Neutral Citation Number: [2021] EWHC 2904 (Comm)

Case No: CL-2020-000561

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
COMMERCIAL COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 01/11/2021

Before :

Peter MacDonald Eggers QC
(sitting as a Deputy Judge of the High Court)

- -

Between :

(1) VARIOUS AIRFINANCE LEASING COMPANIES (listed at Schedule A to the Claim Form)	**Claimants**
(2) ALIF SEGREGATED PORTFOLIO COMPANY (for and on behalf of itself and each of ALIF Segregated Portfolio Company 2, ALIF Segregated Portfolio Company 4 and ALIF Segregated Portfolio Company 5)	
- and -	
SAUDI ARABIAN AIRLINES CORPORATION	**Defendant**
- and -	
INTERNATIONAL AIR FINANCE CORPORATION	**Third Party**

- -
- -

Tom Sprange QC and Kabir Bhalla (of **King & Spalding International LLP)** for the **Claimants and Third Party**
Giles Robertson (instructed by **Norton Rose Fulbright LLP**) for the **Defendant**

Hearing dates: 07 October 2021

- -

Approved Judgment

I direct that no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

.....

PETER MACDONALD EGGERS QC SITTING AS A DEPUTY JUDGE OF THE HIGH COURT

"Covid-19 Protocol: This judgment will be handed down by the judge remotely by circulation to the parties' representatives by email and release to Bailii. The date and time for hand-down will be deemed to be 10:30 am on 1 November 2021. A copy of the judgment in final form as handed down can be made available after that time, on request by email to the judge's Clerk"

Peter MacDonald Eggers QC :

Introduction

1. The Claimants and the Third Party ("the IAFC Parties") apply for an order for disclosure by the Defendant ("Saudia") in an action concerning a dispute relating to Lease Agreements over 50 Airbus aircraft. Originally, the leases were between the Third Party as Lessor and Saudia as Lessee. The First Claimants are the current Lessors of the aircraft (to whom the leases were novated by the Third Party) and the Second Claimants are suing in their representative capacity as the parent portfolio company of the Lessors.

2. The parties' dispute centres around the escalation factors which influence the Basic Rent payable under the Lease Agreements. This dispute translates into a difference between the parties whereby the IAFC Parties allege that Saudia has underpaid some US$38.7 million and Saudia alleges that it has overpaid some US$21.9 million under the Lease Agreements.

3. The dispute between the parties extends to questions of interpretation of the Lease Agreements and estoppels allegedly based on statements or assumptions which were communicated between the parties.

4. The IAFC Parties seek disclosure by Saudia in respect of the data held on personal devices, in particular mobile telephones, owned or used by:

   (1) Mr Saleh Al Jasser who is now the non-executive Chairman of Saudia's board of directors and had been Director General of Saudia when the Lease Agreements were concluded. Since October 2019, Mr Al Jasser has been and is currently the Transport Minister of the Kingdom of Saudi Arabia.

   (2) Mr Abdulrahmen Altayeb who had been Vice President of Fleet Management and Engineering of Saudia from 2014 to 2017 and Vice President of Corporate Communications from 2017 to 2018. It is said that Mr Altayeb was a senior aide to Mr Al Jasser when Mr Al Jasser was Director General.

5. The IAFC Parties maintain that Mr Al Jasser and Mr Altayeb were critical figures in the negotiation, execution and performance of the Lease Agreements. Indeed, Mr Al Jasser signed all fifty Lease Agreements, as well fifty Novation Deeds, fifty Lease Supplements, fifty Acknowledgements of Assignment of Sub-Lease, and the Side Letter and Memorandum of Understanding dated 8th August 2016, all on behalf of Saudia. Saudia's Disclosure Review Document identifies Mr Al Jasser and Mr Altayeb as custodians in respect of various documents and identify mobile telephones as data sources.

6. I understand that, according to the fifth witness statement dated 20th August 2021 (at para. 18-22) and the sixth witness statement dated 8th September 2021 (at para. 6-7) made by Mr Robin Springthorpe (of Norton Rose Fulbright LLP, Saudia's solicitors), Mr Al Jasser has a work mobile telephone and a personal mobile telephone. The personal mobile telephone is not generally used for work purposes, although it might be used for work purposes exceptionally. Mr Al Jasser does not believe that the personal mobile telephone contains any relevant material which should be disclosed.

7. Mr Al Jasser's work mobile telephone which he used when he was Director General of Saudia was owned by Mr Al Jasser but paid for by Saudia. Since October 2019, when Mr Al Jasser became Minister of Transport in the Kingdom of Saudia Arabia, Mr Al Jasser's retained ownership of his mobile telephone (and kept the same telephone number), but the Ministry took over responsibility for paying for the mobile telephone. Every time Mr Al Jasser receives a new mobile telephone by way of upgrade, he deleted the data in the handset to be replaced, transferred the data to his new handset, and provided the old handset to a member of his family.

8. It is understood that Saudia accepts that Mr Al Jasser's work mobile telephone (which I shall continue to refer simply as Mr Al Jasser's mobile telephone) may contain material relevant to Issues for Disclosure 1, 3, 7, 10 and 11 set out in the Disclosure Review Document. For the purposes of this application, I need not explain what those Issues entail. It is understood that Mr Al Jasser's mobile telephone may include relevant email exchanges (which should also be found on Saudia's email server) and in addition instant messaging communications (such as those used in WhatsApp).

9. According to para. 25 of Mr Springthorpe's fifth witness statement, Mr Altayeb - who is no longer employed by Saudia - used his mobile telephone (which I understand belongs to Mr Altayeb) to access his email account to conduct business in relation to Saudia's dealings with the IAFC Parties, including the matters in issue in this case, and that therefore all relevant material on his mobile telephone of which he is custodian should be found on Saudia's email servers.

10. During the oral argument in respect of the IAFC Parties' application for disclosure, the focus was on the data held in Mr Al Jasser's mobile telephone, rather than the mobile telephone of Mr Altayeb. That said, I understand that the IAFC Parties maintained their application in respect of Mr Altayeb's mobile telephone.

11. The central issue upon this application is whether the Court should grant an order for disclosure against Saudia in respect of the data held on Mr Al Jasser's and Mr Altayeb's mobile telephones and in this respect whether such data are within the control of Saudia.

12. The application notice issued by the IAFC Parties was for an order to vary the Extended Disclosure already ordered by the Court requiring Saudia to disclose documents relating to the Issues for Disclosure held on the personal devices of Mr Al Jasser and Mr Altayeb. Immediately prior to the hearing on 7th October 2021, the IAFC Parties had formulated their application for alternative orders, namely that (a) an order that Saudia use "best endeavours" to secure the production of the documents held on the mobile telephones by Mr Al Jasser and Mr Altayeb, and to file witness evidence explaining what steps have been taken in this respect, and/or (b) an order that Mr Al Jasser or Mr Altayeb produce their devices to independent IT consultants to be searched for documents.

13. Therefore, during the hearing on 7th October 2021, the IAFC Parties had essentially restricted their application for an order that Saudia request, or use best endeavours to request, Mr Al Jasser and Mr Altayeb to produce the documents or data held on their mobile telephones, which might well include providing their mobile telephones for review by a nominated IT consultant. I shall refer to this as a "best endeavours" order.

14. In considering this application, I will address the following issues:

(1) Are the documents held on the mobile telephones within the control of Saudia?

(2) If the documents held on the mobile telephones are not within the control of Saudia, does the Court have the jurisdiction to make a "best endeavours" order?

(3) Should the Court make an order for disclosure or a "best endeavours" order?

Are the documents held on the mobile telephones within the control of Saudia?

15. CPR rule 31.8 provides that *"A party's duty to disclose documents is limited to documents which are or have been in his control*". The rule then proceeds to identify when a party to an action has or has had a document in its control, namely when (a) the document is or was in the physical possession of the party, (b) when the party has or has had a right to possession of the document, and (c) when the party has or has had a right to inspect or take copies of the document. However, these three instances of control are not the only circumstances in which such control may be found to exist (*North Shore Ventures Ltd v Anstead Holdings Inc* [2012] EWCA Civ 11, para. 40).

16. As Mr Tom Sprange QC on behalf of the IAFC Parties pointed out, the same definition is reproduced in paragraph 1.1 of Appendix 1 to CPR Practice Direction 51U (the Disclosure Pilot for the Business and Property Courts).

17. Para. 1.9 of CPR Practice Direction 51U provides that CPR Part 31 (with certain specified exceptions), and therefore CPR rule 31.8, does not apply to proceedings within the Disclosure Pilot.

18. However, as Andrew Baker, J observed in *Pipia v BGEO Group Ltd* [2020] EWHC 402 (Comm); [2020] 1 WLR 2582, at para. 12-13, the term "*control*" is barely used in CPR Practice Direction 51U, but it is used (a) to define the meaning of Known Adverse Documents (para. 2.8), (b) to define the documents which a party and a party's legal representative are under a duty to preserve for the purposes of the disclosure exercise (para. 3.1(1) and 3.2(1)); (c) to define the continuing duty to disclose documents in the control of a party which come to the knowledge of a party at a later date (para. 9.3), and (d) to provide that a party cannot rely on a document which should have been disclosed but was not, at least without the permission of the Court (para. 12.5). In addition, para. 12.1 requires the service of a Disclosure Certificate, the form of which is included at Appendix 4 of CPR Practice Direction 51U and which requires the certifying party to identify the documents within its control.

19. Andrew Baker, J concluded that, having regard to the terms of the Disclosure Review Document and the Disclosure Certificate which a party is obliged to provide, "*it is thus implicit throughout that to the extent search-based disclosure is to be used, the concept of "control", as defined, fixes the universe of documents from which, by one or other or a combination of means, a party's extended disclosure is to be generated*". That must be right. The requirement that a document having to be in the party's "*control*" whether at the time of disclosure or earlier is a critical component in delimiting the documents over which the party's obligations of disclosure are to be prescribed. If that were not the case, a party's disclosure obligations would be uncontrollably wide and would create unnecessary and potentially expensive issues for determination as part of an already costly disclosure process.

20. Therefore, a party to an action may be ordered to disclose documents which are or have been in its control. Disclosure in this sense refers to a party stating whether a document exists or had existed insofar as such documents are in the party's control or have been in the party's control. This does not necessarily translate to a party having to produce the document for inspection, if for example the document no longer exists or is no longer in that party's control.

21. Insofar as a document is in the physical possession of a third party, meaning a person who is not a party to the action, that document is in the control of a party to the action not only where the party has a legally enforceable right to obtain access to such a document, but also where there is a standing or continuing practical arrangement between the party and the third party whereby the third party allows the party access to the document, even if the party has no legally enforceable right of such access (see *Schlumberger Holdings Ltd v Electromagnetic Geoservices AS* [2008] EWHC 56 (Pat), para. 21; *Pipia v BGEO Group Ltd* [2020] EWHC 402 (Comm); [2020] 1 WLR 2582, para. 11, 14-21; *BES Commercial Electricity Ltd v Cheshire West and Chester Borough Council* [2020] EWHC 701 (QB), para. 61-63). However, in order to establish that there is such a standing or continuing arrangement or even a specific, time-limited arrangement, whereby a third party allows a party to the action access to the document which the third party has in its possession, it is not generally sufficient to demonstrate that there is a close legal or commercial relationship between the party and third party, such as parent and subsidiary companies or employer and employee relationships; something more is required; there must be more specific and compelling evidence of such an arrangement (*Ardila Investments NV v ENRC NV* [2015] EWHC 3761 (Comm), para. 13-14; *Pipia v BGEO Group Ltd* [2020] EWHC 402 (Comm); [2020] 1 WLR 2582, para. 18-21, 50-51, 58-59).

22. Mr Tom Sprange QC (who appeared with Mr Kabir Bhalla) on behalf of the IAFC Parties submitted that the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones are within Saudia's control, because:

    (1) Under the law of the Kingdom of Saudi Arabia, Saudia is entitled to access the documents held on the mobile telephones of its current non-executive chairman (Mr Al Jasser) and/or its former employees.

    (2) By reason of the fact that Mr Al Jasser currently held and had held senior positions within Saudia's organisation, and Mr Altayeb had held senior positions within Saudia, it should be presumed that Saudia has control over the contents of Mr Al Jasser's and Mr Altayeb's mobile telephones insofar as they relate to the activities of Saudia and arise from the employment relationship.

    (3) The terms of the Disclosure Review Document filed by Saudia, which identify Mr Al Jasser and Mr Altayeb as custodians, indicate that Saudia has a right of access to those documents, at least by reason of some standing arrangement whereby Mr Al Jasser at least has consented to allowing Saudia practical access to the documents on his mobile telephone.

23. Mr Giles Robertson on behalf of Saudia took issue with these submissions.

Expert evidence of Saudi law

24. Mr Mohammed A Al Qarni, who is Head of Litigation of Zarei & Hamdan Law Firm in Riyadh, in a report dated 30th September 2021, served on behalf of the IAFC Parties, stated that Saudia has a right of possession, inspection or control in respect of the documents held on the mobile telephones for the following reasons:

(1) There is nothing in Saudi Arabian law that prevents Saudia from requesting former employees to provide the documents on their mobile telephones, regardless of whether the devices in question were personal, provided that they were created in or relate to the former employees' capacity as employees of Saudia.

(2) Under Shari'ah law, the employer entrusts the employee with information and materials for use in the course of the employee's employment. This trust is codified in the Saudi Arabian Labour Law and Companies Law. That trust does not make the actual information and materials themselves the property of the employee simply because they are stored on a personal device belonging to that employee. Under the Law on the Penalties on Dissemination and Disclosure of Classified Information and Documents, the confidentiality of the information of the government and government-owned entities is protected. Article 1(b) defines confidential information as information obtained by the employee or which the employee holds or obtains by virtue of his employment.

(3) The employment contracts for both Mr Al Jasser and Mr Altayeb do not contain an express provision requiring them to maintain or return electronic records. However, the employment contract of Mr Altayeb (but not Mr Al Jasser) requires him, under Article 14(d), to "[t]ake adequate care of tools, tasks assigned to him, and raw materials owned by [Saudia] and at his disposal or in his custody, and return non-consumable materials to [Saudia]". This provision is included in Article 65(2) of the Labour Law as a duty of the employee. Even though Mr Al Jasser's employment agreement does not contain a similar provision, Mr Al Jasser is nonetheless bound by Article 65(2) of the Labour Law. Typically, this provision would apply to the physical materials required for a labourer or what a craftsman would use in the course of his employment. That said, one could infer that this requirement could extend to digital information and files.

(4) Under Saudi Arabian Labour Law, employees are bound by the contents of employee handbooks and company regulations. By Articles 123 and 134 of the Labour Law, employers are required to establish "work regulations to govern the work performed"; these take the form of employee handbooks or regulations, including the Saudia Employee Regulations and the Saudia Management Policy & Procedure Manual. These employee regulations form a part of the "instructions" that the employer has issued to the employee, typically upon joining the company or at date of issue. Under Article 65(1) of the Labour Law, the employee is obliged to comply with legitimate instructions of the employer in the course of his employment. Under articles 40(4)-(5) of the Saudia Employee Regulations, Saudia employees are required to protect Saudia property and confidentiality. The confidentiality requirement of Article 40(5) of

the Saudia Employee Regulations expressly applies after the termination of the relevant employment (see also Article 65(6) of the Labour Law). Article 41(7) then affirmatively forbids employees to "*Keep papers and formalities relating to work outside the place of work without acceptable justification*". This means that Saudia retains the rights over such work-related information, and there is an expectation that the employee will return any "*papers and formalities relating to work*" at the end of his tenure with Saudia.

(5) It is common practice in Saudi Arabia for companies like Saudia to have data retention and safeguarding content regulations, even with respect to an employee's personal devices.

(6) As Director General of Saudia, Mr Al Jasser owed fiduciary duties to Saudia during his tenure. Under the Saudi Arabian Companies Law, the general manager and "*responsible persons*" can be penalised for failing to abide by these fiduciary duties to a company. Saudi Arabian law does not have a specifically codified set of fiduciary duties, yet they derive from principles of Shari'ah and the penalties listed in the Companies Law, including a duty of loyalty, a duty of no conflicts of interest, and a duty to promote the success of the company.

(7) Under Article 5 of the Saudia Bylaws, the board of directors is the supreme authority which manages and controls the business and affairs of Saudia, which allows the board to propose resolutions and regulations (Article 5). However, although resolutions can be passed by the board, regulations can be made only by the Council of Ministers of which Mr Al Jasser is a member (Article 5(5)).

(8) Under Article 213(m) of the Companies Law, a director or responsible person can face penalties for impeding or causing to impede the duties of persons who are legally authorised to have access to the company's papers, instruments, accounts, and documents, or who refuses to enable such authorised persons to perform their duties.

25. Saudia's expert, Dr Hamid M Harasani of Harasani & Alkhamees Law Firm LLP in Jeddah, in his report dated 30th September 2021, expressed the opinion that there is no entitlement on the part of Saudia to possess, inspect, or control or obtain access to the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones for the following reasons:

(1) Article 40 of the Basic Law of Governance provides that "*Correspondence by telegraph, mail, telephone conversations, and other means of communication shall be protected. They may not be seized, delayed, viewed, or listened to except in cases set forth by law*". This affords sanctity and protection to telephone correspondence and is affirmed by Article 9 of the Saudi Telecommunications Law and Shari'ah law which protects the privacy and confidentiality of information transmitted or received through public telecommunications networks. If, therefore, a person claims to be entitled to possess, inspect, or control another person's telephone messages, in absence of that other's unfettered consent, that person must support his or her claim by reference to an explicit provision from Saudi law.

(2) Under Saudi Labour Law, Article 4 requires Shari'ah law to be adhered to, Article 20 protects employer and employee rights, and Article 65 requires an employee to comply with instructions, "*provided that such instructions do not conflict with the contract, the law or public morality and that they do not expose him to any undue hazards*".

(3) There is no provision in the Labour Law, or its implementing regulations, that affords an employer the right to possess, inspect, or control work-related messages on employee telephones.

(4) There is no provision in the Saudi Arabian Airlines Corporation Employees and Labourers Regulations dated 1999 affording Saudia the right to possess, inspect, or control work-related messages on employee telephones. Even if there were such a provision in the internal labour regulations, it would not be enforceable, as the Labour Law would clearly override a contradictory provision from an internal labour regulation, especially if such a provision is disadvantageous to an employee, when measured against his or her rights in the Labour Law (Article 8). An internal labour manual provision allowing for the possession, inspection, or control of employee telephones would be contrary to Article 20 of the Labour Law, and in applying Article 8, this contrary provision would be null and void.

(5) There is no provision in Saudia's Management Policy & Procedure Manual dated 29th December 2016 affording Saudia the right to possess, inspect, or control work-related messages on employee telephones. Saudia's Management Policy & Procedure Manual does not contain any provisions granting Saudia or its board the power to possess, inspect, control, or pass board resolutions requiring Mr Al Jasser as Chairman to hand over his mobile telephone for the inspection of work-related messages.

(6) There is no provision in Mr Al Jasser's and Mr Altayeb's employment contracts affording Saudia the right to possess, inspect, or control work-related messages on employee telephones. Article 14(d) in Mr Altayeb's employment contract provides that he must, "*take adequate care of tools, tasks assigned to him, and raw materials owned by the First Party and at his disposal or in his disposal or in his custody and return non-consumable materials to the First Party*", but this stops short of obliging Mr Altayeb to submit his telephone for possession or inspection by Saudia. Neither does it provide for Saudia's control of work-related messages; and it must therefore be narrowly interpreted in light of Article 40 of the Basic Law of Governance, Article 9 of the Telecommunications Law, and Articles 8 and 20 of the Labour Law. Further, with respect to Mr Altayeb (who is no longer employed by Saudia), Article 234 of the Labour Law imposes a one-year limitation on bringing legal claims arising out of employment contracts.

(7) There is no provision in the Labour Law, Saudia's internal policies, or the employment contracts that qualifies the general constitutional right in Article 40 of the Basic Law of Governance, or the general law in Article 9 of the Telecommunications Law allowing Saudia such access to the data on employees' mobile telephones. It would be contrary to Saudi law for an

employer to possess, inspect or control work-related messages on employee telephones.

(8) Article 5 of the Saudi Arabian Airlines General Corporation Law and Article 5 of the By-Laws of the Saudi Arabian Airlines Corporation lists the powers available to Saudia's board of directors, none of which grant the board or Saudia the right to possess, inspect, or control work-related messages on Mr Al Jasser's mobile telephone or grant Saudia's board of directors the power to pass a resolution compelling Mr Al Jasser as Chairman to submit his telephone for inspection.

(9) Mr Al Jasser uses the same mobile telephone in respect of his duties as Minister of Transport to carry out his concurrent duties as Chairman of Saudia. He therefore has a legal duty to guard and protect this telephone from inspection by third parties, by virtue of the state secrets that may be contained in his telephone. Article 2 of the Penal Law on Dissemination and Disclosure of Classified Information and Documents imposes an obligation on Mr Al Jasser not to disseminate or disclose classified information or documents which he obtains or is privy to be virtue of his office, if such dissemination or disclosure remains restricted.

26. Mr Al Qarni and Dr Harasani exchanged supplementary reports on 4th October 2021 identifying areas of agreement or disagreement.

27. In cases such as this, it is very often difficult to evaluate the conflicting evidence of two experts expressing their opinions only in writing on the application and effect of foreign law, in this case the law of the Kingdom of Saudi Arabia. In deciding how to judge the effect of this expert evidence, I also take into account the submissions made by Mr Tom Sprange QC on behalf of the IAFC Parties and Mr Giles Robertson on behalf of Saudia. I make the following observations on the expert evidence.

28. First, Article 40 of the Basic Law of Governance provides that "*Correspondence by telegraph, mail, telephone conversations, and other means of communication shall be protected*" and shall not be seized or viewed unless set forth by a relevant law. I did not understand Mr Al Qarni to dispute this.

29. Second, although I recognise that the Law on the Penalties on Dissemination and Disclosure of Classified Information and Documents protects the confidentiality of the information of the government and government-owned entities (although Dr Harasani questions, in his supplementary report, its application to the content on the mobile telephones save to the extent that its disclosure would harm national security), and Article 9 of the Telecommunications Law protects the confidentiality of telephone communications, that does not self-evidently translate into an entitlement on the part of Saudia to access any confidential content on the mobile telephones.

30. Third, there is no clear statement as a matter of Saudi law which explicitly entitles a company in the position of Saudia to access the content on the mobile telephones of former employees or their non-executive Chairman. There appears to be no express provision in Saudi Labour Law, Saudia's employment regulations, and Saudia's Management Policy & Procedure Manual which allow such a right of access to Saudia.

31. Fourth, there is no provision in Mr Al Jasser's and Mr Altayeb's employment contracts which entitles Saudia to access the content on their mobile telephones. In addition, the provision in Mr Altayeb's employment contract, and article 65(2) of the Saudi Labour Law, requiring the employee to take care of tools and raw materials and to return "*non-consumable materials*" to the employer do not on their terms apply to the electronic data held on mobile telephones. Indeed, Mr Al Qarni stated that typically this provision would apply to the physical materials required for a labourer or what a craftsman would use in the course of his employment. Mr Al Qarni could only merely "*infer*" that Saudia has a right of access to their former or current employees' mobile telephones by reason of this provision. That was not sufficient in my judgment to establish a legal right of access on the part of Saudia.

32. Fifth, although I accept that an employee would be obliged to comply with legitimate instructions given by an employer (Article 65(1) of the Labour Law) and although the Saudia Employee Regulations require employees to protect Saudia's property and confidentiality (even after the termination of the employment relationship), and further require employees not to keep papers outside the workplace, without justification, there is no explicit provision requiring the employees to return data held on their electronic devices to Saudia.

33. Sixth, although there is evidence that regulations or resolutions may be proposed by Saudia's board of directors, this does not speak to an existing entitlement on the part of Saudia to obtain access to the documents held on the mobile telephones of Mr Al Jasser and Mr Altayeb. Even if Saudia could bring into effect such resolutions or regulations (the latter of which would require the approval of the Council of Ministers), the process seems to be unnecessarily cumbersome for the purposes of a disclosure exercise such as that before the Court (cf. *Lonrho Ltd v Shell Petroleum Co Ltd* [1980] 1 WLR 627, 636, where the House of Lords held that RSC Order 24 did not require a company to alter its articles to bring documents within its power).

34. Seventh, although Saudi companies law imposes penalties on a person who impedes those who are entitled to access documents to obtain such access, that begs the question whether there is an entitlement to access. In any case, according to Dr Harasani, this legislation is not applicable to Saudia because it is not a company but instead a general corporation created by Royal Decree.

35. Eighth, while I accept that private information is protected by Saudi law, that does not necessarily mean that any data which is not private but relates to Saudia's commercial activities is likewise protected. However, there remains a question as to how such private and other information could be separated on a personal device for the purposes of reviewing the same in order to provide disclosure. I refer to this consideration later in this judgment.

36. Ninth, although I am prepared to accept that there are fiduciary duties applicable to Mr Al Jasser (Mr Al Qarni did not explain in his evidence the fiduciary responsibilities of Mr Altayeb), which would include a duty of loyalty, a duty to ensure that there are no conflicts of interest and a duty to promote the success of the company, I do not consider that the evidence was sufficiently clear to establish that such a fiduciary duty extended to allowing Saudia access to the content on Mr Al Jasser's mobile telephone.

37. Tenth, finally, as Mr Robertson submitted, there is no evidence of any academic commentary or judicial decision which interprets the legislation being considered by the experts or which comments on the existence of a more general fiduciary duty in support of the suggestion that Saudia has a right of access to the information held on Mr Al Jasser's and Mr Altayeb's mobile telephones.

38. In my judgment, having regard to these observations and the expert evidence more generally, I am not satisfied that the expert evidence supports the submission that Saudia has a right to take possession or to access or to inspect the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones. Accordingly, for the purposes of this application, I find that the element of "*control*" which is the basis of an order for disclosure under the Disclosure Pilot is absent.

39. In addition, there were internal Saudia documents to which I was taken, in particular the Information Security Standards, the Information Security Policy, and the Acceptable Use Policy. These documents were disclosed by Saudia only on 4th October 2021, shortly before the hearing and after any opportunity existed for the experts to consider them. Mr Sprange QC referred me to the following provisions:

    (1) The Information Security Standards: para. 6.2.5 (which classifies confidential information), para. 6.2.8.2 which provides that "*All data should be securely wiped using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks*" and para. 11.2.7, which provides that "*Data segregation between personal information and data owned by the SAUDIA should be enabled and enforced. Additionally, segregated data should be encrypted*".

    (2) The Information Security Policy: para. 5.2.6, which provides that "*Personnel must adhere to information security policies and Acceptable Use Policy before they are granted access to IT services and systems*", para. 9.2.15, which provides that "*Email must be archived and backed up on a regular basis following Backup and Recovery Management Policy*", para. 9.2.16, which provides that "*Personal email must not be used for business related work except retirees are allowed to use their personal email in order to access retiree services*", para. 11.2.1, which provides that "*SAUDIA's data stored on mobile devices and BYODs must be separated and encrypted following Cryptography Policy*" and para. 11.2.4, which provides that "*SAUDIA's data stored on mobile devices and BYODs [Bring Your Own Device] must be securely wiped in cases of device loss, theft or after termination/separation from SAUDIA*".

    (3) The Acceptable Use Policy: para. 3.1.8, which provides that there should be "In case of using SAUDIA IT services on personal devices (e.g. mobile and laptop), immediate reporting to SAUDIA IT of any theft or loss of these devices", para. 3.2.4 which prohibits "Using of personal mail or file sharing services for work related matters or saving/sharing SAUDIA's data" and para. 3.2.26 which prohibits "Leaving personal devices (e.g. mobile and laptop) unattended/unprotected in public areas if the device is used for SAUDIA services".

40. Even though the Information Security Standards, at para. 11.2.7, refers to data "*owned*" by Saudia, it is unclear what is meant by that reference. In any case, there is no reference in these documents allowing Saudia access to the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones. Accordingly, there is nothing in these documents which disturbs my conclusion that such documents are not in the control of Saudia.

The proposed presumption of control given the employment relationship

41. Mr Sprange QC submitted on behalf of the IAFC Parties that, by reason of the fact that Mr Al Jasser currently held and had held senior positions within Saudia's organisation, and Mr Altayeb had held senior positions within Saudia, there are fiduciary or equivalent obligations on Mr Al Jasser and Mr Altayeb to afford assistance to Saudia for the purposes of disclosure in these proceedings (*North Shore Ventures Ltd v Anstead Holdings Inc* [2012] EWCA Civ 11, para. 11; *Fairstar Heavy Transport v Adkins* [2013] EWCA Civ 886; [2013] 2 CLC 272, para. 51-56; *Phones 4U (in administration) v EE Ltd* [2021] EWCA Civ 116; [2021] 1 WLR 3270, para. 4). Therefore, unless there is a contrary provision in their respective employment contracts, there is at least a presumption that Saudia has a right of access to such documents and therefore the data held on Mr Al Jasser's and Mr Altayeb's mobile telephones are within Saudia's control.

42. I can address this submission relatively briefly. I would be sympathetic to this submission if the employment relationships were governed by English law. However, the employment relationship between Saudia on the one hand and Mr Al Jasser and Mr Altayeb on the other hand are governed by the law of the Kingdom of Saudi Arabia. This is common ground.

43. In those circumstances, I do not consider that there is any place for the presumption proposed by Mr Sprange QC, especially in circumstances where the Court has had the benefit of detailed expert evidence on Saudi law (see by way of comparison *Pipia v BGEO Group Ltd* [2021] EWHC 86 (Comm), para. 88).

The Disclosure Review Document

44. Mr Sprange QC on behalf of the IAFC Parties submitted that there must be a standing or continuing practical arrangement between Mr Al Jasser and Mr Altayeb on the one hand and Saudia on the other hand which allows Saudia access to the Saudia-related data on their mobile telephones such that such data can be said to fall within the control of Saudia (*Pipia v BGEO Group Ltd* [2020] EWHC 402 (Comm); [2020] 1 WLR 2582, para. 11, 14-21).

45. The Disclosure Review Document filed by Saudia confirmed at question 2 of section 2, that Saudia's proposed data sources included "*Computer systems/electronic storage devices … Mobile phones, tablets and other handheld devices*", as well as document management systems, email servers, cloud based data storage, webmail accounts and back-up systems, and that, "*At this stage, the Defendant does not anticipate that there will be any restrictions to the availability of relevant documents*". In addition, question 6 of section 2 states that both Mr Al Jasser and Mr Altayeb are custodians. However, at question 12 of section 2, it is said that "*It is not anticipated at this stage that any documents will be irretrievable however it is noted that Saleh Al Jasser, Abdulrahman Altayeb, Rene Gsponer, Said Daaloui, Hashim Koshak, Abdullah Algahtani and Ahmed*

Al Aiesh are no longer employed by the Defendant which may affect the availability of their contemporaneous documents".

46. I do not consider that the Disclosure Review Document suffices as evidence that the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones are within the control of Saudia for the purposes of making an order for disclosure, given the qualification expressly made by Saudia as quoted above.

The Court's jurisdiction to make a "best endeavours" order

47. I have concluded that the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones are not within Saudia's control for the purposes of making an order for disclosure under the Disclosure Pilot. The question arises whether the Court has the jurisdiction to make an order requiring Saudia to exercise or use best endeavours to obtain access to Mr Al Jasser's and Mr Altayeb's mobile telephones for the purposes of disclosing documents held on those devices.

48. I was and am uncertain whether the IAFC Parties persist in this aspect of the application even if there were the relevant documents are not in Saudia's control. If they do not, then this question does not arise. If, however, the IAFC Parties persist in this part of the application, I now consider the extent of the Court's jurisdiction in this respect.

49. Mr Sprange QC submitted on behalf of the IAFC Parties that:

(1) There is nothing in CPR Part 31 or Practice Direction 51U that prohibits such a "best endeavours" order.

(2) The ability to make such an order is consistent with the spirit of the Disclosure Pilot and the CPR generally, having regard to the overriding objective. Such an order is in accordance with the co-operation expected of the parties when dealing with disclosure under the Disclosure Pilot (*McParland & Partners Ltd v Whitehead* [2020] EWHC 298 (Ch); [2020] Bus LR 699, at para. 4, 53, 58).

(3) The Court has an analogous express power to order that a party should use "*best endeavours to obtain and disclose documents which are not or have not been in his control … at any stage of the proceedings and on such terms … as the court thinks fit*" in proceedings relating to a marine insurance policy under CPR rule 58.14 (a '"ship's papers" order). The rationale in support of such an order applies equally to the circumstances of the present case.

(4) In practice, "best endeavours" orders have been made (see *BES Commercial Electricity Ltd v Cheshire West and Chester Borough Council* [2020] EWHC 701 (QB), para. 77-79).

50. Mr Robertson on behalf of Saudia submitted that:

(1) Prior to the CPR, the House of Lords held in *Lonrho Ltd v Shell Petroleum Co Ltd* [1980] 1 WLR 627 that the Court could not order a party to make a request of a third party to provide documents for disclosure.

(2) There is no authority which establishes such a jurisdiction. There are three authorities identified in *Hollander on Documentary Evidence* (14th ed., 2021), at para. 9-24, where an order requiring a party to request a third party to produce documents have been made or contemplated, but none on analysis establish the Court's jurisdiction. Two of the authorities (*BES Commercial Electricity Ltd v Cheshire West and Chester Borough Council* [2020] EWHC 701 (QB) and *Phones 4U (in administration) v EE Ltd* [2021] EWCA Civ 116; [2021] 1 WLR 3270, para. 31) were cases where the Court had held that the documents in the possession of a third party were in the control of a party to the action. The third authority was the decision in *Bank St Petersburg PJSC v Arkhangelsky* (No 2) [2015] EWHC 2997 (Ch); [2016] 1 WLR 1081, where the Court held that no relevant control existed, but nonetheless proposed at para. 45 an order requiring a party to request documents from a third party, although this was said to be "*subject to further argument if required*" and it is not clear what, if any, argument resulted.

(3) The Court's power to order disclosure is statutory, being derived from delegated legislation and it is appropriate that the Court's jurisdiction is defined by the Civil Procedure Rules, rather than being developed as a matter of general law (*The Siskina* [1979] AC 210, 262; *Dubai Bank Ltd v Galadari (No. 6)*, unreported, 6th October 1992 ([1992] 10 WLUK 39)). The existence of such a power under CPR rule 58.14 is confined to marine insurance actions and should not be extended (*The West of England and South Wales District Bank v The Canton Insurance Company* (1877) 2 Ex D 472).

51. In my judgment, Mr Robertson is correct in his submission that the Court has no general power to require a party under CPR Practice Direction 51U to request a third party to produce a document to a party for disclosure in an action where that document is not within the party's control.

52. In *Lonrho Ltd v Shell Petroleum Co Ltd* [1980] 1 WLR 627, the House of Lords considered the meaning of the words "*possession, custody or power*" which determined the scope of discovery under RSC Order 24 (and the phrase remains in sections 33 and 34 of the Senior Courts Act 1981) and held that the Court could not order discovery of documents to which the party had no presently enforceable right of access. At pages 635-636, Lord Diplock said that:

> "*… in the context of the phrase "possession, custody or power" the expression "power" must, in my view, mean a presently enforceable legal right to obtain from whoever actually holds the document inspection of it without the need to obtain the consent of anyone else. Provided that the right is presently enforceable, the fact that for physical reasons it may not be possible for the person entitled to it to obtain immediate inspection would not prevent the document from being within his power; but in the absence of a presently enforceable right there is, in my view, nothing in Order 24 to compel a party to a cause or matter to take steps that will enable him to acquire one in the future …*

> *For the reasons already indicated Shell Mocambique's documents are not in my opinion within the "power" of either of Shell or B.P. within the meaning of R.S.C., Ord. 24. They could only be brought within their power either (1) by their taking steps to alter the articles of association of Consolidated and procuring Consolidated through its own board of directors to take steps to alter the articles of association of Shell Mocambique, which Order 24 does not require them to do; or (2) by obtaining the voluntary consent of the board of Shell Mocambique to let them take copies of the documents. It may well be that such consent could be obtained; but Shell and B.P. are not required by Order 24 to seek it, any more than a natural person is obliged to ask a close relative or anyone else who is a stranger to the suit to provide him with copies of documents in the ownership and possession of that other person, however likely he might be to comply voluntarily with the request if it were made.*"

53. It may or may not be the case that the respective meanings of "*control*" and "*possession, custody or power*" are the same in scope, but they must at the least substantially overlap. There is no reason to suppose that the reasoning adopted by the House of Lords in *Lonrho v Shell* should not apply when considering the scope of "*control*" under CPR Practice Direction 51U.

54. There is no authority of which I am aware which allows the Court to require a party to exercise best endeavours to obtain or to request a third party to provide documents for disclosure under the Disclosure Pilot or generally under CPR Part 31. Such an order might well be made if the requisite "*control*" is established (*Phones 4U (in administration) v EE Ltd* [2021] EWCA Civ 116; [2021] 1 WLR 3270). Indeed, even if the relevant party does not have control of a document, the Court has a separate power to make orders requiring a third party to provide disclosure of that document (at least to the extent that the Court has jurisdiction over that third party) (under CPR rule 31.17, which is expressed to be applicable to CPR Practice Direction 51U by para. 1.9 and Section II). However, where a party to the relevant proceedings has no relevant control over the documents in question, absent any specific provision in the CPR permitting such an order, the Court does not have the power to make such a "best endeavours" order by way of an extension of the powers allowed it by the CPR, because the Court's jurisdiction is derived exclusively from statute or delegated legislation, namely the CPR (*Vinos v Marks & Spencer plc* [2001] 3 All ER 784, para. 26), and because the CPR makes no provision for such a power in a case such as this. Thus, in *The Siskina* [1979] AC 210, at page 262, Lord Hailsham commented on the Court's then jurisdiction to grant a *Mareva* injunction as follows:

> "*The second point upon which I wish to comment is the argument of Lord Denning M.R., fortified by the authority of a quotation from Hymns Ancient and Modern, that the judges need not wait for the authority of the Rules Committee in order to sanction a change in practice, indeed an extension of jurisdiction, in matters of this kind. The jurisdiction of the Rules Committee is statutory, and for judges of first instance or on appeal to pre-empt its functions is, at least in my opinion, for the courts to*

> *usurp the function of the legislature. Quite apart from this and from technical arguments of any kind, I should point out that the Rules Committee is a far more suitable vehicle for discharging the function than a panel of three judges, however eminent, deciding an individual case after hearing arguments from advocates representing the interests of opposing litigants, however ably*."

55. In *Dubai Bank Ltd v Galadari (No. 6)*, unreported, 6th October 1992 ([1992] 10 WLUK 39), Glidewell, LJ referred to the decisions in *The Siskina* and *Lonrho v Shell* in considering whether the Court had the power to order the defendants to use all lawful means to obtain documents held by a third party, so that if they obtained the documents they would become discoverable. The Court of Appeal then referred to the decision in *James Nelson & Sons Limited v Nelson Line (Liverpool) Limited* [1906] 2 KB 217, at page 222, where Sir Henn Collins MR said:

> "*The question is whether the rules as to discovery, as interpreted by decided cases, entitle the Court to make the order applied for by the defendants … We are not, as it seems to me, at large to do abstract justice in the matter, but are limited by the express provisions of the rules on the subject. The whole matter of discovery has been the subject of special legislation, and we must look to that legislation, as interpreted by the cases, to see whether we are not really being invited by the defendants' counsel to take a step beyond anything which has heretofore been regarded as covered by the enactments as to discovery. I think that is what we are invited to do; and, though I sympathize to some extent with a good deal that the defendants' counsel said, I do not feel justified in taking that step into the infinite, and departing from the firm foothold afforded by the statutory enactments and decisions on the subject.*"

56. Glidewell, LJ then concluded that there was no general jurisdiction to order discovery of documents absent any warrant allowed by the Rules of the Supreme Court (subject to certain exceptions, such as in respect of *Mareva* injunctions and *Norwich Pharmacal* orders):

> *"… we agree with Mr Davies that this order is an extension of the power to order discovery for which there is no legal justification. In some cases (of which this may well be one) the making of such an order may be an aid to a just and practical solution to a problem. Nevertheless in our judgment we do not have it in our power to extend the ambit of discovery in this way. As Sir Henn Collins M.R. reminded us, we "are limited by the express provisions of the Rules on the subject"."*

57. In *Phones 4U (in administration) v EE Ltd* [2020] EWHC 1921 (Ch), Roth, J considered the decision in *Dubai Bank v Galadari (No. 6)*, but made it clear at para. 61 that the order sought was "*for a step towards the practical exercise of that established jurisdiction, by seeking to identify documents that fall under the Defendants' control*"

(this was affirmed by the Court of Appeal at [2021] EWCA Civ 116; [2021] 1 WLR 3270, para. 31). Accordingly, Roth, J was not suggesting that the Court could extend the jurisdiction to order disclosure of documents which are not in a party's control. See also *Unicredit Bank AG v Euronav NV* [2021] EWHC 1753 (Comm), para. 21-23. Cf. *Montpellier Estates Ltd v Leeds City Council* [2012] EWHC 1343 (QB), para. 30-35.

58. Of course, the Court does have an express power under CPR rule 58.14 to require a party to exercise best endeavours to obtain documents from third parties even though the documents are not in that party's control, but that power exists only "*in proceedings relating to a marine insurance policy*" and often or invariably only in respect of "scuttling allegations" (*Probatina Shipping Co Ltd v Sun Insurance Office Ltd* [1974] 1 QB 635, 641-642). This, therefore, is an exceptional power and the absence of any rule in the CPR permitting a similar order to be made in other circumstances indicates that there is no such wider power.

59. Therefore, the Court has no jurisdiction to make an order requiring a party to exercise best endeavours to obtain or request a third party to produce documents for disclosure which are not already in the party's control.

Should the Court make an order for disclosure?

60. For the reasons explained above, I have arrived at the conclusion that the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones are not within Saudia's control and that therefore the Court has no jurisdiction to require Saudia to exercise best endeavours to obtain or request Mr Al Jasser or Mr Altayeb to produce those documents for disclosure which are not already in Saudia's control.

61. Accordingly, how the Court might have exercised this jurisdiction in this case does not arise. However, if I am wrong in my decision on the scope of the Court's jurisdiction, I would have decided to refuse the IAFC Parties' application in any event for the following reasons.

62. First, the documents on Mr Al Jasser's mobile telephone would have included data relating to the affairs of the Ministry of Transport, Mr Al Jasser's personal affairs and Saudia's activities. There would have been a complex exercise in arranging for Saudia's data to be removed for the purposes of disclosure without prejudice to the other types of data on the device. For example, the question arises as to who or on whose behalf the mobile telephone's data content should be reviewed and separated from the other private or state-related data on the same device and how such other data would be protected during this exercise. The same practical problem would have arisen in respect of Mr Altayeb's mobile telephone but to a lesser extent. I am not convinced that the practicalities and cost of this exercise would have been justified.

63. Second, as I understand the position, the emails which are recorded on the mobile telephones are accessible from Saudia's own email server. Accordingly, the only additional documents which might be on the mobile telephones were instant messaging items (such as on WhatsApp). Although I suspect that there might be some relevant material included in these mobile telephones, it is unclear to me how much material there is or how substantially relevant that material might be, over and above the documents available from other sources, and therefore the prospect of obtaining such

documents might afford little practical benefit for the purposes of the determination of the issues in these proceedings.

64. I bear in mind that Mr Al Jasser and Mr Altayeb are said to have occupied a significant role in respect of the transactions which are the subject of the claims in these proceedings. Nevertheless, I am not convinced that the cost of and practical problems associated with the disclosure exercise would justify the disclosure of material which might be relevant to the issues in this action, especially where much of this material can be obtained from other sources.

Conclusion

65. For the reasons explained above, I dismiss the IAFC Parties' application, principally because the Court does not have jurisdiction to make the orders sought in respect of the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones, as they are not within the control of Saudia and because the Court does not have jurisdiction to make an order requiring Saudia to exercise best endeavours to obtain the documents held on Mr Al Jasser's and Mr Altayeb's mobile telephones for the purposes of disclosing the same in these proceedings.