Neutral Citation Number: [2021] EWHC 1162 (Fam)

Case No: FD19P00246, FD19P00380
FD19F05020 and FD19F00064

IN THE HIGH COURT OF JUSTICE
FAMILY DIVISION

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 05/05/2021

Before :

The President of the Family Division

Re Al M (Fact-finding)

Mr Charles Geekie QC, Mr Timothy Otty QC, Ms Sharon Segal, and **Mr Daniel Burgess** (instructed by **Payne Hicks Beach**) for the **mother**
Lord Pannick QC, Mr Richard Spearman QC, Mr Nigel Dyer QC, Mr Andrew Green QC, Mr Godwin Busuttil, Mr Daniel Bentham, Mr Stephen Jarmain and **Mr Jason Pobjoy** (instructed by **Harbottle & Lewis**) for the **father**
Ms Deirdre Fottrell QC and **Mr Tom Wilson** (instructed by **Cafcass legal**) for the **Children's Guardian**

Hearing dates: 13th, 15th, 16th & 19th April 2021

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

.....

THE PRESIDENT OF THE FAMILY DIVISION

Sir Andrew McFarlane P :

Introduction

1. The focus of this judgment is the determination of a number of factual allegations that have been made in the course of ongoing proceedings relating to the welfare of two children. The children are Sheikha Al Jalila bint Mohammed bin Rashid Al Maktoum and Sheikh Zayed bin Mohammed bin Rashid Al Maktoum, who are now aged 13 and 9 years respectively. Their mother is Her Royal Highness Princess Haya bint Al Hussein. Their father is His Highness Mohammed bin Rashid Al Maktoum. The ultimate purpose of the proceedings is the resolution of issues relating to the children's welfare, in particular with respect to the contact that they are to have with their father and with respect to their education.

2. In 2019 the court conducted an extensive fact-finding process. In the 'First Fact-finding Judgment' handed down on 11 December 2019 ([2019] EWHC 3415 (Fam)) a number of very serious findings were made against the father. It had been anticipated by the court and the parties that no further fact-finding process would be needed and the court could, therefore, move on to determine the outstanding welfare issues. However, events in July and August 2020 have generated a number of additional factual allegations made by the mother against the father and those acting on his behalf in Dubai. As will become apparent, it has been necessary for the court to determine a number of legal and evidential issues between the parties relating to these new factual allegations before, finally, conducting a hearing to determine whether or not any of them is established.

3. In this judgment, following a recital of the detailed factual allegations that have been made, I will describe the legal context within which the factual matters fall to be determined and the various procedural steps that have been undertaken in preparation for the final hearing, before turning to the detailed evidence and, finally, to the court's conclusions.

Factual allegations

4. The mother seeks the following findings:

   i. The mobile phones of the mother, two of her solicitors (Baroness Shackleton and Nicholas Manners), her Personal Assistant and two members of her security staff have been the subject of unlawful surveillance during the course of the present proceedings and at a time of significant events in those proceedings.

   ii. The surveillance has been carried out by using software licensed to the Emirate of Dubai or the UAE by the NSO Group.

   iii. The surveillance has been carried out by servants or agents of the father, the Emirate of Dubai or the UAE.

   iv. The software used for this surveillance included the capacity to track the target's location, the reading of SMS and email messages and other messaging apps, listening to telephone calls and accessing the target's contact lists, passwords, calendars and photographs. It would also allow recording of live activity and taking of screenshots and pictures.

v. The surveillance has occurred with the express or implied authority of the father.

5. At issue, are two basic assertions, firstly, whether any phones of those identified in paragraph 4(i) have been, in lay terms, hacked and, secondly, if the fact of hacking is established, whether it has been carried out by servants or agents of the father, the Emirate of Dubai or the UAE and whether the hacking has occurred with the express or implied authority of the father.

The legal context

6. The legal context within which factual allegations are determined is well settled and is not controversial as between the parties. The burden of proof is on the party who makes the allegations, the mother in this case, and it applies both to the fact of hacking and the question of the attribution of responsibility. The standard of proof is the simple balance of probabilities. The burden of proof is not reversible and there is no responsibility on the father in this case to prove anything. In particular, if the court is satisfied that the fact of hacking is proved, that state of affairs does not establish a 'pseudo-burden' upon the father to prove that responsibility should be attributed to some other person or State (to adopt the phrase used by Mostyn J in *Lancashire v R* [2013] EWHC 3064 (Fam)).

7. Findings of fact must be based on evidence rather than speculation. In *Re A (Fact-finding: Disputed Findings)* [2011] 1 FLR 1817, Munby LJ (as he then was) said:

> "(it is an) elementary proposition that findings of fact must be based on evidence, (including inferences that can properly be drawn from evidence) and not on suspicion or speculation."

In *Re B (Care Proceedings: Standard of Proof)* [2008] UKHL 35 Baroness Hale (at paragraph 31) said:

> "In this country we do not require documentary proof. We rely heavily on oral evidence, especially from those who were present when the alleged events took place. Day after day, up and down the country, on issues large and small, judges are making up their minds whom to believe. They are guided by many things, including the inherent probabilities, any contemporaneous documentation or records, any circumstantial evidence tending to support one account rather than the other, and their overall impression of the characters and motivations of the witnesses. The task is a difficult one. It must be performed without prejudice and preconceived ideas. But it is the task which we are paid to perform to the best of our ability."

8. The court must consider all of the evidence, and consider the picture created by the evidential jigsaw as a whole. In *Re T* [2004] 2 FLR 838 Dame Elizabeth Butler-Sloss P described the process in these terms:

> "...evidence cannot be evaluated and assessed separately in separate compartments. A judge in these difficult cases has to have regard to the relevance of each piece of evidence to other evidence and to exercise an overview of the totality of the

> evidence in order to come to the conclusion whether the case put forward...has been made out to the appropriate standard of proof."

9. The present case involves a good deal of expert evidence. It is for the court to determine the factual issues upon which expert opinion may then be offered. The role of the expert and of the judge are distinctly different as described by Ward LJ in *Re B (Care: Expert Witnesses)* [1996] 1 FLR 667:

> "The expert advises but the judge decides. The judge decides on the evidence. If there is nothing before the court, no facts or no circumstances shown to the court which throw doubt on the expert evidence, then, if that is all with which the court is left, the court must accept it. There is, however, no rule that the judge suspends judicial belief simply because the evidence is given by an expert."

10. Where more than one person or agency may be responsible for behaviour which the court has found proved, the court must be careful to ensure that a positive finding is only made against one or other on the balance of probabilities. The approach was correctly described by Lord Justice Peter Jackson in *Re B (A Child)* [2018] EWCA Civ 2127:

> "20. Even where there are only two possible perpetrators, there will be cases where a judge remains genuinely uncertain at the end of a fact-finding hearing and cannot identify the person responsible on the balance of probabilities. The court should not strain to identify a perpetrator in such circumstances: *Re D (Care Proceedings: Preliminary Hearing)* [2009] EWCA Civ 472 at [12].
>
> 21. In what Mr Geekie described as a simple binary case like the present one, the identification of one person as the perpetrator on the balance of probabilities carries the logical corollary that the second person must be excluded. However, the correct legal approach is to survey the evidence as a whole as it relates to each individual in order to arrive at a conclusion about whether the allegation has been made out in relation to one or other on a balance of probability. Evidentially, this will involve considering the individuals separately and together, and no doubt comparing the probabilities in respect of each of them. However, in the end the court must still ask itself the right question, which is not who is the more likely, but does the evidence establish that this individual probably caused this injury? In a case where there are more than two possible perpetrators, there are clear dangers in identifying an individual simply because they are the likeliest candidate, as this could lead to an identification on evidence that fell short of a probability. Although the danger does not arise in this form where there are only two possible perpetrators, the correct question is the same, if only to avoid the risk of an

> incorrect identification being made by a linear process of exclusion."

11. The father's case includes the suggestion that there may be a 'pool of possible perpetrators', if the fact of phone hacking itself is established. In *North Yorkshire County Council v SA* [2003] EWCA Civ 839, the Court of Appeal established that a person would only be included in the pool of possible perpetrators if the evidence established that there was 'a likelihood or real possibility' that they were the perpetrator. That approach was endorsed by the Supreme Court in *Re S-B (Children)* [2009] UKSC 17 where Baroness Hale said (paragraph 43) 'if the evidence is not such as to establish responsibility on the balance of probabilities it should nevertheless be such as to establish whether there is a real possibility that a particular person was involved.'

Foreign Act of State

12. As part of his response to the allegations, the father asserted in September 2020 that the 'Foreign Act of State' doctrine ['FAS'] precluded the court from investigating the allegations. After a full hearing the court (The President and Mr Justice Chamberlain) held, in a judgment handed down on 20 October 2020 ([2020] EWHC 2883 (Fam)), that the FAS doctrine did not prevent the court from carrying out a fact-finding investigation and adjudicating upon all of the mother's allegations. On 8 February 2021 the father's appeal against this decision was dismissed by the Court of Appeal (The Master of the Rolls, Moylan and Andrews LJJ; [2021] EWCA Civ 129). On 8 March 2021, the father's application for permission to appeal was refused by the Supreme Court. Thus, it was only after that date the court was able to proceed with the fact-finding hearing.

The origin of the mother's allegations

13. In order to maintain the overall fairness of the court process it has been necessary to adopt certain novel, or at least out of the ordinary, procedural measures. Resort to these additional procedural steps were necessary largely in consequence of the two separate channels through which the mother's principal solicitor, Baroness Shackleton, came to learn of possible phone hacking in the course of 5 August 2020.

14. The first contact to Baroness Shackleton was via a message from another solicitor, Mr Martyn Day of Leigh Day Solicitors, which informed Baroness Shackleton of the identity and role of a computer surveillance expert, Dr Marczak. The second, and entirely separate, source of information came in a telephone call from Mrs Cherie Blair QC who had been invited to make contact with Baroness Shackleton by a senior official in NSO Group, an Israeli based software company responsible for marketing highly sophisticated surveillance programs for the exclusive use of State Governments and their intelligence services ['NSO' or 'NSO Group'].

(a) Dr Marczak

15. Dr William Marczak is a post-doctoral researcher in computer science at the University of California, Berkeley. He is also a research fellow attached to 'Citizen Lab', which is an independent research body based in Canada with an interest in electronic surveillance.

16. Through Citizen Lab, and independently, Dr Marczak has for some years conducted research into nation-state use of spyware and hacking tools to carry out covert surveillance against journalists, dissidents and other individual targets. It will be necessary to describe Dr Marczak's methods and his evidence in more detail at a later stage. For the present a broad overview will suffice.

17. To the ordinary layman phrases such as 'spyware' or 'malware' are likely to indicate the unwelcome deposit into their computer or mobile phone of a malevolent program which then seeks to extract confidential data or otherwise function in a destabilising manner. The software program which is at the centre of this fact-finding hearing, and which is manufactured and sold by NSO Group, operates in a different manner. The software is called 'Pegasus'. A principal feature of the Pegasus operation is that at no stage during the process of surveillance should it be possible to detect any trace of its covert processes. Thus, rather than requiring the owner of the device to be tricked into clicking on a link and downloading a subversive program onto their device, where it could then be detected by conventional antivirus software, the Pegasus software operates by linking the device with a remote server or servers, which may be anywhere in the world. The server will then send 'command and control' messages to the hacked device. Each of the remote servers used by Pegasus, and there are many, must, in common with any other internet connected device, have its own individual IP address ('IP' stands for 'internet protocol'). In order to cover up the trail of transmission of messages using Pegasus to and from a hacked device, command and control signals sent down the line will be likely to pass through a number of such 'proxy servers' before connecting to the ultimate controller, being an operative in the intelligence services of a particular customer State.

18. The trigger event that may cause a target device to communicate with a Pegasus proxy server may be a single click by the device's owner to a link in a spoof text message. Alternatively connection may be made without any action on the part of the device's owner at all by an 'over-the-air' method of infection, which involves sending a 'push message' that triggers the device to connect to the proxy server.

19. It follows that it is unlikely to be possible to detect that a phone or computer has been hacked by Pegasus software if the method of investigation is limited to searching for the electronic presence of spyware or malware even with the most sophisticated and professional antivirus search mechanisms. There will simply be no trace of Pegasus on the device because it does not need to maintain a presence there even for a very short time in order to control the device's functions and harvest data from it.

20. In order to detect the deployment of Pegasus software Dr Marczak has therefore had to adopt different methods of investigation. In broad terms these have involved the following three avenues:

    (a) Identifying Pegasus proxy server IP addresses;

    (b) Identifying unconventional applications ('apps') used by Pegasus;

    (c) Spotting idiosyncratic grammar and syntax used by Pegasus software programmers.

21. A breakthrough occurred some few years ago when Mr Ahmed Mansoor, a human rights campaigner active in the Middle East, received a text message which seemed suspicious. Mr Mansoor passed his phone to Dr Marczak. Dr Marczak, having established the ability to monitor the phone's activity, clicked on the link and was able to detect and record the various IP addresses with which the device then fell into communication. Dr Marczak advised the court that the format of a spyware program's 'check-in' and a server's response to it is often unique to the particular family of spyware being used. Dr Marczak has the ability to screen computer messages across every single IP address in the world. He undertook this process with the check-in message generated by clicking on the link contained in the text message received by Mr Mansoor's phone. Dr Marczak was then able to record those IP addresses which returned a response consistent with the functioning of that seen on Mr Mansoor's phone. On that occasion he identified some 237 IP addresses in this way. He was then able to check back using historical internet scanning data to see which other IP addresses had returned the same response and he found 83 addresses which were recorded as having done so between October 2013 and April 2014. These included some IP addresses which were formally registered to NSO Group.

22. Dr Marczak labelled the historic list of sites 'version 1' and the sites found on the scan contemporaneously with the hacking of Mr Mansoor's phone as 'version 2'. He then used a period of months, or it may have been longer, to continue tracking the 237 IP addresses (version 2) found at the time that Mr Mansoor's phone was infiltrated. Whilst, no doubt to maintain maximum covert agility, many of these IP addresses are used only for a very short time, Dr Marczak noted that 3 of the 237 addresses came back into use at a later date with a new decoy trigger. By tracking this new decoy trigger in the same way and screening it across every IP address currently in use, he identified a further 1,091 IP addresses which he labelled 'version 3'.

23. Finally, and in a wholly different way, Dr Marczak has identified a particular idiosyncrasy of the Pegasus spyware based on the method used to forward data to subsequent servers. Dr Marczak labelled an earlier idiosyncrasy as the 'first fingerprint'. He has disclosed the detail of the first fingerprint and it forms part of the general process of detection that I have already described and which is already publicly available in articles and other papers that Dr Marczak has authored over recent years. Dr Marczak does not, however, understand that the further idiosyncrasy that he has spotted, and which forms his 'second fingerprint', is known to others and, particularly, not known to the NSO Group. It therefore has continuing investigative, and no doubt commercial, value to Dr Marczak and he has declined to disclose it openly in these proceedings.

24. Dr Marczak has also asserted the need for maintaining confidentiality over the identity of an individual, 'Mr X', whose telephone was, he asserts, hacked in the same time period as the alleged hacking of the phones of the mother, her solicitors and staff. I will turn in more detail to consider the evidence relating to Mr X's phone at a later stage. The purpose of referring to him now is to explain his relevance with respect to the decisions made relating to the overall fairness of the proceedings which have, indeed, been conducted on the basis that his identity has remained confidential as to the parties and the court.

25. Dr Marczak describes Mr X as 'a UAE activist'. In the summer of 2020 Dr Marczak was engaged in monitoring the internet traffic for several devices used by Mr X because

he suspected that Mr X might be targeted with spyware. Dr Marczak asserts that Mr X was previously targeted with Pegasus spyware in 2015 by the same State operator who targeted Mr Mansoor the following year. On 12 July 2020 and on 3 August 2020 Dr Marczak saw Mr X's iPhones download a substantial amount of encrypted data from servers pointed to by two domain names that he had identified as belonging to the version 4 group of NSO servers. In accordance with his usual practice Dr Marczak then followed up the lines of communication and sought to identify the IP addresses and other distinctive features of the attempted infiltration of Mr X's device. Once he had done so he then attempted to discover the identities of other victims that were communicating with these suspected Pegasus command and control proxy servers at the same time. This led Dr Marczak to spot the IP address of the firm of solicitors instructed in these proceedings by the mother, led by Baroness Shackleton, Payne Hicks Beach ('PHB'). An internet search of PHB led to news stories relating to the present proceedings involving the mother and the father. On 4 or 5 August 2020 Dr Marczak made contact with Mr Martyn Day, a London solicitor who was known to him.

26. Mr Day, in turn, made contact with Baroness Shackleton and informed her of his connection with Dr Marczak and the general area of Dr Marczak's work. He told Baroness Shackleton that Dr Marczak had identified someone at PHB as being possibly targeted by UAE directed spyware and that Dr Marczak had asked Mr Day to introduce him to PHB in order that, if they were interested, he would be able to advise them.

(b) Mrs Cherie Blair CBE QC

27. On the evening of the same day, 5 August 2020, Mrs Cherie Blair CBE QC received a telephone call from a senior member of the management team of NSO Group. Mrs Blair apparently acts as an adviser to NSO on business and human rights matters. Two witness statements from Mrs Blair have been filed in these proceedings. Mrs Blair states that the call from NSO in Israel took place at nearly midnight Israeli time. She was told that 'it had come to the attention of NSO that their software may have been misused to monitor the mobile phone of Baroness Shackleton and her client, Her Royal Highness Princess Haya.' The NSO senior manager apparently expressed great concern. Mrs Blair was told that NSO had taken steps to ensure that the identified phones could not be accessed again by their software. The NSO manager asked Mrs Blair to help in contacting Baroness Shackleton.

28. Mrs Blair was able to obtain the phone number for Baroness Shackleton and she made contact with her that evening. Again, it will be necessary to turn to more detail within Mrs Blair's evidence at a later stage.

29. It is, therefore, part of the mother's case that Baroness Shackleton was alerted to the possibility of phone hacking by two entirely separate mechanisms on 5 August 2020. The one, Dr Marczak, investigating signs of the consequence of any attempted hacking and the other, from NSO Group, originating from its source.

Dr Marczak as 'an expert witness'

30. Understandably the mother and those acting for her readily accepted Dr Marczak's offer of further advice and assistance in investigating the possibility that there had been phone hacking. Shortly after 5 August, Dr Marczak examined a number of phones said to be used by the mother and her staff, together with phones used by Baroness

Shackleton and others at PHB. He examined system diagnostic data ('sysdiagnose') from each phone together with the internet usage logs taken from the routers at the mother's London home and her home in Berkshire.

31. As a result of his investigation Dr Marczak produced a forty-two page 'witness statement' dated 7 September 2020 in which he concluded 'with high confidence' that the phones of the mother, Baroness Shackleton and Nicholas Manners (another solicitor, and since December 2020 a partner, at PHB) had been hacked by a single operator of NSO Group's spyware. On the basis that any such operator would be a nation State he concluded 'with medium confidence' that the government in question is the UAE Government. Further, there was evidence that the phones of the mother's Personal Assistant and two others on her staff had also been hacked.

32. The mother issued her application to this court seeking findings of fact on 7 September 2020. It is thus the case that Dr Marczak did not enter the proceedings in the manner conventionally used for the obtaining of expert evidence. He was not formally instructed in the manner required of the procedural rules before he began his work and by the time he had produced his written statement he had engaged in extensive and detailed communication with the mother, her security staff and those at PHB. Whilst, given the sequence of events that I have described, and given the need for the mother and her advisers to have the assistance of bespoke expertise in this narrow area of computer science, it is understandable that Dr Marczak entered the process and the application of the fact-finding were made in the way that they were and in the sequence that they were, that state of affairs generated a need for the court to adopt a careful strategy permitting the mother to deploy and rely upon the evidence of Dr Marczak, whilst, at the same time, conducting a process that was fair to the interests of the father and the children. In addition the process adopted was aimed at allowing the court to test the evidence which, at the start of the process, came from one source, Dr Marczak, supported at that stage to a degree by non-specific hearsay evidence originating from NSO and reported to the court subsequently in the statements of Mrs Blair.

Procedural Decisions

33. I have taken time to describe the procedural and evidential landscape as it existed prior to and at the time of the mother's application for a further fact-finding hearing in order to make sense of the procedural steps that were then undertaken which were as follows.

34. In order to meet the unusual circumstances generated both by the method by which the evidence was introduced into the proceedings, and by the scientific complexity and sophistication of its content, it was necessary for the court to consider a range of procedural steps with the aim of achieving a fact-finding process that was both viable and fair to all the parties. These included the following:

    (a) appointment of a confidential scientific adviser to the father and his legal team;

    (b) appointment of an independent Single Joint Expert ['SJE'];

    (c) communication between the court and NSO Group;

(d) appointment of independent counsel to review the extent of disclosure/redaction of all communications between Dr Marczak, the mother, her staff and her legal advisers;

(e) appointment of a second independent counsel to review information about Mr X;

(f) the presentation of the father's case.

35. I propose to describe each of these steps in turn.

(a) Instruction of a specialist scientific adviser to the father

36. During a case management hearing on 6 October 2020, Lord Pannick QC, leading counsel for the father, sought permission for the instruction of a cyber-security expert to advise the father and his lawyers on a confidential basis. In the circumstances, the application was not actively resisted by the other parties and permission was given. I dealt with the issue shortly in one paragraph in my judgment on that day:

> "So far as the father being able to instruct his own privileged expert for the purposes of informing him and his team of the technical aspects, there is really no objection to that. I give that course my blessing as a wholly exceptional course taken in these proceedings, because the nature of the question to be considered by any such expert is wholly outside the comprehension of any ordinary human being and can only really be understood by someone of immense and particular experience and knowledge."

37. Paragraph 15 of the order of 6 October set out the basis upon which permission had been given:

> "Subject to the following conditions the father shall have permission, in the wholly exceptional circumstances of this case, to obtain advice from an expert or experts on cyber security on a privileged basis for the purposes of considering Dr Marczak's witness statement. The conditions are:
>
> a) The name of the expert(s) must be made known to the court and parties before the instruction is effected;
>
> b) The expert(s) must provide an undertaking (in like form as provided by the father's expert on security costs) to the court as to confidentiality prior to receipt of any papers;
>
> c) The statement of Dr Marczak dated 7 September 2020 but no other court document may be disclosed to the expert(s).The statement may be provided in unredacted form save that all redactions as to the phone names, phone individual and phone numbers should remain redacted;
>
> d) None of the data supplied to Dr Marczak for analysis shall be supplied to the expert(s).
>
> e) Permission to the father to apply to the court in relation to c) and d) above for the restrictions to be removed or varied."

38. The appointment of a shadow technical adviser to the father, whose advice and opinion were not required to be disclosed into the proceedings, was a wholly exceptional step. It was in part justified by a need to level up the forensic playing field in the early stages of the case during which the mother had open access to expert advice from Dr Marczak, yet the father had none. In the light of the highly technical content of Dr Marczak's statement, it was important that the father and his advisers should have their own source of specialist advice to enable them to understand the detailed content of Dr Marczak's statement and to be advised upon it.

39. At all stages, and on a number of occasions, the court has made it plain to the father that it would favourably consider an application by him for the instruction of his own expert witness, but that that instruction would have to be on the ordinary basis involving full and open disclosure of both the process of instruction and any resulting expert opinion. The father has at all times declined to make such an application.

40. The father instructed a firm based in Israel, Sygnia, as the special technical adviser for which permission had been granted to him. Despite the clear boundaries upon the extent of that instruction established by the court's decision, Lord Pannick QC has consistently pressed for the disclosure of the core data in the form of sysdiagnose files extracted from the phones of the mother, her staff and her solicitors, together with the records of network logs and Dr Marczak's own records of IP addresses, domain names and applications which he asserts are relevant to the Pegasus software. Lord Pannick has been plain that the purpose of disclosure was not to inflate the status of Sygnia into an expert whose opinion would be open to the court and filed in the proceedings. Lord Pannick nevertheless asserted that it is a basic requirement of fairness for the father's adviser to examine the core material upon which Dr Marczak's opinion was based in order to provide confidential advice to the father and his lawyers.

41. The court has consistently refused the father's applications in this regard. Although sub-paragraph (e) of the order granted permission to the father to apply to vary the embargo upon disclosure, I have been clear that the unprecedented relaxation of the long established approach to the open instruction of expert witnesses, whilst necessary and proportionate at the time that leave was given in this case, should not be extended further. Refusal was justified firstly as a matter of ordinary principle, but secondly because, by then, the court had embarked upon the instruction of a SJE and thirdly because the father was fully able to apply for his own FPR 2010, Part 25 compliant expert witness, but chose not to do so.

42. The father's access to, and receipt of advice from, Sygnia has, so far as the court is aware, continued throughout the trial process. It was no doubt available to inform the questions raised by the father's legal team during the instruction of the SJE and at the expert's meeting. It was also available to inform the lines of questioning during the extensive cross-examination of Dr Marczak.

(b) Single Joint Expert

43. Finding a source of expertise with sufficient knowledge and experience to act as a SJE on the question of whether or not the Pegasus software had been deployed to hack the phones of the mother and others proved to be a most difficult task. The endeavour was no doubt complicated by my insistence that it should be taken in stages, with the expert

only being exposed to Dr Marczak's statement at the second stage, once they had conducted their own examination of the sysdiagnose files and other core data.

44. The first SJE that was instructed, IntaForensics Ltd, undertook the first stage of investigation and reported that there was no sign that any of the relevant devices had been the subject of surveillance. I pause there to observe that, if it is the case that any of these phones have been infiltrated by Pegasus software, it is no surprise that a search for viruses, spyware or malware produced a 'nil' return as a principal selling point of Pegasus is said to be that it leaves no trace.

45. However, when Dr Marczak's statement was disclosed to IntaForensics they quickly responded indicating that they were unable to continue with the instruction. This message was followed up in a report dated 16 March 2021, which stated that the findings in IntaForensics' previous reports should not be relied upon. The report confirmed that the unusually named apps identified by Dr Marczak and the behaviour observed in these apps attempting to access standard features on the phones had been observed by IntaForensics. There was evidence that five of the six phones may have been the subject of surveillance and/or interference from an unidentified source.

46. The court is grateful to IntaForensics for taking up the instruction and being prepared to act as the SJE in this case. Because of the staged level of disclosure that the court insisted upon, IntaForensics were not to know the scale and character of the task for which they were being recruited and they command the court's respect, rather than criticism, for flagging up their inability to complete the instruction as soon as the situation became clear.

47. Fortunately, it was possible to identify a replacement SJE who was able to take up the instruction and respond quickly within the court's wider timetable. The expert instructed was Professor Alastair Beresford, who is Professor of Computer Security at the Department of Computer Science and Technology in the University of Cambridge. Professor Beresford's research work examines the security and privacy of large scale networked computer systems, with a particular focus on networked mobile devices such as smartphones, tablets and laptops. He has worked on mobile computing platforms in either industry or academia since 1995.

48. Before his instruction Professor Beresford was told that the court was interested in understanding whether or not the phones concerned had been infiltrated by the Pegasus software and that the court had received expert advice from Dr Marczak (whose general work was known to Professor Beresford). Professor Beresford was not given access to Dr Marczak's statement at that stage. Following his initial report which, like that of IntaForensics, confirmed that there was no trace of the Pegasus software on the sysdiagnose files or network logs, Dr Marczak's statement was then disclosed to Professor Beresford and there followed a short period of written communication through further written statements or reports orchestrated at the court's direction and culminating in an expert's meeting conducted by Ms Melanie Carew of Cafcass Legal and at which questions submitted by all three parties were addressed by Dr Marczak and Professor Beresford.

49. Professor Beresford gave oral evidence at the fact-finding hearing and was cross-examined by counsel on behalf of both the mother and the father.

(c) NSO Group

50. A full account is given of the involvement of NSO Group in the proceedings at paragraph 94 to 110. In terms of process, during October and November 2020 the court made directions requesting NSO to provide an account of the investigation that it had assured PHB it was carrying out. In the event a letter dated 14 December 2020 was sent to the court, via CAFCASS, by NSO. The relevant content of this letter is described at paragraphs 102 to 105. Since receipt of that letter no party has applied for a direction seeking to engage further with NSO either by way of requesting additional information or otherwise. On the first day of the fact-finding hearing Lord Pannick suggested that NSO might be asked a narrow and specific question arising out of the letter that had been received over three months earlier. This was expressly a 'suggestion' and not an application for a direction. After observations from the court as to a possible wider question that might be asked of NSO, the suggestion was not pursued.

(d) Independent Counsel

51. In early December 2020 PHB disclosed details of the extensive communication that had taken place between the mother's staff and PHB with Dr Marczak. The communication, which was largely in the form of emails, text messages or other electronic communication, when committed to paper ran to some 900 pages. Whilst much of the content was open to be read, there was, nevertheless, a very substantial element that had been redacted. Basic codes had been attributed to each redacted section indicating the general reason said to justify non-disclosure. Whilst the father's legal team accepted that some redaction was justified, for example withholding the names of security staff or an individual's telephone number, they questioned the extent of the redaction that had been undertaken and the range of categories relied upon.

52. Following full submissions from all parties, the court determined that the redaction process should be audited and checked by a senior member of the Bar, who had been security cleared for instruction in other cases as a special advocate, and who would act as independent counsel for this purpose (see judgment [2021] EWHC 156 (Fam)).

53. The court is grateful to Jennifer Carter-Manning QC for taking up instruction as the independent counsel and for the diligent manner in which she has plainly discharged her instruction. Whilst the arrangements put in place by the court allowed for any dispute between the independent counsel and PHB to be referred to me for final determination, in the event all matters were resolved without the need for my involvement. The result was that a substantial number of redacted passages were opened up and disclosed to the father's legal team, albeit only a few working days before the start of the hearing. This material was referred to extensively during cross-examination of Dr Marczak on behalf of the father.

(e) Mr X

54. Mr X, who features in Dr Marczak's analysis on the basis described at paragraph 24 above, is of relevance for two separate reasons. Firstly, irrespective of his underlying identity, Dr Marczak asserts that Mr X's telephone was targeted by Pegasus in a way that revealed the deployment of version 3 or version 4 IP addresses and the second fingerprint, domain names and apps that he attributes to Pegasus. The alleged hacking of Mr X's phone happened in precisely the same time window at the end of July and

early August as the asserted infiltration of the phones relevant to these proceedings. Mr X is therefore directly connected to Dr Marczak's analysis on the first question of whether or not the mother's and other phones in this case have been hacked. Secondly, Dr Marczak asserts that Mr X is a known 'UAE activist' and that the fact, as Dr Marczak asserts is the case, that his phone was hacked by Pegasus and that the same State operator was involved in hacking Mr X's phone and also the phones of the mother and those connected with her is, claims Dr Marczak, of relevance in attributing the identity of the hacking to the UAE.

55. The father has consistently sought an order requiring the disclosure of Mr X's identity. Dr Marczak is unwilling to disclose it without Mr X's consent. The mother contends that Mr X should be told who the parties are to these proceedings before he is asked whether or not he consents to the disclosure of his identity to those parties. The father refuses to agree to the disclosure of his identity to Mr X. There was, therefore, a standoff.

56. The court has no knowledge of the identity of Mr X over and above that which is stated in Dr Marczak's written statement. It is therefore simply not possible for me to assess what risk, if any, might open up for Mr X were his identity to be disclosed to the father and his advisers in the UAE were I to direct it. Whilst, at one end of the spectrum, disclosure may have no consequence for Mr X, at the other it is possible to contemplate exposing him to actions which might engage rights under Article 2 or Article 3 of the European Convention of Human Rights. Being mindful that Mr X's identity is irrelevant to the first question, namely whether hacking has taken place, which turns entirely on technical evidence, and given my preliminary view that Mr X's involvement and what is said about him can only be of peripheral probative value on the second question of attribution, I have consistently refused to require his identity to be disclosed into the proceedings. However, in order to at least provide some check on Dr Marczak's assertion that Mr X is 'a UAE activist', I sanctioned the instruction of a second independent counsel, Gareth Weetman, who was tasked with undertaking a search via Google and other public source material to see what was said about Mr X.

57. The court is most grateful to Mr Weetman for undertaking this role. He has provided a schedule recording each reference that he was able to find to Mr X and I will turn to that material in due course.

(f) The Father's Case

58. In contrast to the first fact-finding hearing, where the father instructed his lawyers to vacate the courtroom and play no part in the process, the father has been represented throughout the current process by a very substantial legal team of the highest quality. On the question of jurisdiction, the issue relating to FAS was pursued to a full appeal and an application of permission to appeal to the Supreme Court. In addition, the court has heard applications upon, and made determinations about, a wide range of procedural matters raised by the parties. None of the court's determinations has been the subject of an appeal.

59. Unusually in a fact-finding process, and in contrast to the first fact-finding hearing, the father has chosen not to file any evidence whatsoever on the issues. The only material filed on behalf of the father is open source media and other articles to which the court has not been specifically taken other than via limited reference during cross-

examination. In addition the court has received position statements and skeleton arguments which put the mother to proof of the allegations and which, from time to time, have made varying suggestions as to other States that may be responsible for any hacking that may be proved, other than the father or those acting on his behalf.

60. In his skeleton argument for the fact-finding hearing under the heading 'The father's response to the mother's allegations' it is asserted that 'the mother has not established on the balance of probabilities', the following matters in particular:

- that there has been surveillance of the relevant mobile phones,
- that such surveillance was carried out using NSO software,
- that such software was licensed to the UAE or Dubai,
- that the surveillance was carried out by the UAE or Dubai,
- that the alleged technical capabilities of the NSO software are established, and
- that the alleged surveillance occurred with the father's express or implied authority.

The case has been conducted on the basis that the father can neither confirm nor deny that the UAE (including Dubai) has or had any contract with NSO for the supply or use of the Pegasus system.

61. In circumstances where the father has filed no evidence at all in response to the allegations, where he has not sought leave to instruct his own open court expert, where there is effectively no substantial dispute between the evidence of Dr Marczak and that of the SJE and where the father does not seek to put forward a positive case before the court (other than to make various and varying suggestions), it might be possible to justify closing down or severely limiting the father's ability to contest the factual allegations. At this hearing, however, the court adopted the contrary course. Lord Pannick was permitted full and equal range to that attributed to Mr Geekie QC and the mother's legal team to advance arguments prior to the hearing and in closing submissions. Most importantly, Mr Andrew Green QC, on behalf of the father, conducted an extensive, most thorough and professionally adept cross-examination of Dr Marczak which was spread over two days and lasted at least seven hours.

The previous fact-finding judgment

62. The first fact-finding judgment, given in December 2019, made wide ranging findings against the father. These included the forced abduction of one of the father's older daughters, Princess Shamsa, from England in 2000 by those acting on behalf of the father, the restraint and house-arrest of another daughter, Princess Latifa, in 2002 and in the years following, the capture and forced return to Dubai of Princess Latifa from a boat in international waters off India by Indian Special Forces and the Dubai military in 2018 and her subsequent house-arrest, a campaign of fear and intimidation against the mother prior to her departure from Dubai in April 2019 and the campaign of harassment and threats that continued once she had arrived in England.

63. At paragraph 181 of the judgment I concluded that the findings established a consistent course of conduct by the father and those acting for him, over the course of two decades, 'where, if he deems it necessary to do so, the father will use the very substantial powers at his disposal to achieve his particular aims'.

64. It is not necessary to set out the earlier findings in more detail here, but before moving on from reference to the first fact-finding hearing it is necessary to correct a statement made by the father following the judgment in December 2019 and issued by his solicitors, Harbottle and Lewis. The father stated:

> 'As Head of Government I was not able to participate in the Court's fact finding process, this has resulted in the release of a "fact-finding" judgment which inevitably only tells one side of the story.'

That statement was at least disingenuous. It did not give a true account of the father's position before the court where, despite his position as Head of Government, the father had filed two full witness statements, where others named by the mother as being implicated could have given evidence on his behalf, and where he was represented by a large legal team who could (as at the present hearing) have been deployed to cross-examine the mother's witnesses and make submissions, but who were, on the father's instructions, simply withdrawn from the courtroom.

Fairness

65. Having described the various features of these proceedings which are to varying degrees unusual, it is possible to make the following observations as to fairness:

a) every single piece of evidence that has been admitted into the hearing has been fully disclosed to the father and his team. I, as the judge, have not seen any evidence that the father's lawyers and those acting for the children have not also seen. In so far as material has not been admitted into the hearing and has been withheld from disclosure to the father, it is not evidence in the case and forms no part of the material upon which I will make my decision.

b) In so far as Dr Marczak has examined and commented upon electronic data which has not been disclosed to the other parties and the court, that data has been fully examined and checked by both IntaForensics and Professor Beresford who, subject to minor corrections, have confirmed its accuracy.

c) In so far as Dr Marczak has relied upon data drawn from his investigations over the past five years and more, that data (including the 'second fingerprint') has been disclosed to Professor Beresford who, in turn, has reported upon its validity and accuracy in his evidence.

d) In so far as part of the content within the extensive records of communication between Dr Marczak and others relating to this case has not been disclosed to the court, the father or the children's guardian, that material has been fully considered and, where appropriate, challenged on the issue of disclosure by independent counsel instructed for that task.

e) In so far as the identity of Mr X has not been disclosed to the father, the children's guardian or the court, details of his identity have been given to the second independent counsel who has conducted searches of public facing material and reported to the court.

f) The father has at all times been able to apply to have his own openly instructed expert within the proceedings who would be instructed in accordance with the court rules and subject to the same stringent conditions as Professor Beresford.

g) Despite having filed no evidence at all and having not put forward a positive case before the court, the father has continued to enjoy all the rights of a party to participate in the proceedings including making full submissions through counsel and conducting a thorough and extensive cross-examination of Dr Marczak.

h) The fact-finding hearing, which was conducted entirely remotely over a Teams link, was open for the attendance of any UK accredited media representative. A number of media representatives attended throughout the hearing. In addition full transcripts of all of the interim and case management hearings which have taken place in the lead up to the fact-finding hearing have been made available for scrutiny by the media representatives.

Dr Marczak's written evidence

66. Dr Marczak is, on his own account, a computer scientist who has taken a particular interest in cyber security and covert surveillance. In particular he is the leading author of a series of articles published over recent years by 'Citizen Lab', an interdisciplinary laboratory based at the University of Toronto. The articles have sought to expose alleged abuses of spyware (in particular Pegasus) to target individuals (for example journalists or political activists). Dr Marczak's work in this regard has focussed on the Middle East and the UAE in particular. The father, rightly, submits that Dr Marczak entered these proceedings with a pre-established mindset and perspective on these issues. There is a danger, which I also accept, that Dr Marczak's goal was to establish that misuse of Pegasus software attributable to the UAE/Dubai had taken place. Lord Pannick, again rightly, submits that the court should be cautious both to avoid 'confirmation bias' in Dr Marczak's evidence and in the court's own approach to it.

67. Despite the unconventional route by which Dr Marczak's evidence has come before the court, I concluded at an early stage that it was right in these proceedings relating to children for it to be admitted. If the mother's case is right that her phone and those of others close to her have been hacked by this highly sophisticated surveillance software, it is almost inevitable that she would not know that this were the case unless either she were alerted by a whistle-blower within the operating organisation (which to a degree is her case) or she was alerted to the potential for hacking by an individual such as Dr Marczak who could only confirm the possibility that there had been hacking after he had examined all of the relevant devices and networks. In contrast to a more ordinary case where a party may make a factual allegation which is then investigated by an expert witness within the context of court proceedings, the mother in this case did not know

that she had an allegation to make until Dr Marczak had conducted his investigation and told her of his conclusions.

68. I have, however, been cautious to ensure that Dr Marczak is not regarded as an independent expert before the court. He comes to the court both as an individual who had reached his conclusions before the case commenced and one who is open about his interest in investigating covert surveillance activities which are attributable to the UAE. I have at all times been keen to follow and understand the science to identify such solid ground as there may be within it, rather than considering more general assumptions and assertions that Dr Marczak may make regarding the identity of the perpetrator.

69. Dr Marczak's evidence inevitably descended into a good deal of detail both as to the operation of the Pegasus software system and the various strategies that he has employed to detect it. Much of Dr Marczak's work in that regard is in the public domain. For that reason, for reasons of general public policy as to the disclosure of the workings of a system which is of importance to security services around the world and, most importantly, because it is not necessary to do so, I will not include such detail within this judgment.

70. I have already (paragraphs 20 to 23) described the basic method of investigation that Dr Marczak has developed to identify and track use of the Pegasus software over the years. I therefore turn to record the steps that he took once his invitation to assist PHB and the mother had been accepted in early August 2020.

71. Dr Marczak had noticed suspicious activity in mid-July and then again in early August on several devices used by Mr X. In particular he identified a number of domain names associated with IP addresses that he had previously identified as being connected with NSO in recent times ('version 4'). Also, the way in which Mr X's phones were made to communicate with the suspicious domain names, by sending a sequence of 'knocking' packets before it sent a request, rather than simply making contact, further suggested that covert surveillance was being undertaken. 'Knocking' in this sense is similar to a resident not answering the door to their home unless a knocker taps in a specific previously agreed pattern of knocks.

72. In addition, Dr Marczak observed that a number of unusually named applications ('apps') were active on the phones and were attempting to communicate with Pegasus command and control proxy servers. Dr Marczak assumed that these unusually named apps represented Pegasus spyware.

73. Initially, Dr Marczak provided PHB and the mother's staff with the IP addresses and domain names that he had observed on Mr X's phone as well as other IP addresses and domain names drawn from his wider research so as to enable those to be compared with data on the network logs at the mother's homes and at PHB. Dr Marczak then examined the sysdiagnose data from each of the relevant phones.

74. Examination of the phone attributed to Baroness Shackleton showed that an unusually named temporary app had connected with two IP addresses that were the same as those to which Mr X's phone had also linked. In addition the temporary app attempted to access three of the standard apps on the phone namely 'preferences', 'siri' and 'mail'. The 'mobile container manager' logs from Baroness Shackleton's phone also showed

several earlier cases where other apps with odd names had attempted to access the same standard apps on her phone without the user's permission.

75. The sysdiagnose from the phone attributed to Nicholas Manners showed that another unusually named temporary app had, between 3 and 5 August, attempted to communicate with six different IP addresses related to Pegasus domain names. Another temporary app had attempted to access the same three pre-installed standard apps on his phone together with a fourth one, 'notes'.

76. The network logs recording activity at the mother's Berkshire home showed that between 17 July and 3 August six attempts were made to access a particular domain name connected with Pegasus. Further, another Pegasus domain name and a further suspicious domain name uploaded 265 megabytes of data from the mother's phone. By way of illustration, that amount of data equates to some 24 hours of digital voice recording data or 500 photographs. It is a very substantial amount of data. Further, the sysdiagnose data from the mother's phone demonstrated that a temporary unusually named app had sought to communicate with the same four pre-installed applications as had been the case on Mr Manners' phone.

77. Signs of infiltration on the further three phones, namely those attributed to the mother's Personal Assistant and two of her security staff, were less specific in terms of directly connecting to Pegasus, however the same named temporary apps were found on those three phones and each of which had attempted to access the same pre-installed standard apps.

78. Dr Marczak stated his conclusions in his first witness statement as follows:

> "I conclude that the following phones were successfully hacked by NSO Group's Pegasus spyware between the dates indicated. I have "high confidence" in this conclusion, which means that I do not believe there are any plausible alternative conclusions that could explain the data I have gathered. The phones may not have been under continuous surveillance during the entire period, as the Pegasus spyware is not necessarily "persistent", i.e. turning the phone of and on again may remove the spyware and necessitate re-infection. It is also possible that additional phones were infected, or that the following phones were also infected on prior dates and there is insufficient log data in the sysdiagnoses to establish this. [he then listed the six phones]
>
> I conclude with high confidence that Nick Manners, Princess Haya and Baroness Shackleton were hacked by a single operator of NSO Group's spyware. I conclude with high confidence that this operator is a nation-state, because NSO Group's CEO asserted this in a sworn declaration and extensive reporting on NSO Group has yielded no evidence to the contrary. I conclude with "medium confidence" that the government in question is the UAE Government, meaning that I believe there are other conclusions as to the identity of the government that are within the realm of plausibility, but that the UAE Government hypothesis seems to be the most likely conclusion. The spyware

> on the phones of Nick Manners, Princess Haya and Fiona Shackleton communicated with some of the same IP addresses and domain names as the spyware on Mr X's phone. Mr X is a UAE activist who was previously targeted by the same Pegasus operator that targeted Ahmed Mansoor, a well-known UAE activist, in 2016. The UAE Government is known to be a customer of Pegasus.
>
> There is at present no technical evidence to suggest which government operator hacked the phones of Princess Haya's Personal Assistant [and the two unnamed members of her security staff] with Pegasus. However, given the lack of evidence of a second operator targeting individuals linked to Princess Haya, I conclude that it is more likely than not that these targets were hacked by the same operator as targeted Nick Manners, Princess Haya and Fiona Shackleton.
>
> It is hard to say for certain what data Pegasus exfiltrated from the hacked phones, though according to a 2016 analysis of Pegasus, its capabilities included: tracking: tracking the targets location; reading messages including SMS and email, and from a variety of apps including iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype, Line, Kakaotalk, WeChat, Surespot, Imo.im, Mail.Ru, Tango, VK and Odnoklassniki; listening in on calls including phone calls, as well as calls placed through the WhatsApp and Viber apps; accessing the target's contact list, calendar, saved passwords, photos and other files, browsing history, and call logs; recording live activity by enabling the microphone; and taking screenshots and pictures through the camera."

79. Separately, Dr Marczak found that one of the phones attributable to the mother's security staff had a sysdiagnose which showed that on five dates in November 2019 three further Pegasus apps attempted to access software on the phone without success.

80. On 7 February 2021 Dr Marczak filed a second witness statement commenting upon the initial report of the first SJE, IntaForensics. It is not necessary to refer to the detail of that statement here. In a third witness statement dated 1 March 2021, Dr Marczak gave greater detail as to the process he had adopted when analysing the logs from the wifi system of the mother's home with particular reference to the phone that he understood was attributed to her. The statement included a table recording no fewer than eleven occasions when data had been downloaded and then uploaded between the mother's phone and destination IP addresses or domain names which Dr Marczak attributes to Pegasus. In particular, this includes the occasion already referred to when two hundred and sixty five megabytes of data was uploaded.

81. Dr Marczak's final witness statement, dated 28 March 2021 engages with specific points that had by then been raised by Professor Beresford. They are matters of detail and do not require recording here.

82. Finally Dr Marczak provided further information in two documents explaining his analysis of the purported targeting of Mr X's phone by Pegasus in 2015. In one of these documents Dr Marczak gives an extensive explanation of a method of calculating the approximate location of individual servers where the 'last-modified' header of an activity is either precisely the same, down to the last second, as GMT or is precisely and exactly a whole number of hours different (with no difference as to the minutes and seconds). Thus suggesting that the activity happened at precisely the same time, but was measured at a different clock time, precisely one hour different, because the clock of the proxy server was calibrated in accordance with local time in a different time zone. On the basis of this analysis Dr Marczak inferred that two of the suspicious Pegasus servers which appeared in links sent to Mr X in 2015 may have been run by the same Pegasus operator because all three IP addresses pointed to by these servers had a single inferred time zone of GMT+4 which is the time zone of the United Arab Emirates as well as other countries in that region.

Professor Beresford: written evidence

83. I have already set out Professor Beresford's academic post and his relevant experience in short terms at paragraph 47. In his first report dated 9 March 2021 he concluded:

> "I have found no evidence that the iPhones in question have been the subject of surveillance and/or interference. This finding is not necessarily in conflict with those of Dr Marczak since I lack the technical details of how recent versions of the Pegasus spyware operate and manifest themselves as evidence in sysdiagnose files and in network logs. Access to further information on the operation of Pegasus from Dr William Marczak or another source may allow me to identify such evidence."

84. By the time of his second report, 24 March 2021, Professor Beresford had reviewed the overall methodology used by Dr Marczak as outlined in his three witness statements as well as in the core data that had been provided to him. He concluded:

> "The overall approach taken appears sound and I have been able to confirm much of the technical detail."

85. Professor Beresford raised a number of detailed questions about precise entries and reference numbers in a small number of points recorded in the reports of Dr Marczak and Intaforensics. He sought clarification with respect to these various matters.

86. Professor Beresford described the proposed method of searching for command and control proxy servers as 'sound', however he observed it may produce incomplete results if connections from specific machines are blocked or techniques such as port knocking are required to elicit a response. Secondly, the method of scanning the entire internet is, he confirmed, 'a reasonable means to find servers which exhibit a response consistent with a C and C or installation server'. Professor Beresford had been sent underlying detail relating to Dr Marczak's 'version 3' fingerprint and he concluded that 'the overall setup used looks reasonable however a more detailed description of the method would be welcome.'

87. With regard to Dr Marczak's 'second fingerprint', details of which have been withheld from the court and the father's team, Professor Beresford said this:

> "(Dr Marczak) also describes a second fingerprint which Dr Marczak has developed. I have been supplied with the technical details of this fingerprint. The method is distinct from the approach used for fingerprinting version 1, version 2 and version 3 Pegasus infrastructure. The idea proposed appears sound however I have some technical questions on the degree to which the new method might lead to false positives (asserting that an IP address is part of the Pegasus infrastructure when it is in fact not) as well as false negatives (failing to notice that an IP address is part of the Pegasus infrastructure when it is). My questions are perhaps best used as discussion points with Dr Marczak if this is permitted."

88. With respect to 'version 1' and 'version 2' Professor Beresford advised:

> "The above methodology provides evidence that 'version 1' and 'version 2' responses were linked to NSO Group. While I have some outstanding questions in terms of checking the detail, the overall approach offers a route to demonstrate that the spyware installation intended for Mr Mansoor came from NSO group and therefore it is likely to represent their product Pegasus."

89. With respect to Mr X Professor Beresford was unable, on the information before him, to identify the domain name regarded as suspicious as being one connected to 'version 4' proxy servers.

90. In an addendum dated 28 March 2021 Professor Beresford confirmed that his investigation demonstrated that the methodology and more detailed arguments given by Dr Marczak on a discrete point in his second witness statement were sound. In a further addendum dated 4 April 2021 Professor Beresford returned to the topic of the 'second fingerprint' in the light of further information that he has been given. He concluded:

> "The effectiveness of this technique rests on the fact that the fingerprint produced is distinguishing in the sense that it is able to detect all instances of Pegasus proxy servers (i.e. no false negatives) and does not accidentally claim unrelated services are Pegasus proxy servers (i.e. no false positives). Given the set of tests Dr Marczak includes, the range of possible variants is large. Having reviewed the fingerprint information and the data from the rest of the scan I am satisfied that the fingerprint is distinctive and therefore the rate of false positives or false negatives will be low."

91. Following the experts' meeting Professor Beresford provided a further final report on 9 April tying up a number of details and, in particular, concluding that there was good evidence linking Dr Marczak's 'version 2' and 'version 3' servers.

The experts' meeting

92. An experts' meeting was held remotely on 6 April 2021. It was attended by Dr Marczak and Professor Beresford, and chaired by Melanie Carew of CAFCASS Legal. Detailed questions for the experts had been submitted by the legal teams for each parent prior to the meeting.

93. It is not necessary to rehearse the detail of this meeting, which included the resolution between the two experts of a number of matters of outstanding detail and resulted in a unanimity of opinion between them.

NSO Group

94. I have already described in summary terms how the NSO Group first sought to make contact with Baroness Shackleton via Mrs Cherie Blair QC. It is now necessary to record more detail of the unchallenged evidence of the Baroness and Mrs Blair in this regard.

95. In her first statement to the court Mrs Blair stated that she received a telephone call on the evening of 5 August 2020 from 'a senior member of the management team of NSO', who she was specifically asked not to name. She states:

> "I was told by the NSO senior manager that it had come to the attention of NSO that their software may have been misused to monitor the mobile phone of Baroness Shackleton and her client, Her Royal Highness Princess Haya. The NSO Senior Manager told me that NSO were very concerned about this and asked me to contact Baroness Shackleton urgently so that she could notify Princess Haya. The NSO Senior Manager told me they had taken steps to ensure that the phones could not be accessed again."

96. Mrs Blair was able to contact Baroness Shackleton and inform her of the information received from NSO. Baroness Shackleton told Mrs Blair that she had, on the same day, been contacted by a senior partner in another city law firm delivering a very similar message. After that call Mrs Blair spoke again to the NSO Senior Manager who 'confirmed that NSO had not contacted another city firm to approach Baroness Shackleton.'

97. Mrs Blair is clear that she has never been told the identity of the NSO customer suspected of carrying out this alleged surveillance. She does, however state:

> "It had always been my assumption that 'the country' (or the government agency/security agency within this country) was Dubai. This is because I assumed no one else would have an interest in targeting Princess Haya and Baroness Shackleton. I have not had any explicit confirmation from NSO who their client was. However, during a conversation with the NSO Senior Manager, I recall asking whether their client was the 'big state' or the 'little state'. The NSO Senior Manager clarified that it was the 'little state' which I took to be the state of Dubai."

98. At this point it is right to explain that, in terms of a 'State', the Emirate of Dubai is a constituent member of the sovereign State of the United Arab Emirates. Dubai is not therefore a sovereign State itself, it is a federal state within the sovereign State of the UAE. Loose use of language, including by the court in the earlier fact-finding judgment and elsewhere, has at times referred to Dubai as a State, which, in the sense of a sovereign State, is incorrect. NSO' Chief Executive Officer has made it clear that it only enters into contracts to supply Pegasus software to sovereign States.

99. On 11 August 2020, Cherie Blair spoke again on the telephone with Baroness Shackleton at PHB. The call was attended by two other members of the family team at PHB. An attendance note of that call made by PHB has been shown to Mrs Blair who has confirmed that it is consistent with her broad recollection. She did not, herself, take notes of the call. The note states that during the call 'CB confirmed it was the Emirate of Dubai, not UAE in general, who she was talking about.'

100. On 28 August 2020, solicitors directly instructed by NSO Group (Schillings) wrote to PHB confirming that their client was 'investigating this matter' and could not confirm any factual information at that stage. A subsequent letter from Schillings, dated 1 September 2020, stressed that the identity of NSO clients is strictly confidential and that Mrs Blair was not privy to the identity of any of NSO's clients. The letter also stated that 'since 5 August 2020…onwards our client has no reason to believe that its technology is being or can be, deployed in the UK by any government agency against those identified in your letter, either by name or by reference to their roles. Whether there had been any breach prior to this is the subject of our client's investigation.'

101. In response to a direct request made by the court, NSO provided a letter, dated 14 December 2020, setting out an account of its investigation and subsequent actions. The court is grateful to NSO Group, who are outside the jurisdiction of this court, for responding to its request.

102. The letter includes general background information including the following:

> "NSO's purpose is to create technology which is licensed only to government intelligence and law enforcement authorities to enable those intelligence agencies and authorities to identify, investigate and prevent serious crimes and terrorism, and otherwise protect public safety.
>
> NSO is committed to aligning with the UN Guiding Principles on Business and Human Rights ('UN Guiding Principles'). Human rights protections are integrated in all aspects of NSO's work. Our desire to implement the highest ethical standards is demonstrated by NSO's detailed Human Rights Policy, and Transparency Statement of Principles, whereby we publicly report on the effectiveness of our policies and procedures.
>
> NSO takes its responsibility for ethics and accountability very seriously. The Human Rights Policy, Transparency Statement, and Whistleblower Policies feature prominently on our website and undergo constant review.

> ...
>
> NSO does not condone, assist in or encourage the use of its software for purposes other than the agreed purposes specified and identified in the contracts it concludes with its customers on a lawful basis. Nor does it, or would it, agree with its customers to facilitate such use."

103. The letter later moves on, under a heading 'Relevant Background', to give the following account:

> "On 4 August 2020, NSO became aware of a possible use of the technology by a customer that was not in accordance with the contractual terms applicable to it, or which appeared to be beyond the purposes for which the technology was supplied... . As part of its review of this possible use, information was provided to NSO that raised the possibility that Baroness Shackleton's mobile phone, that of another unnamed member of her firm and that of her client (the Respondent Mother), may been compromised. At this stage, NSO did not know the full facts of whether phones belonging to other individuals may have been compromised. We cannot reveal confidential information or the methodology by which NSO seeks to verify that its technology is used strictly in accordance with the contractual terms on which it is licensed, for the purposes set out above. To do so would prejudice NSO's capacity to investigate future incidents."

104. The letter then gives an account of the investigation carried out by NSO before stating:

> "The activity of gathering information for the purposes of the Investigation itself concluded on or around 15 September 2020, although the post-investigative process which NSO follows in order to make a final determination has only recently concluded. While the Investigation could not make any determinative conclusions as to what in fact happened, the recommendation following the Investigation was that the contract with the customer should be terminated, and that the systems which that customer had contracts for be shut down."

105. The letter confirmed that the provision of services by NSO to the customer stopped completely as of 7 December 2020. In summary, the letter confirmed that, following its investigation, NSO had based its decision on the 'working assumptions' that 'the customer acted in breach of its contract with NSO' and that the phones of Baroness Shackleton, a member of her firm and the mother 'may have been compromised'. The following is then stated:

> "Following the investigation, NSO has not been able to establish any indication that the surveillance of the identifiers for (i) Baroness Shackleton and (ii) a member of her firm occurred prior to 7 July 2020. The investigation was also not able to

> establish when the surveillance of the identifier for (iii) the Respondent Mother began."

106. During the concluding section of the letter NSO confirmed that it was not able to reveal or confirm the identity of any of its customers. But it did confirm that 'our products are used exclusively by government intelligence and law enforcement agencies' and that therefore the father was not himself a customer.

107. That statement is consistent with a Declaration by Shalev Hulio, Chief Executive Officer of NSO Group, dated 16 April 2020, that has been filed in litigation in the USA. The court has seen a full copy of Mr Hulio's Declaration which includes the following statement:

> "NSO Group innovates cyber solutions that NSO Group does not itself use. NSO's only customers are sovereign states and the intelligence and law enforcement agencies of sovereign states…"

A subsequent Declaration by Mr Hulio, dated 13 May 2020, sets out further details of the steps to which NSO Group goes to ensure that its product is used exclusively by sovereign governments.

108. It is of note that the dates given for the assumed compromise of the three phones to which reference is made accords with the evidence of Dr Marczak.

109. The court has seen a copy of NSO's 'Human Rights Policy' dated September 2019. At a number of points the policy indicates the seriousness with which NSO will regard any serious misuse, or breach of contract by a customer. For example, paragraph xiii includes the following statement:

> "After either our own investigation or a state investigation, if we have sufficient grounds to believe that our products may have been misused we promptly take appropriate action. Ultimately where necessary, we may suspend or terminate use of the product or take other steps that may be warranted."

110. In the present case, as the NSO letter of December 2020 makes plain, after its investigation NSO has adopted the extreme remedy of terminating its customer's use of the Pegasus software. In commercial terms, this step is to be understood as having great significance. The court has been given general information, but it is plain that the contract price flowing from a customer to NSO for access to and use of the Pegasus software is measured in tens of millions of dollars. Further, termination of a customer's contract is likely, not only to affect the revenue flowing from the current licence term, but may well impact upon future revenue from that sovereign State in the years to come.

Mr X

111. Independent counsel, Mr Weetman, was provided with details of Mr X's identity, including various spellings of his name in English and Arabic. Armed with this information he was able to identify some 30 or more references to Mr X via internet

searches; the number is approximate as there is some potential duplication between English and Arabic articles.

112. Dating is by reference to a year only and a distinction is drawn between [Year] and 'Recent'. Mr Weetman was not invited to clarify this distinction. I have proceeded on the basis that 'Recent' indicates current activity in 2021, but [Year] indicates activity which is clearly limited to that year. I have not assumed that 'Recent' activity only commenced in 2021; the reference is taken simply as indicating that it is current.

113. The distinction between 'Recent' and any entry for [Year] or earlier is of importance. All of the 'Recent' entries relate to articles connecting Mr X with interest in the affairs of [another state], whereas the earlier references, including [Year], refer solely to interest in the UAE and do not refer to any other State (save for one [Year] reference to the justice system in [another state]). Finally, one 'recent' social media site is recorded as including recent comments by Mr X, or highlighting comments by him, regarding alleged human rights abuses in [another state], UAE, [four other states] [redacted].

114. The conclusion to be drawn from this material can only be that, insofar as he has publicly commented on matters, Mr X was, at least up until and during [Year], focussed on matters that were of concern to him in the UAE. More recently he has moved away from that focus and is now predominantly concerned with matters relating to [another state].

Dr Marczak: oral evidence

115. Dr Marczak gave oral evidence over a video link from California. The court sitting time was adapted as much as possible to accommodate the time difference, but the court is grateful to Dr Marczak for making himself available at an early stage on the two days over which his evidence was heard.

116. In response to the firm submission made by Lord Pannick that it was inappropriate for Dr Marczak to give any evidence in chief in the light of the very full and technically complicated statements that had been filed, Mr Charles Geekie QC's short opening questions for the mother were confined simply to matters of housekeeping. Ms Fottrell QC on behalf of the children's guardian had no cross-examination. Mr Geekie had no re-examination.

117. Dr Marczak gave oral evidence for over 6½ hours. This period was almost entirely taken up by cross-examination from Andrew Green QC on behalf of the father. It is right to record that Mr Green demonstrated cross-examination skills of the highest professional order. The structure of the cross-examination and the content of the questions were designed to test Dr Marczak's testimony across a wide canvas, including not only matters of technical detail but also possibilities of bias or fixed mindset against the UAE and Dubai. In addition Dr Marczak was questioned closely on the detailed communications that had been disclosed of discussions that he had had with the mother's security staff and others during the course of his investigation. The questioning was entirely justified and, given the unconventional route by which Dr Marczak had been introduced into the proceedings, the court benefitted greatly from having these matters tested in such detail by an advocate who plainly had total command of his brief and the skill with which to deploy that information in the best

interests of his client, the father. Save for one aspect that did not require further elaboration, I do not think that I intervened at any stage to restrain or direct Mr Green in the questions that he sought to put.

118. For his part, Dr Marczak also demonstrated, as might be understandable, a thorough grasp of the detail (both technical and factual) upon which his evidence was based. He gave clear answers to each of counsel's questions and in all other respects co-operated with the cross-examination process fully.

119. The following aspects of Dr Marczak's oral evidence are of particular note:

(a) He began monitoring Mr X's phone around January 2020. Mr X was one of a dozen or so other activists he was also monitoring. The UAE was not the only State of interest in the monitoring process. Other States including Bahrain, Saudi Arabia, Ethiopia, South Korea and Tibet.

(b) Dr Marczak has a working 'victims list' which is a list of leads towards investigation. The list identifies the IP addresses of supposed victims. The source of information leading to inclusion on the 'victims list' does not come from examination of sysdiagnoses or the identification of a server. It comes from elsewhere. Dr Marczak accepted that the identification of others who may be on the 'victims list' could be of relevance to these proceedings, but he was not prepared to disclose the list.

(c) There were IP addresses registered to Jordan on the 'victims list'. Dr Marczak accepted that this was not mentioned in his report. Dr Marczak confirmed that there were potential Jordanian targets on his 'victims list'. He was not able to recall the precise number, but thought it may be ten or twenty, but subject to quite a margin of error.

(d) Dr Marczak had had no communication with the mother or anyone acting for her before the 4th August when he made contact with Martyn Day at Leigh Day.

(e) Network logs for PHB were never examined and, on his understanding, were simply not available.

(f) Dr Marczak did not know anything about the history of the phones. He was simply given access to the sysdiagnose and the devices and told that these were the phones of named individuals.

(g) Dr Marczak accepted that the 'mobile container manager logs' went back many months on the phones. If the sysdiagnose files had been altered in any way deliberately, that would be hard to detect.

(h) Dr Marczak confirmed that the phones of the mother's Personal Assistant, and the two security officers did not contain

> direct evidence of those phones trying to communicate with the Pegasus proxy server. The analysis nevertheless indicated that these three phones had been infiltrated was based upon the identification of distinct app names and the distinctive pattern of the security failure that exhibited in the mobile container manager logs for each of the phones that was similar to those which did communicate with Pegasus proxy servers.
>
> (i) Dr Marczak referred to a distinctive pattern of entitlement failure which involved specific apps trying to access preferences, Siri and mail, but failing. For Dr Marczak the pattern of accessing only those apps, combined with the fact that the requesting app has an unusual name is 'quite distinctive'. Most of the apps seen on iPhones are installed, as they have to be, through the AppStore controlled by Apple. The names of these apps are totally different from the format of App Store app names. The unusual behaviour is a combination of the unusually named apps, trying to access the same three or four ordinary apps, and no other, and doing so immediately after they log into the phone. This behaviour was observed on all of the suspect phones.

120. Towards the end of the first day of oral evidence, and at the beginning of the second, Dr Marczak was questioned about his analysis of the network logs at the mother's Berkshire home. He had examined the network log at the mother's London home, but had found no material evidence and had not, therefore, referred to that log in his written statement. During the initial search of the Berkshire home network log Dr Marczak's invoice records that he 'reverse engineered…to extract dates and times at which four unidentified Pegasus victims called devices' at the home. It went on to state 'Goal is to ID these additional victims linked to the case'. Dr Marczak explained that these individuals could not be said to be 'identified'. At that stage he had simply identified an overlap between the proprietary information on his 'victim list' and communications noted on the mother's network logs to or from those named IP addresses. When first giving evidence about this he could not recall whether they had eventually been identified. He did not regard this as being a particularly important part of the process.

121. On further questioning Dr Marczak had not included this information in his written statements because the information was based on his 'list' and he did not wish to reveal the content of the list or its source. Because the provenance of IP addresses on the list may be variable, Dr Marczak did not 'feel comfortable' saying with any level of certainty 'look, there are these additional victims'. He accepted that, with hindsight, he might have referred to this in his statement.

122. In his evidence at the start of the second day Dr Marczak explained that he had a number of lists with Pegasus servers, or probable Pegasus servers, identified on them. There was a list drawn from Mr X. There was also a wider list of Pegasus servers and then there was a 'victims list' referring to the specific servers in this case. Only the 'victims list' has any detail about victims, the other lists show detail about IP addresses and domain names linked to Pegasus servers. When he had referred to Jordanian IP addresses at an earlier stage of his evidence, he had been referring to addresses on the 'victims list' associated with Pegasus servers linked to this particular case.

123. Dr Marczak confirmed that the home network log identified an IP address of a supposed Pegasus victim connecting with the mother's home network. As far as he could recall this data referred to one of the six phones on the list, but he could not be 100% sure.

124. Dr Marczak explained that the IP addresses that were seen on the home network log were not users of the home wifi system, they were IP addresses that were being communicated with, for one reason or another, from users inside the home. He therefore questioned the relevance of each of these links. He also questioned of how useful this information might be given that it might indicate a false positive or a false negative connected with the victims list. The firmer evidence, he suggested only came when one examined the phones and saw what was on the sysdiagnose. He therefore only referred to individual devices in his first witness statement if any earlier information was also confirmed by examination of the sysdiagnose.

Professor Beresford: oral evidence

125. Professor Beresford's written reports demonstrated a meticulous demeanour with a commendable obsession for detail which had enabled him to spot small typographical errors in various IP addresses, app and domain names (some of which are long and complicated) contained in Dr Marczak's various statements. This attention to detail was further demonstrated throughout his oral evidence. I formed the clear impression that he was an extremely careful witness who was keen not to say anything unless he had confidence in the accuracy of his answer.

126. Professor Beresford confirmed the contents of his reports by being taken to the specific headline points by Mr Geekie. In particular, with regards to the 'second fingerprint', he confirmed that he had had full access to it and had discussion with Dr Marczak about it. As a result he was satisfied that Dr Marczak had successfully identified the version 4 Pegasus servers.

127. Professor Beresford expressly confirmed Dr Marczak's analysis of the sysdiagnose from the six phones. He confirmed Dr Marczak's conclusion that the phones of the mother, Baroness Shackleton and Mr Manners showed infection by Pegasus as being 'a proper conclusion to come to'. And that a lesser degree of specificity applied to the other three.

128. Professor Beresford had the following exchange with Mr Geekie:

> "Q To be clear, there are four phones, Mr X, Baroness Shackleton, Her Royal Highness and Mr Manners, that you are satisfied are infected with Pegasus software and it is the same operator?
>
> A Yes, based on the material I have been provided with and the extra checks that I have performed, yes."
>
> "Q There was also - you were satisfied because you could see the data for this – 265 megabytes of data were taken from Her Royal Highness' phone and communicated to a Pegasus server?
>
> A Correct, that is what the logs I have been provided with show.

> Q As you have acknowledged today and have acknowledged in your written reports, there are some, I would suggest relatively small, areas where, for reasons explained by you and Dr Marczak, it has not been possible for you directly to verify the steps taken by Dr Marczak?
>
> A No, there are a number of areas where I am reliant on Dr Marczak. They include for example the provision of some of the data and that that data has been collected correctly, and there is an appropriate chain of custody around those data items, yes.
>
> Q So in relation to that set of material, just concentrating on that set of material, you are satisfied as to the methodology he has applied, you just have not been able to look at the primary data yourself and followed it through in the way that you have in many other areas?
>
> A Dr Marczak has often provided me with the primary data, so for example the data from …(examples given)… of course I am still reliant on him having collected that correctly similarly with the sysdiagnoses I am reliant on those having been collected from the correct handsets and provided. A few other areas for example in the case of the analysis of the version 9 servers, the origin input files, the pcap files are not available. Given the time that has passed it is not possible for me to collect them again, so I am reliant on Dr Marczak there. There are a number of areas where we are reliant on his data collection process.
>
> Q Yes, that is set out very clearly, both by you and Dr Marczak. Just to confirm, with that caveat in mind, so far as the methodology is concerned, you are content with the methodology he has applied?
>
> A I am content with the approach taken, yes."

129. In cross-examination Professor Beresford confirmed that he had never been asked to look at the Pegasus system before or otherwise been involved with it. He had not conducted a full worldwide internet scan to check Dr Marczak's evidence on this point. He said that it would now, probably, not be possible to do so.

130. Professor Beresford confirmed that in his first report he had not identified the unusually named apps relied upon by Dr Marczak as not being issued by Apple. He accepted that maybe he should have seen them and if he had they would have struck him as odd.

131. Professor Beresford confirmed that he had conducted his own independent research around the data associated with Dr Marczak's 'version 1' servers. In his second report he had set out the reasons why he considered there were links to NSO Group. He also confirmed the existence of the link working backwards from version 4 through versions 3 and 2 to version 1.

132. It was explained that evidence of the presence of Pegasus software on a phone did not, of itself, establish that the person connected with that phone was the primary target of any surveillance operation or a subsidiary means of getting to a different primary target connected with that person who may make contact with them and has communications with them and could be observed when they did so. Professor Beresford responded:

> "So, I guess there is evidence from multiple phones here. I guess if the centrepoint was somewhere else, then I guess the interesting question is: would you expect to see the same pattern of phones targeted in this case or not? So some other person let us call them 'Mr Z', so if Princess Haya was somehow related to Mr Z, would it also make sense for some of the other phones in this case that we have seen to also be targeted if the central focus was Mr Z or not?
>
> ...
>
> So, one of the problems with this sort of line of reasoning is that if you compromise the people associated with the victim you get a lot less data. You are only going to get information if Mr Z is talking with the phones that you have hacked. Whereas if you want, for example, the archive of photos off the device, you are not going to get that via another third party. There are significant advantages for attempting to hack the actual target rather than associates."

133. Following that explanation, Professor Beresford nevertheless accepted that he could not say that the mother in this case was the primary target from the information that he had seen.

Conclusions

(i) The Fact of Hacking by Pegasus software

134. Having now referred in detail to the evidence, it is possible to set out my conclusion on the first issue, namely whether the six mobile phones of the mother, her solicitors and her staff have been the subject of unlawful surveillance, or attempts to achieve such surveillance, in July and August 2020 and that the means of surveillance, or attempted surveillance, was via NSO Group's Pegasus software.

135. In approaching Dr Marczak's evidence I have exercised a great deal of care. He does not come into the case as an expert in the conventional sense. He stepped forward to offer assistance to the mother and her team which they readily took up. It was only after that that he became a potential witness. The assistance that he gave meant that he was in very close communication with the mother's staff and solicitors during his investigation. That route into the litigation does not render him automatically biased or irreversibly partisan, but it must be a matter for concern that that may be the case and it has therefore been a matter upon which I have maintained a keen eye throughout.

136. Further, Dr Marczak has an acknowledged interest in tracking the use of the Pegasus software by the UAE (including Dubai). He states that the episode in July 2020 that put

him on notice of this case, originated from his relationship with Mr X. He stated that he had reached the conclusion, before contacting Martyn Day, that Mr X's phone was being infiltrated by Pegasus and that, because of Mr X's interests as 'a UAE activist', this was likely to be via an operator in the UAE. To this extent, and it is an important factor, Dr Marczak does not stand above the fray. He is not a disinterested academic who simply monitors events from a distance, he is actively on the lookout for potential abuse of the Pegasus system. He is known as such to activists and, as evidence about Mr Mansoor and Mr X suggests, it is to him that activists turn if they are suspicious that they are being targeted. It is therefore entirely right that Lord Pannick advises the court to be on the guard for 'confirmation bias' in Dr Marczak's evidence.

137. Despite these important caveats and the justified need for caution, during the course of Dr Marczak's oral evidence I was progressively more and more impressed. His grasp of the detail of the Pegasus system and his own researches, previous encounters with it and published articles was to be expected, but it was, nevertheless, impressive and was maintained without significant falling off or error over the course of the two days. He was equally clear and firm in the detailed knowledge and recall that he had of his investigation for this case. He presented foremost as a scientist, who worked strictly within the confines of the data and the principles of computer science. His opinions, both micro and macro, were carefully built upon and supported by the data and the underlying engineering of the complex systems with which he works. I did not detect any occasion when he might be seeking to stretch the science to fit a pre-determined conclusion in relation to the fact of hacking and the identification of Pegasus software.

138. Despite being properly and thoroughly tested at every turn by the intelligent and probing questioning of Mr Green, Dr Marczak gave measured, clear and full answers to each question. Where there was a need to do so, he conceded matters or readily accepted corrections. As each stage of the cross-examination proceeded, I became more and more impressed with the witness.

139. Dr Marczak was, in short, an impressive witness who presented a detailed, logical account, supported by the core data that he had found, which led to the conclusion that there was strong evidence that the three principal phones had been hacked by Pegasus software and that it was probable that the other three phones, which exhibited some but not all of the suspicious features, had also been infiltrated. It is not necessary in this conclusion to go back through the detail that I have already set out, leading from Mr Mansoor to versions 1 to 4 and the second fingerprint. Despite very close analysis, there is no break in that chain which links the alien apps and the IP addresses found in the sysdiagnose and network logs in this case with the deployment of NSO Pegasus spyware.

140. The court has been most fortunate both to have located Professor Beresford and to find that he has been able to meet our extremely tight time-table. Whatever may be said about Dr Marczak's standing as an interested party and player in the relation to tracking down the use and abuse of Pegasus spyware, the same cannot be said of Professor Beresford, who has more than 25 years experience in the narrow field of computer security, but who comes to the Pegasus system having had no prior direct involvement with it. His independence from having any attraction to one outcome or another was clear, as was his expertise in this narrow and highly complex field. Professor Beresford adopted an approach to the case which demonstrated a meticulous attention to detail, and a need to have issues or assertions fully clarified before he was prepared to sign-

off on them and move on. That approach was amply demonstrated both in his written reports and in his oral evidence. I am fully satisfied that the court can place substantial weight on Professor Beresford's endorsement both of Dr Marczak's overall approach to this analysis and his detailed conclusions on the core data.

141. The evidence from Dr Marczak and Professor Beresford, which is supported to a degree by confirmation from IntaForensics, is based on detailed, logically developed, analysis which itself (in Dr Marczak's case) arises from research in this precise field going back over six or more years.

142. Dr Marczak has explained his process of analysis to the court in detail. He has been fully open with Professor Beresford in explaining what lies beneath it in computing terms and he has expressly disclosed details of his second fingerprint. After an apparently meticulous audit, and some research of his own, Professor Beresford has pronounced Dr Marczak's method and conclusions as 'sound' and he has found no reason to challenge them insofar as they establish hacking via the Pegasus software.

143. Separately, the court has the evidence from NSO, both in the form of the account given by Cherie Blair QC and in the NSO letter. It is clear from Mrs Blair's account that, from Day One, NSO had sufficient information that its software had been used against Baroness Shackleton and the mother to cause the senior management to take steps to make contact, during the night, to alert PHB that this was apparently the case. Thereafter NSO state, and I have no reason not to accept, that they undertook a full investigation, including visiting the customer State. Whilst the letter is written in careful terms, the 'assumption' that this hacking had indeed occurred was sufficient for NSO to terminate the customer's contract. That is a step which NSO documentation describes as only being taken 'ultimately where necessary'. It is a step with very significant commercial consequences for NSO and, I am entitled to assume, would only be taken if there was a clear basis for doing so.

144. There is a need for caution. The court cannot attach the weight to the NSO letter as would be open to it were the NSO investigator to have filed a full report with the court and been available to give oral evidence. To an extent, despite the letter, the court still looks at this side of the evidence through a glass darkly, hence my reference to the Delphic quality of the letter soon after its receipt. That said, it is a letter from a source which is extremely well placed to be able to say whether or not its software has been used, as it assumes has been the case. On its own, the letter might be sufficient to prove the first factual allegation. I do not have to determine that proposition as it is not on its own, it is but one part of the overall evidential picture on this issue.

145. Standing back, therefore, and looking at the overall picture, the evidence in favour of a finding of hacking comes from two distinct sources and travels in two separate directions. One source, the phones and network logs focus on evidence of the hacking event at the receiving end. The other source, namely that from NSO, involved an investigation of activity at the command and control, or sending, end. In their separate ways, using differing methods, both sources support a positive finding.

146. I see no reason to question the evidence and conclusions of Dr Marczak and Professor Beresford (supported by IntaForensics), on this first issue. That evidence alone establishes very clearly, and well beyond the tipping point of the balance of probabilities, that hacking by Pegasus of these 6 phones took place. That state of affairs

is fully supported by the evidence that has originated from NSO and goes further to strengthen the firmness of my conclusion on the first issue.

147. I therefore find that all six of these phones have either been successfully infiltrated, or at least the subject of an attempted infiltration, by surveillance software. I find that the software used was NSO's Pegasus software. In relation to the mother, it is clear that the attempt succeeded with a very substantial amount of data (265 MB) being covertly extracted from her phone. It is also probable, and I so find, that there was successful hacking of the phones of Baroness Shackleton and Mr Manners. The finding in relation to the other three phones is that there was an attempt to hack into them and that this was part of the same attack by Pegasus software as that affecting the principal three phones.

148. In setting out these findings I have used 'attempted' on a number of occasions. This arises because, unless there is evidence of data being transmitted from the phones, signs that alien software has been at work within them but, on a number of occasions, has 'failed' to connect with, for example, the 'mail' app, proves that there was a successful infiltration of the phone but does not prove that any data was actively extracted on those occasions. My understanding is that if the alien app is successful in accessing the phone's standard apps this event will not appear in the phone's memory manager log; thus only the failures are recorded. Thus, where I have used the word 'attempted' that is at least what has occurred, rather than the limit of the activity.

149. It is also necessary to explain that the sysdiagnose from the phones themselves do not apparently record whether any data has been extracted or not; the fact of connection with a proxy server is recorded, not the content of any transmission over that connection. Dr Marczak was able to say that on one occasion 265MB of data was extracted from the mother's phone because of records in the network log at her home, not from information on her phone itself. PHB did not have a network log at this time, hence it is simply not possible to know what and how much data, if any, was harvested from the phones of Baroness Shackleton or Mr Manners during this period.

150. Finally, in terms of clarifying matters, whilst the fact that 265MB can be stated as the amount of data taken from the mother's phone on one occasion, it is not possible to identify what this data was (save that it was a very substantial amount). The summary copied from Dr Marczak's report at paragraph 78 above describes just how wide the Pegasus software can reach in capturing an individual's personal data from a phone.

151. On the basis of those findings, and in further reliance upon the evidence of Dr Marczak, supported by Professor Beresford, I also find that one of the mother's security staff's phone had earlier been the subject of at least an attempt at hacking on five dates in November 2019.

(ii) Attribution: who originated the hacking?

152. Turning to the second and final set of findings, relating to attribution, the starting point is the firm and clear account from NSO that only a sovereign State, or the security services of a sovereign state, can purchase a licence to use the Pegasus software.

153. In the context of this case, as the Emirate of Dubai is not a sovereign State, Dubai could not, therefore, be the customer.

154. Moving on, standing back from the detail of the evidence and asking the question 'who would have an interest in hacking the phones not only of the mother and her staff, but also (and at the same time) the solicitors who are instructed to represent her in these proceedings?', the father and those acting for him in Dubai must fall for prominent consideration. No one has a closer interest in these proceedings than the two parents and the children. Whilst others, the Press, commentators, the general public may be aware of the case and may be interested in it, that interest is on an altogether different plane to that of the father and mother.

155. Although Dubai could itself not be the customer, the sovereign State of the UAE could be. The father is the Prime Minister of the UAE and Head of Government. The court is entitled to assume that the father and those acting for him must have the ability to instruct those in the security services of the UAE to take action on his behalf. The findings of fact previously made with respect to Princess Latifa establish that the father is prepared and able to use the government security services for his own family needs, and that this has occurred in the recent past. When one adds the father's natural and proven interest in these proceedings, which far outweighs anyone's save for the mother and the children, to the need for the perpetrator of the hacking to have access to the levers of control in a sovereign State sufficient to order its security services to act on his behalf, the prospect that it is the father comes yet more clearly into focus.

156. Lord Pannick, at preliminary hearings, has raised the prospect that the court may be in the position of contemplating a number of potential originators of the hacking. The court has been reminded that an individual may only be considered as a potential perpetrator if there is a 'real possibility' that this is the case. The father's case is, however, that if there is a pool of perpetrators then the evidence is insufficient for him to be in that pool. In other words that there is no 'real possibility' that he is the originator. It is a submission that has been repeated on more than one occasion. It is one that I find is impossible to accept. In the circumstances of this case, it is beyond contemplation that the court, or indeed any rational person acquainted with the facts, could say that there is no 'real possibility' that the father originated the hacking of his former wife, her staff and her lawyers. No conclusion other than that there must be a real possibility that it is him is tenable.

157. Establishing a 'real possibility' is not, however, the relevant test of proof. It does not establish a pseudo-burden of proof on the father to point to someone else. The right question, as Peter Jackson LJ identified, is 'does the evidence establish that the individual probably' acted as it is alleged that he did.

158. I do not place any reliance upon evidence from Dr Marczak on the issue of attribution. On that issue, however, it is necessary to evaluate the degree of weight, if any, that can be attached to what is said about Mr X.

159. For the reasons that I have already given, I accept Dr Marczak's evidence that the indications of hacking activity on Mr X's phone in July 2020 are of a piece with that found on the phones in this case. I also accept his evidence that NSO issues each of its customers with access to separate, bespoke, proxy servers. I am satisfied that the proxy servers with which Mr X's phone was communicating were replicated on the phones in England. I am therefore satisfied, on the balance of probability, that Mr X, the mother, her staff and her solicitors were all subject to infiltration from the same State government's operation of Pegasus software.

160. The independent counsel's internet searches regarding Mr X have limited probative value. The court does not itself know anything of Mr X and must be cautious. With those caveats in mind, the independent counsel's researches do indicate that, until recently, and certainly during [redacted], Mr X continued to demonstrate an established critical interest in human rights and other activities within the UAE and that he was not, at that stage, publicly interested in the activities of other States. The hacking took place in July or August 2020.

161. To a degree it is possible to make a case, and Mr Geekie seeks to do so, that late July 2020 was a particularly busy and financially interesting time in these proceedings, with the build up to key hearings relating to the mother's long-term financial claims for herself and the children. I am not, however, able to put any weight on this factor. Dr Marczak's evidence demonstrated that the Pegasus software is to a degree opportunistic in the sense that it will become very active, and will capitalise upon, the haphazard opening up of gaps in the security software protecting phones which lead to 'exploits' arising which, as that label suggests, are then exploited. It is also clear from Dr Marczak that he had observed a good deal of Pegasus activity in this very period and was trying to check out a range of potential 'victims'. That is how he found PHB and became connected with this case. I do not therefore consider that the date of the hacking arises from the fact that there was something of interest in July to gain information about in this case; rather the opening up of an exploitive window gave the operators the chance to do so, which they plainly took.

162. Whilst the father does not have to prove anything, it is the case that he has chosen not to attempt to do so. The court does not therefore have any evidence to put in the balance against a finding that the originator was the UAE on his authority. That state of affairs does not, I repeat, prove the case; it is simply an acknowledgement that there is no evidence to the contrary.

163. What the father has done is to float various suggestions before the court to the effect that another sovereign State is, or may be, the originator of the hacking. These have changed from hearing to hearing. At various times the states of Iran, Israel and Saudi Arabia have been suggested. In the main hearing itself, the suggestion being pushed was that it may be the State of Jordan. In the past Lord Pannick has proffered the idea that it would be in the interests of another State to undertake the hacking in order for the mother and for the court to jump to the conclusion that the father was the culprit. The purpose, it was suggested, of this subterfuge being to embarrass the father and thereby somehow further the interests of the originating State. Nothing was said as to the mechanism by which the mother or the court might find out that this highly sophisticated software had been used against her, or why another State might risk losing its very valuable contract with NSO, in order just to embarrass the father in this way even if NSO ever discovered that hacking had occurred. These various propositions were not pursued at the final hearing.

164. The suggestion now, very lightly laid out in cross examination and submissions, is that the State of Jordan may be responsible. The fact that Dr Marczak's 'victims list' may contain 20 or so Jordanian IP addresses and the possibilities that it may be that some unidentified individuals may have communicated with the mother's home using hacked phones and that they may be Jordanian, are referred to. The current apparent political and familial unrest in the ruling class in Jordan is also referred to.

165. These shifting suggestions, none of which is backed up by any evidence, are so insubstantial as to be without consequence in the evaluation of the question of attribution. If the standard of proof were 'beyond reasonable doubt', they might have some traction, but to my mind, where the standard of proof is the balance of probabilities, they have none.

166. One small piece of evidence, which is unchallenged, is Mrs Blair's account in her statement for the court of her conversation with the NSO senior manager:

> "However, during a conversation with the NSO Senior Manager, I recall asking whether their client was the 'big state' or the 'little state'. The NSO Senior Manager clarified that it was the 'little state' which I took to be the state of Dubai."

This evidence, like others, should not carry more weight than is reasonable, but it is a considered account in a witness statement from a source upon which the court is entitled to rely for care and accuracy on a point such as this. It proves, as I find, that the NSO manager did speak in this way and refer to the 'little state' as opposed to the 'big state'. That conversation is compatible, and I place no greater reliance upon it, with the two 'States' being Dubai within the bigger State of the UAE.

167. Drawing these matters together, of those to which I have referred, I regard two elements of the overall evidential canvas to be of particular weight.

168. Firstly, it is obvious that the father, above any other person in the world, is the probable originator of the hacking. No other potential perpetrator, being a person or government that may have access to Pegasus software, can come close to the father in terms of probability and none has been put forward other than via transient and changing hints or suggestions.

169. Secondly, as the previous findings of fact establish, the father, who is the Head of Government of the UAE, is prepared to use the arm of the State to achieve what he regards as right. He has harassed and intimidated the mother both before her departure to England and since. He is prepared to countenance those acting on his behalf doing so unlawfully within the UK.

170. The evidence concerning Mr X and from Mrs Blair is entirely compatible with, and is not contrary to, a conclusion that the source of the hacking was the UAE.

171. The previous findings of fact and the evidence adduced at this hearing, as I have described it, taken together are more than sufficient to establish that it is more probable than not that the surveillance of the six phones that I have found was undertaken by Pegasus software was carried out by servants or agents of the father, the Emirate of Dubai or the UAE and that the surveillance occurred with the express or implied authority of the father.

The children's welfare

172. Having stated my conclusions on these factual matters, the focus of the court will, at last, turn fully to the welfare of the two children. In this context, I note that in a Position Statement dated 2 October 2020 the father stated that 'it is hard to see how the hacking allegations make a substantial difference' to the issue of the father's contact with the

children. The court will return to this aspect in detail at the welfare hearing, but to assist the father at this stage I wish to make it plain that I regard the findings that I have now made to be of the utmost seriousness in the context of the children's welfare. They may well have a profound impact upon the ability of the mother and of the court to trust him with any but the most minimal and secure arrangements for contact with his children in the future.

173. It does not take long to contemplate just how an individual would react to discovering that their personal phone, and those upon whom they rely for confidential advice, support and protection, have been infiltrated by the most sophisticated spyware that is available, and to know that a very substantial amount of personal data has been stolen, yet not knowing precisely what. It is often said that the most important thing that a house-burglar steals is the peace of mind of the householder. The same must surely be true of phone hacking.

174. The court has, on many occasions, stressed to the father since the start of these proceedings that the most important goal should be to build up 'trust', so that the mother and the court, and indeed the children, can trust him – in particular trust him not to take unilateral action to remove the children from their mother's care. The findings made in this judgment prove that he has behaved in a manner which will do the opposite of building trust. The findings represent a total abuse of trust, and indeed an abuse of power, to a significant extent. It is an abuse which has been compounded by the manner in which the father has contested these allegations and instructed his lawyers. Despite the weight of evidence, the fact of hacking was never conceded, nor was the fact that such hacking had been by Pegasus. At no stage has the father offered any sign of concern for the mother, who is caring for their children, on the basis that her phones have been hacked and her security infiltrated. Instead he has marshalled a formidable forensic team to challenge the findings sought by the mother and to fight the case against her on every point. It is of course the right of a litigant to contest proceedings as they see fit, but to do so may not be without consequences for the relationships of trust and mutual understanding that the court has been keen at all stages to see developing.