,
230:21, 231:15,
231:17, 231:20
**USA** [4] - 19:26,
72:4, 152:4, 173:10
**use'** [1] - 196:1
**useful** [6] - 14:10,
20:21, 20:22, 20:29,
21:29, 38:2
**user** [2] - 138:6,
144:12
**users** [4] - 145:8,
160:5, 172:28, 173:24
**users'** [2] - 144:28,
145:1
**uses** [3] - 17:6,
137:25, 142:23
**Utah** [1] - 21:26
**utilise** [1] - 217:23

# V

**vacated** [1] - 8:10
**vagaries** [1] - 31:22
**Valdez** [1] - 21:24
**valid** [2] - 33:1, 92:11
**validity** [5] - 19:19,
36:23, 92:21, 230:8,
230:10
**value** [6] - 10:4, 11:1,
12:6, 208:28, 208:29,
209:3
**variations** [1] - 27:14
**variety** [1] - 33:4
**various** [21] - 8:3,
9:28, 14:8, 33:17,
34:21, 35:9, 35:18,
40:27, 48:23, 65:17,
70:19, 78:3, 97:20,
102:7, 108:7, 110:2,
112:24, 117:29,
140:9, 218:20, 219:27
**vary** [1] - 213:4
**vast** [5] - 139:22,
142:16, 144:6,
144:19, 158:26
**vector** [1] - 178:7
**ventilated** [1] - 93:8
**venues** [1] - 22:12
**verbatim** [1] - 1:24
**Verdugo** [2] -
155:11, 176:29
**Verdugo-Urquidez**
[2] - 155:11, 176:29
**verify** [1] - 53:12
**verifying** [2] - 58:16,
188:5
**Verizon** [1] - 139:5
**versa** [1] - 17:19
**version** [3] - 75:14,
75:17, 108:9
**versions** [2] - 137:4,
167:21
**via** [2] - 138:11,
208:3
**viable** [1] - 158:28
**vice** [1] - 17:19
**victims** [2] - 121:5
**view** [16] - 32:3,
42:22, 44:24, 46:13,
48:16, 71:10, 122:21,
123:26, 125:4, 125:7,
178:24, 187:8,
213:29, 226:4, 228:4,
231:15
**viewed** [1] - 162:23
**viewpoint** [3] - 35:1,
41:25, 90:14
**views** [4] - 31:7,

125:4, 125:11, 224:13
**VII** [3] - 40:19, 48:25,
64:21
**violate** [4] - 119:26,
120:4, 207:14, 227:8
**violated** [2] - 5:24,
157:29
**violates** [2] - 13:27,
204:21
**violation** [24] - 13:2,
26:29, 27:3, 28:3,
77:6, 82:6, 104:27,
113:11, 191:7,
192:11, 193:13,
193:16, 198:9,
198:12, 199:11,
205:4, 205:7, 206:6,
209:19, 212:26,
214:11, 215:20,
217:10, 217:14
**violation'** [1] -
212:22
**violations** [17] -
42:28, 112:22,
158:29, 178:3,
182:26, 186:21,
189:23, 193:28,
197:14, 207:6,
207:15, 207:22,
214:5, 214:16, 218:7,
226:26, 226:29
**virtually** [3] - 29:13,
143:8, 150:19
**virtue** [2] - 20:17,
68:18
**vis-à-vis** [1] - 63:22
**visas** [1] - 119:26
**visited** [1] - 152:14
**vital** [1] - 231:24
**Vladeck** [28] - 29:4,
29:19, 30:22, 31:11,
32:2, 32:12, 164:21,
164:29, 166:13,
166:23, 174:17,
174:29, 176:28,
177:14, 178:14,
178:17, 178:26,
179:27, 180:4, 182:5,
183:18, 183:27,
184:9, 185:24,
218:29, 219:4, 219:6
**Vladeck's** [1] -
177:19
**volumes** [2] - 136:7,
159:3
**voluntarily** [2] -
56:15, 62:20
**voluntary** [4] - 96:29,
177:1, 177:12, 177:18

# W

**wait** [1] - 39:20
**waived** [1] - 203:2
**waiver** [2] - 193:20,
206:29
**Walden** [1] - 207:24
**WALL** [2] - 2:31, 2:32
**warrant** [4] - 155:15,
176:14, 176:19,
210:15
**warrantless** [6] -
129:28, 130:1,
132:23, 155:22,
190:24, 214:8
**warrantlessly** [1] -
133:6
**WAS** [1] - 232:23
**ways** [4] - 149:29,
157:23, 225:15,
225:17
**weak** [2] - 136:26,
160:14
**weakened** [1] -
132:14
**weapons** [2] - 141:4,
147:12
**website** [6] - 51:4,
54:14, 54:15, 118:19,
173:18
**websites** [2] - 54:22,
152:14
**weeks** [1] - 220:22
**welcomes** [1] -
108:3
**well-being** [2] -
230:15, 231:25
**well-defined** [1] -
159:28
**well-pleaded** [1] -
22:20
**well-pled** [1] - 22:16
**Western** [1] - 5:27
**whatsoever** [1] -
90:8
**Whereas** [1] - 32:8
**whereas** [3] - 26:12,
32:8, 133:25
**whereby** [4] - 34:20,
36:9, 63:17, 124:5
**which'** [1] - 134:28
**whichever** [3] -
191:28, 193:17,
206:10
**Whilst** [1] - 187:12
**White** [1] - 223:27
**who've** [1] - 121:12
**whole** [8] - 39:5,
63:10, 79:8, 86:3,

86:10, 122:21,
122:23, 220:24
**wide** [2] - 142:24,
223:5
**wider** [2] - 17:23,
61:13
**Wikimedia** [7] -
13:17, 23:18, 31:1,
31:14, 152:13,
152:19, 152:23
**willful** [3] - 191:7,
193:28, 206:6
**willfully** [3] - 120:3,
198:9, 198:11
**willfulness** [1] - 75:1
**WILLIAM** [1] - 2:26
**Williams** [1] - 8:20
**Wilner** [1] - 156:25
**WILTON** [1] - 2:6
**win** [1] - 183:4
**Wind** [3] - 167:21,
167:26, 168:5
**Winter** [1] - 22:12
**wire** [4] - 167:17,
173:24, 204:16,
205:11
**Wire** [1] - 207:1
**Wiretap** [8] - 204:18,
204:19, 204:25,
205:1, 205:5, 206:6,
207:6, 227:10
**wiretap** [3] - 207:22,
223:28, 227:8
**wiretapping** [1] -
214:8
**wish** [6] - 14:12,
35:1, 59:5, 59:14,
98:22, 189:6
**wishes** [2] - 138:6,
220:19
**with'** [1] - 103:5
**withdraw** [1] - 124:1
**withheld** [3] -
196:19, 208:7, 208:10
**withhold** [1] - 156:5
**withholding** [2] -
196:17, 208:9
**within'** [1] - 202:2
**witness** [3] - 29:19,
164:22, 187:16
**word** [1] - 17:29
**words** [7] - 11:21,
12:21, 15:24, 92:6,
105:14, 142:19, 148:6
**workable** [1] -
109:17
**works** [2] - 39:5,
105:6
**world** [3] - 130:24,
139:10, 152:14

**World** [1] - 223:15
**worried** [1] - 122:26
**worry** [1] - 75:24
**worthy** [1] - 91:5
**WP** [1] - 109:26
**WP238** [2] - 108:5, 109:25
**WP29** [7] - 108:2, 108:6, 108:7, 108:15, 108:25, 109:15, 110:9
**writes** [1] - 115:14
**writing** [5] - 143:22, 149:24, 206:16, 210:23, 211:10
**written** [5] - 3:10, 21:15, 134:5, 210:18, 222:22
**wrong..** [1] - 73:27
**wrongful** [2] - 131:15, 206:22
**wrongly** [1] - 169:21
**wrote** [1] - 223:28
**WT29** [1] - 108:21

## Y

**Yahoo** [1] - 144:12
**Yale** [1] - 129:2
**year** [7] - 45:26, 46:5, 71:7, 135:8, 152:25, 156:29, 208:29
**yearly** [1] - 45:27
**years** [11] - 137:14, 137:17, 143:15, 149:20, 153:16, 206:17, 222:20, 223:13, 223:25, 228:10
**yellow** [1] - 98:1
**yesterday** [15] - 19:24, 26:28, 34:11, 43:5, 43:17, 66:8, 72:8, 72:15, 73:8, 73:20, 74:29, 117:28, 118:7, 118:9, 200:27
**York** [1] - 186:7
**young** [1] - 100:7
**yourself** [2] - 14:12, 138:20

## –

**–** [1] - 229:19

## —

**—** [12] - 9:10, 22:24,

25:2, 27:13, 69:4, 69:5, 82:4, 82:5, 126:21, 178:6, 182:9
**—so** [1] - 22:23

46