Neutral Citation Number: [2022] EWHC 2199 (QB)

Case No: QB-2019-003909

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
MEDIA AND COMMUNICATIONS LIST

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 19/08/2022

Before :

MR JUSTICE JULIAN KNOWLES

- -

Between :

GHANEM AL-MASARIR	**Claimant**
- and -	
KINGDOM OF SAUDI ARABIA	**Defendant**

- -
- -

Richard Hermer QC, Ben Silverstone and Professor Philippa Webb (instructed by **Leigh Day**) for the **Claimant**
Antony White QC and Michelle Butler (instructed by **RPC**) for the **Defendant**

Hearing dates: **15-16 June 2021**

- -

Judgment Approved by the court for handing down (subject to editorial corrections)

If this Judgment has been emailed to you it is to be treated as 'read-only'.
You should send any suggested amendments as a separate Word document.

Mr Justice Julian Knowles:

Introduction

1. Suppose, to take a not entirely theoretical example, a foreign state (not, I emphasise, the Defendant) sends two agents to the UK to kill a dissident opponent by poisoning him. The operation is planned abroad. The radioactive poison is made abroad. The operatives bring the poison into the UK from abroad. They meet with the dissident in a London hotel, poison his tea, and he dies. The foreign state's responsibility is clearly established by the evidence. Can the dissident's representatives sue the foreign state in the High Court for damages for his wrongful death ? Or is the responsible foreign state immune from civil proceedings by virtue of the State Immunity Act 1978 (SIA 1978) ?

2. To take another example, suppose agents of a different foreign state kidnap a dissident off the streets of London, hold him captive there, and torture him. Is the foreign state liable to a claim for damages for personal injury by the victim, or is it immune under the SIA 1978 ?

3. These scenarios involve some of the issues raised by this case. There are others.

4. In the case before me the Claimant, a critic of the Kingdom of Saudi Arabia (KSA/the Defendant), sues it for damages for personal injury. He obtained permission to serve the claim form outside the jurisdiction from the Master on an *ex parte* basis. The KSA now applies, in effect, for a declaration that it is immune under the SIA 1978, and to set aside the order for service out on that basis.

5. I will need to consider the SIA 1978 in detail later, but for now it is sufficient to explain that s 1(1) provides for a general immunity from jurisdiction. It states:

> "A State is immune from the jurisdiction of the courts of the UK except as provided in the following provisions of this Part of this Act".

6. The effect of this provision is that in order for a state to be subject to the jurisdiction of the courts of the UK, the proceedings must be of a kind specified in the exceptions to immunity listed at ss 2 to 11 of the SIA 1978. If none of those exceptions apply then the court lacks jurisdiction: *Jones v Ministry of the Interior of the Kingdom of Saudi Arabia* [2007] 1 AC 270, [9]; *Benkharbouche v Embassy of the Republic of Sudan* [2019] AC 777, [39].

7. The exception relied upon by the Claimant in this case is s 5, which provides:

> "5. Personal injuries and damage to property.
>
> A State is not immune as respects proceedings in respect of –
>
> (a) death or personal injury; or
>
> (b) damage to or loss of tangible property,
>
> caused by an act or omission in the United Kingdom."

8. It is common ground that the burden of proving that the claim falls within s 5 as one of the exceptions to the general immunity provided by s 1 lies on the Claimant and not the Defendant. It will not suffice for the Claimant to show a 'good arguable case' that the claim falls within one of the exceptions. The question of whether the case falls within one of the exceptions is to be determined on the balance of probabilities as a preliminary issue: *JH Rayner (Mincing Lane) Ltd v Department of Trade and Industry* [1989] Ch 72, 193-194 (Kerr LJ) and 252 (Ralph Gibson LJ), applied in *London Steam Ship Owners' Mutual Insurance Associated Limited v Kingdom of Spain* [2020] 1 WLR 4943, 4956 at [30] per Henshaw J.

9. At the heart of this case is the alleged infection of the Claimant's iPhones with surveillance software – or spyware – by persons acting on behalf of the Defendant. Dr Bill Marczak, the expert on whom the Claimant relies, has made three witness statements (Marczak 1, Marczak 2 and Marczak 3), dated 10 December 2019, 24 March 2021 and 14 June 2021 respectively. In Marczak 1 at [4] he says that spyware is:

> "… any software or hardware component that is installed on a target's electronic device, without their consent, to facilitate third-party access to data stored on the device, or to the device's functions (eg, turning on the device's microphone to record audio in the device's vicinity)."

10. This case involves a considerable quantity of technical material relating to computers and the internet. The legal issues are not straightforward either. The papers run to well over 3000 pages, and I was taken to a large body of international and comparative law, as well as much domestic authority. The Skeleton Arguments are very lengthy. All of this has taken some time to analyse. I am grateful to both legal teams for their assistance on a complex matter.

The issues

11. The parties are agreed that this case raises the following issues. The overarching issue is whether the Claimant has established, to the requisite evidential standard, that the s 5 exception is applicable to his claim. In particular:

    a. Does the claim relate to alleged acts which are inherently sovereign or governmental in nature, and thus fall outside the scope of s 5 of the SIA 1978, or does s 5 encompass such acts?

    b. Does the claim fail to meet the requirements of s 5 because the alleged personal injury resulting from the spyware claims was not caused entirely by acts or omissions in the UK?

    c. Does the claim fail to meet the requirements of s 5 because there is insufficient evidence of the Defendant's responsibility for the persons responsible for the alleged spyware?

    d. Does the claim fail to meet the requirements of s 5 because there is insufficient evidence of the Defendant's responsibility for the persons responsible for the assault on the Claimant?

e. Does the evidence relied upon by the Claimant provide no coherent or realistic basis on which to advance the Claimant's pleaded case such that the Court should take steps to halt the proceedings in any event ?

The claim in summary

12. The Claimant's Particulars of Claim (POC) and Skeleton Argument summarise his claim in the following terms. As is normal in this kind of case, the Defendant has not filed a Defence. The following is obviously not agreed.

13. The Claimant is a satirist and human rights activist. He has resided in England since 2003 and has been prominently involved in campaigning for political reform and human rights in Saudi Arabia. He was granted asylum in October 2018 following an appeal to the First-tier Tribunal (Immigration and Asylum Chamber).

14. He claims that malicious text messages were sent to two of his iPhones by or on behalf of the Defendant and that, after he clicked on links contained within those messages, spyware known as 'Pegasus' was installed on his devices. This software was developed and is marketed by an Israeli company called NSO Group (NSO).

15. The operation of the Pegasus spyware resulted in the covert and unauthorised accessing by the Defendant of the Claimant's information stored on, or communicated or accessible via, his iPhones. As set out in NSO's 'Pegasus – Product Description' document, among Pegasus' functions are: the extraction and ongoing collection of all data stored on or by an infected device; location tracking of the device; interception and recording of voice calls on the device; real-time interception and recording of sounds in the vicinity of the device (by covert activation of the in-built microphone); and real-time interception and recording of images in the vicinity of the device (by covert activation of the in-built camera).

16. In addition, on 31 August 2018, the Claimant was followed and attacked in Knightsbridge, London. He claims this assault was instigated, directed, authorised and/or ratified by the Defendant and/or its employees, officials and/or agents acting on its behalf.

17. The Claimant and his iPhones were located in England at all material times during which the alleged wrongs and personal injury occurred.

18. The claim is brought in misuse of private information; harassment; trespass to goods; and assault.

19. In overview, the claim in misuse of private information is based on the covert and unauthorised collection, accessing, retention, disclosure, transfer and use of the Claimant's private information stored on or communicated or accessible via the iPhones. The harassment claim is founded on a course of conduct which included each or all of the following: the sending of the malicious text messages; the infection of the iPhones with Pegasus; the surveillance of the Claimant; and the attack on the Claimant in Knightsbridge (which latter event also forms the basis of the assault claim). The claim in trespass to goods is premised on the direct and unauthorised interference with

the Claimant's iPhones, which altered their functioning, configuration and hardware in numerous ways.

20. The claim is for damages for personal injury (and loss consequential on that injury) in the form of psychiatric injury suffered by the Claimant as a result of learning that: (a) the text messages were malicious messages sent by or on behalf of the Defendant; (b) learning that he had been subject to surveillance; and (c) the attack in Knightsbridge; and the physical damage suffered as a result of the Knightsbridge attack.

21. The Claimant alleges that the Defendant is not immune in respect of the claim because the exception to sovereign immunity under s 5 of the SIA 1978 is applicable, in that these proceedings are in respect of personal injury and damage to or loss of tangible property caused by acts or omissions in the UK, which acts are pleaded at [71] of the POC. The Claimant does not know whether any other acts of relevance to the claim took place outside the jurisdiction.

The parties' submissions

General background

22. As I have indicated, the Claimant accepts that s 1 of the SIA 1978 confers a general immunity on foreign states from the jurisdiction of the UK's courts except as provided in the relevant exceptions in Part I of the Act.

23. The s 5 exception to state immunity applies to claims for personal injury, including psychiatric injury. It is not limited to cases in which personal injury is a 'direct consequence' of the conduct complained of: *Federal Republic of Nigeria v Ogbonna* [2012] 1 WLR 139, [6(5)] and [13], *per* Underhill J (as he then was).

24. As a matter of domestic law, Part I of the SIA 'is a complete code': *Benkharbouche*, [39]. It is to be construed against the background of customary international law: *Alcom Ltd v Republic of Colombia* [1984] AC 580, p597G.

25. However, while it is highly unlikely that Parliament intended to require courts to act contrary to international law unless the clear language of the SIA 1978 were to compel that conclusion, the statute 'does not do more than this' since it purports to deal comprehensively with the jurisdiction of the UK courts both to adjudicate upon claims against foreign States and to enforce by legal process judgments pronounced and orders made in the exercise of that adjudicative jurisdiction: *Alcom*, p600B.

26. International law recognises a distinction between acts done by a state in the exercise of sovereign or governmental authority (ie, acts done *jure imperii*), and acts done by it of a private law nature (acts done *jure gestionis*), typically (but not exclusively) commercial activities: *Benkharbouche*, [8]. That distinction is important to the first issue I have to resolve.

The Claimant's case

Issue (a): Section 5 applies to both sovereign/governmental acts and acts of a private law nature (ie, non-sovereign acts)

27. The Claimant submits that the text of s 5 draws no apparent distinction between sovereign and private acts. On its plain terms, s 5 applies to both categories of act. The text simply refers to injury or damage 'caused by an act or omission in the United Kingdom'. That meaning should be applied without the interpolation advanced by the Defendant, in accordance with the presumption that the grammatical meaning of an enactment is the meaning that was intended by the legislator.

28. The approach adopted in s 5 is in contrast to other parts of the SIA 1978, in which the scope of immunity *is* defined by reference to notions of sovereign acts: see s 3(3)(c) ('any other transaction or activity (whether of a commercial, industrial, financial, professional or other similar character) into which a State enters or in which it engages otherwise than in the exercise of sovereign authority') and s 14(2) ('A separate entity is immune from the jurisdiction of the courts of the United Kingdom if, and only if— (a) the proceedings relate to anything done by it in the exercise of sovereign authority…').

29. In s 5, Parliament chose not to condition immunity by reference to such language, and so reading it in to the section, as the Defendants would have me do, would exceed the proper bounds of statutory construction. In other words, the Defendant's limitation on s 5 to purely private acts would overturn the plain meaning of s 5.

Issue (b): The requirement in s 5 that the injury or damage be 'caused by an act or omission in the United Kingdom' does not require all of the alleged acts to have occurred in the United Kingdom. It is sufficient if a causative act or omission occurs here, even if other causative acts occur abroad.

30. The s 5 exception applies when the death, injury or damage is 'caused by an act or omission in the United Kingdom'. In accordance with the plain meaning of this phrase, it is only necessary for a single relevant act or omission causative of the death, injury or damage to take place within the UK in order to engage the exception. Contrary to the Defendant's submissions, there is no proper basis on which the Court, under the guise of statutory construction, could replace the words 'caused by an act or omission in the United Kingdom' with the phrase 'where the entire tort took place in the United Kingdom'. Nor can s 5 be interpreted so as to require *all* of the acts and omissions causative of the death, injury or damages, and in respect of which the proceedings are brought, to have taken place in the UK. If that was what Parliament had intended, it would not have used the words that appear in s 5.

31. Adopting the plain and literal approach to s.5, it is apparent in respect of the hacking claim (as well as the assault claim) that numerous acts and omissions causative of personal injury and damage to or loss of tangible property, and in respect of which the proceedings are brought, occurred in the UK. These include the various acts by which information was transmitted to and from the Claimant's devices within the UK so as to cause psychiatric injury to him and damage to his iPhones, involving the receipt of the harassing text messages, the unauthorised interference with his devices and the exfiltration of his private information. These were discrete self-contained acts occurring within the UK which were causative of personal injury and damage to property and fell within s 5.

Issue (c): The sufficiency of evidence as to the Defendant's vicarious liability for the persons responsible for the alleged spyware attack

32. The Claimant accepts, for present purposes, that the test to be applied to this aspect of the Defendant's application, at this *inter partes* stage, is whether, on the balance of probabilities, the claim falls within the exception in s 5, in accordance with the approach adopted by the Court of Appeal in *Al-Adsani v Government of Kuwait (No 2)* (1996) 107 ILR 536.

33. The Claimant submits that the evidence of his expert, Dr Bill Marczak, a computer scientist and expert in spyware, more than satisfies this test. The Defendant has filed no evidence in response, although it has made forensic observations about Dr Marczak's evidence.

Issue (d): The sufficiency of evidence as to the Defendant's vicarious liability for the persons responsible for the alleged assault

34. The Claimant submits that I can be satisfied on a balance of probabilities that the Defendant was responsible for the physical attack on him by several men in Knightsbridge in August 2018. Contrary to the Defendant's case, he says his case goes beyond mere assertion. He relies on a combination of circumstances, namely: (a) Saudi Arabia's record in targeting dissidents with violence (including, most notoriously, the murdered journalist Jamal Khashoggi); (b) that one of the men can be seen on a video of the incident wearing an earpiece; (c) the attack took place after the Claimant's phone had been infected by spyware, but before he knew that it had; (d) what was said by the attackers had a political component; (e) it is unlikely that the attack was a random one.

35. He also points out that although the Defendant's solicitor has indicated that the Defendant, via its London Embassy, knows who the attackers are, they have not made witness statements, although they could have done. He also says there are inconsistencies in the Defendant's accounts, as set out by the Defendant's solicitor on a hearsay basis.

Issue (e): Whether the Claimant's evidence provides a coherent or realistic basis on which to advance his pleaded case

36. This aspect of the Defendant's application is based on the following passage from *Propend Finance Pty Ltd v Sing* (1997) 111 ILR 611, 662:

> "Independent of any steps which may have been taken by a party to litigation, this Court has an interest in ensuring that its process is not used for purposes which are not explicable or do not make sense. If it is obvious that proceedings are misconceived, or are being conducted on an unrealistic hypothesis, this Court may, in its inherent jurisdiction, take steps to halt their misuse. During the course of the hearing before us, in the context of the issue of state immunity that was argued before us, we sought to understand the basis on which it could be suggested that the Commissioner had some vicarious responsibility for a contempt which was committed, at most, by one of his officers acting in breach of an order directed to that officer personally. We became increasingly concerned that there was and is no coherent or comprehensible basis for such a suggestion.

37. The Claimant says that the first four issues should be resolved in his favour, and hence it follows the fifth issue should also be resolved in his favour. There is no question of this case being a misuse of the process.

38. Thus, the Claimant invites me to dismiss the Defendant's application.

The Defendant's case

39. On behalf of the Defendant, Mr White QC submitted as follows.

Issue (a): The claim relates to alleged acts which are inherently sovereign or governmental in nature and so fall outwith s 5, which is limited to acts of a private law character

40. Mr White's core submission on behalf of the Defendant is that the claim relates to alleged acts which are inherently sovereign or governmental in nature, namely allegations of spying and an attack by a state on a political opponent. Such acts, like torture or state-sponsored terrorism, are not of a private law character, or otherwise incidental to a State's sovereign status, but rather are integral to it, and so cannot properly be regarded as falling within the limits of s 5.

41. In other words, the Defendant invites me to read the words 'act or omission' in s 5 as excluding acts or omissions which are of an inherently sovereign or governmental nature, ie, acts done *jure imperii*. It submits that s 5 only covers acts done *jure gestionis*. Recognition in English law of the centrality of the customary international law distinction between acts of a private law character and acts of a sovereign character when applying state immunity from civil claims is well established: see for example the views of Lord Wilberforce in *Playa Larga v I Congreso del Partido* [1983] 1 AC 244 at pp.265-7, and Lord Millett in *Holland v Lampen Wolfe* [2000] 1 WLR 1573, 1583-4. As an exception to general immunity, s 5 should be narrowly interpreted so as to apply only to acts of a private nature occurring in the UK which cause death, personal injury or injury to property.

42. In the event I were to conclude that s 5 is ambiguous, Mr White invited me, in accordance with *Pepper v Hart* [1993] AC 593, to consider various *Hansard* materials in relation to the passage of the Bill which became the SIA 1978 which he said supported his position.

43. Further and in any event, Mr White submitted that the issue had been determined in his favour in terms which were binding upon me in *Propend*, p652, per Laws J, in a passage which was subsequently upheld by the Court of Appeal (Leggatt, Pill and Mance LJJ) at pp664-665.

Issue (b): The alleged personal injury resulting from the spyware claims was not caused by an act or omission in the UK within the meaning of s 5 SIA 1978

44. Mr White submitted that s 5 requires the whole tort to take place within the UK and that, subject to *de minimis* exceptions, where a tort takes place partly inside and partly outside the UK, then it falls outside the exception in s 5 and the foreign state is entitled to immunity: Dickinson, Lindsay and Loonam, *State Immunity: Selected Materials and Commentary* (OUP, 2004) pp369-370. Section 5 therefore has stricter jurisdictional requirements for States as defendants than an ordinary defendant pursuant to CPR r

6.36 and 6.37: see Fox and Webb, *The Law of State Immunity* (3rd rev Edn, 2015), p203, fn 185.

45. It is inapposite to rely, as the Claimant does, on cases on the tort jurisdictional gateway in CPR PD 6B, 3.1(9)(b), despite the similarity in language between it and s 5 ('damage which has been or will be sustained results from an act committed, or likely to be committed, within the jurisdiction …'). The CPR rule was drafted in a different context.

46. Mr White placed particular emphasis on the decision of the US Court of Appeals for the District of Columbia in *Kidane v Ethiopia* 851 F 3d 7 (2017), which was also a claim arising out of a spyware attack on a dissident, who was located in the United States. The Court found it lacked jurisdiction because the Foreign State Immunities Act (FSIA) (28 USC 1605(a)(5)) granted Ethiopia immunity from the claim as the non-commercial tort exception was inapplicable because the entire tort did not occur in the United States.

Issue (c): The persons responsible for the alleged spyware in relation to the Claimant's devices were not persons for whom the Defendant is vicariously responsible

47. For the reasons set out in the first witness statement of Davina Given (Given 1) (the Defendant's solicitor), the Defendant submits that the Claimant's case as to the alleged infiltrations of his iPhones being carried out by the Defendant and/or its employees, officials and/or agents acting on its behalf is entirely circumstantial. The Claimant has not established that the Pegasus operator (ie, a group of remote servers controlling the infected phone) designated by Citizen Lab as 'Kingdom' is under the control of a person or persons for whom the Defendant is responsible.

Issue (d): The persons responsible for the alleged assault on the Claimant were not persons for whom the defendant is vicariously responsible

48. In relation to his assault claim, the Claimant has no evidence beyond his mere assertion to that effect that the assault was committed by the Defendant's employees, officials and/or agents acting on its behalf. The individuals involved were just patriotic students who just happened to overhear things said by the Claimant to a friend which offended them. Ms Given has made two statements on instructions given to her by the Embassy to this effect.

Issue (e): The evidence relied on by the Claimant does not provide a coherent or realistic basis on which to advance the Claimant's pleaded case

49. Finally, the Claimant's case is of such a weak and/or speculative nature that this is a case in which it would be appropriate for the Court to exercise its inherent jurisdiction in ensuring that its process is not used for purposes which are not explicable or do not make sense. The claim is misconceived, unviable and/or is being conducted on an unrealistic hypothesis and the Court should take steps to halt the misuse of the proceedings.

Discussion

50. I have re-formulated some of the issues in light of the arguments as advanced, in order (hopefully) to elucidate the real issues which I have to determine.

(a) Did the act of installing Pegasus on the Claimant's iPhones and the assault fall outside the scope of s 5 as acts done in the exercise of the Defendant's sovereign authority, or does s 5 extend to any act of whatever type done by a foreign state in the UK which causes personal injury?

51. At one time foreign states enjoyed absolute immunity from suit in the courts of the UK. The classic statement was that of Lord Atkin in *Cia Naviera Vascongada v Steamship Cristina; (The Cristina)* [1938] AC 485, 490:

> "The courts of a country will not implead a foreign sovereign, that is, they will not by their process make him against his will a party to legal proceedings whether the proceedings involve process against his person or seek to recover from him specific property or damages."

52. Over time, as a matter of customary international law, and as sovereign States increasingly engaged in commercial enterprises, immunity became more restricted. It continued to attach to acts undertaken by a state *jure imperii*, ie, in the exercise of sovereign authority, but not to those arising out of activities which it undertook *jure gestionis*, ie, transactions of a kind which might appropriately be undertaken by private individuals instead of sovereign states, in particular those which were done in the course of commercial or trading activities. This became known as the restrictive theory of immunity.

53. Although, as Lord Diplock said in *Alcom*, p598, the law of nations had long been accepted to be part of the common law, English courts during the 20th century were slow to recognise and give effect to the changes that had by then been taking place in public international law over the last 50 years, whereby, among the great majority of trading nations, the restrictive theory of sovereign immunity had replaced the absolute theory.

54. That recognition first occurred in a judgment of the Privy Council in *The Philippine Admiral* [1977] AC 373 delivered in November 1975; though this in its terms was limited to actions *in rem*. It was the judgment of Lord Denning MR in *Trendtex Trading Corporation v Central Bank of Nigeria* [1977] QB 529 that marked the definitive absorption by the common law of the restrictive theory of sovereign immunity. Lord Denning's statement in *Trendtex* as to what had become the revised common law rule as to the immunity of foreign sovereign states from the jurisdiction of the English courts, before the passing of the SIA 1978, received the approval of the House of Lords in *I Congreso del Partido* [1983] AC 244.

55. Those who wish to read more about the development of the restrictive theory of immunity are referred to Lord Sumption's judgment in *Benkharbouche,* [40] *et seq*.

56. The long title of the SIA 1978 states that it is:

> "An Act to make new provision with respect to proceedings in the United Kingdom by or against other States; to provide for the effect

> of judgments given against the United Kingdom in the courts of States parties to the European Convention on State Immunity; to make new provision with respect to the immunities and privileges of heads of State; and for connected purposes."

57. In *Al-Adsani v Government of Kuwait (No 2)* (1996) 107 ILR 536, p542, Stuart-Smith LJ said that the Act 'is a comprehensive code and is not subject to overriding considerations.' In *Benkharbouche*, [39], Lord Sumption said:

> "No one doubts that as a matter of domestic law, Part I of the State Immunity Act 1978 is a complete code. If the case does not fall within one of the exceptions to section 1, the state is immune."

58. In *London Steam-Ship Owners' Mutual Insurance Association Ltd v Spain*; *The Prestige (Nos 3 and 4)* [2021] EWCA Civ 1589, [39]-[40], the Court of Appeal (Males, Popplewell and Phillips LLJ) said, summarising earlier high authority:

> "39. We start with some observations on the relationship between the 1978 Act and public international law. The provisions of the Act fall to be construed against the background of the principles of customary international law, which at the time it was enacted, as now, drew a distinction between claims arising out of those activities which a state undertakes *jure imperii*, i.e. in the exercise of sovereign authority, and those arising out of activities which it undertakes *jure gestionis*, i.e. transactions of a kind which might appropriately be undertaken by private individuals instead of sovereign states, in particular what is done in the course of commercial or trading activities. The former enjoyed immunity; the latter did not. This came to be known as the restrictive theory of immunity, which had by then been adopted by the common law in this country. See *Alcom Ltd. v Republic of Colombia* [1984] AC 580 at pp. 597-599, *Playa Larga and Marble Island (Owners of Cargo Lately Laden on Board) v I Congreso del Partido* [1983] 1 AC 244 at pp. 261-262, and *Benkharbouche* at [8]. The Act did not, however, merely seek to frame immunity in terms of this binary distinction, choosing instead to formulate the exceptions to immunity in a series of detailed sections, such that the existence of immunity under public international law is not conclusive as to whether immunity has been removed by the 1978 Act. As Lord Diplock observed in *Alcom* at p. 600, the fact that the bank account of the Colombian diplomatic mission which the respondents in that case sought to make the subject of garnishee proceedings would have been entitled to immunity from attachment under public international law, at the date of the passing of the 1978 Act, was not sufficient to establish that it enjoyed immunity under the Act; it made it highly unlikely that Parliament intended to require United Kingdom courts to act contrary to international law unless the clear language of the statute compelled such a conclusion; but it did not do more than this.

> 40. In the converse situation, however, in which there would be no immunity under customary international law, there is a more direct correlation between immunity under customary international law and the 1978 Act as a result of the enactment of sections 3 and 4 the Human Rights Act 1998 and the application of article 6 ECHR, together with Article 47 of the Charter of Fundamental Rights of the European Union. As explained in *Benkharbouche*, any immunity granted to a State is necessarily incompatible with Article 6 as disproportionate if and to the extent that it grants to a state an immunity which would not be afforded in accordance with customary international law. Section 3 of the Human Rights Act requires that so far as it is possible to do so, legislation must be given effect in a way which is compatible with the Convention rights. This is an interpretative obligation of strong and far reaching effect which may require the court to depart from the legislative intention of Parliament, in accordance with the principles articulated in *Ghaidan v Godin-Mendoza* [2004] UKHL 30, [2004] 2 AC 557 and *Sheldrake v Director of Public Prosecutions* [2004] UKHL 43, [2005] 1 AC 264. The alternative remedy of a declaration of incompatibility under section 4 is a remedy of last resort (*Ghaidan* at [46], *Sheldrake* at [28]).”

59. Paragraph 39 accords with the well-understood rule that international law obligations, while relevant in resolving any ambiguity in the meaning of statutory language, are not capable of overriding the terms of a statute which lack such ambiguity: *Lesa v AG of New Zealand* [1983] 2 AC 20, 33. This was the approach of Lord Porter in *Theophile v Solicitor-General* [1950] AC 186, (cited in relation to the SIA 1978 in *Al-Adsani (No 2)*, p548), in which the House of Lords had to consider the impact of the law of nations (now generally referred to as customary international law) upon certain provisions of the Bankruptcy Act 1914. At p195 Lord Porter said this:

> “Interpreted in accordance with its strict wording, the latter sub-section applies to British and foreign nationals alike, and unless some principle to the contrary can be established I should so construe it. If I am right in this an invocation of the comity of nations is irrelevant. If the meaning of an Act of Parliament is ambiguous that doctrine may be prayed in aid, but where an English statute enacts a provision in plain terms no such principle applies. Any foreign nation of which the person affected is a member or with which such person is domiciled is free to disregard the provisions of the English enactment, but the person concerned cannot himself take exception to it, though it may be that he will escape from compliance with its terms because he is out of the jurisdiction and cannot be reached by the English process.”

60. Section 5 is not a complicated provision. On its face, it is concerned with *all* acts and omissions in the UK, of whatever type (ie, both those done *jure imperii* and those done *jure gestionis*) causing death, etc.

61. In *Al-Adsani (No 2)*, p549, Ward LJ rejected the submission advanced on behalf of the claimant that s 5 could be read to include acts of torture committed abroad, so that there is an exception to immunity for acts of torture (the prohibition of which is *jus cogens*, ie, a rule of international law from which no derogation is permitted), committed by a foreign state *outside* of the UK. He said (emphasis added):

> "An action for damages for torture is a form of proceeding in respect of personal injury. It is inconceivable that Parliament legislated for the loss of State immunity when the acts causing that person injury are committed in the United Kingdom without having borne in mind its clearest international obligations to recognize the fundamental freedom from torture which everyone should enjoy everywhere. *Unfortunately, the Act is as plain as plain can be.* A foreign State enjoys no immunity for acts causing personal injury committed in the United Kingdom and if that is expressly provided for the conclusion is impossible to escape that State immunity is afforded in respect of acts of torture committed outside this jurisdiction."

62. This passage was approved by Lord Bingham in *Jones*, [13]:

> "On a straightforward application of the 1978 Act, it would follow that the Kingdom's claim to immunity for itself and its servants or agents should succeed, since this is not one of those exceptional cases, specified in Part 1 of the 1978 Act, in which a state is not immune, and therefore the general rule of immunity prevails. It is not suggested that the Act is in any relevant respect ambiguous or obscure: it is, as Ward LJ observed in *Al-Adsani v Government of Kuwait (No 2)* (1996) 107 ILR 536, 549, 'as plain as plain can be'. In the ordinary way, the duty of the English court is therefore to apply the plain terms of the domestic statute."

63. Therefore, it seems to me that the key issue is whether there is a sound basis for construing s 5 in the restrictive way Mr White urged upon me, despite its plain terms. The starting point is to apply the ordinary canons of statutory construction.

64. The first canon is Lord Bingham's stricture that the duty of the English court is to apply the plain terms of the domestic statute. Next, I consider to be relevant the presumption (to the extent it is different from Lord Bingham's statement) that the grammatical meaning of an enactment is the meaning that was intended by the legislator: *Bennion, Bailey and Norbury on Statutory Interpretation* (8th Edn), s 11.4. *Bennion* says at s 11.4, in a section which has been judicially approved in *R (Shropshire and Wrekin Fire Authority and others) v Secretary of State for the Home Department* [2019] EWHC 1967, [55]; *Edwards v S J Henderson & Company Ltd* [2019] EWHC 2742,[63]; *Jeffrey v Sawyer* (1993) 16 OR (3d) 75, 78; *Maguire v DPP* [2004] 3 IR 241, [45]; *Alcan (NT) Alumina Pty Ltd v Comr of Territory Revenue* (2009) 239 CLR 27, [47]:

"There is a presumption that the grammatical meaning of an enactment is the meaning that was intended by the legislator.

Comment

The grammatical meaning is arrived at without taking into account legal considerations (see Code s 10.4).

The initial presumption is in favour of the grammatical meaning, since the legislature is taken to mean what it says. The presumption is of very longstanding (sic), being embodied in early maxims of the law. Broom cites the maxim *Quoties in verbis nulla est ambiguitas, ibi nulla expositio contra verba non fienda est* (where nothing in the words is ambiguous, no exposition of them shall be made which is opposed to the words) [Legal Maxims (1st edn, 1845) pp 266ff (one must not depart from the words of a statute:see 5 Co Rep 119)].

This presumption in favour of grammatical interpretation was stated by a nineteenth-century Lord Chancellor, Lord Selborne, in the words 'there is always some presumption in favour of the more simple and literal interpretation of the words of the statute' [*Caledonian Rly Co v North British Rly Co* (1881) 6 App Cas 114 at 121]

More recently, in *Maunsell v Olins* [[1975] AC 373 at 391F] Lord Simon said 'statutory language must always be given presumptively the most natural and ordinary meaning which is appropriate in the circumstances.'

Judges of the present day show no inclination to abandon the presumption. So, for example, in *R v Secretary of State for the Environment, Transport and the Regions, Ex p Spath Holme Ltd* [[2001] 2 AC 349 at 397]. Lord Nicholls said:

> '… an appropriate starting point is that language is to be taken to bear its ordinary meaning in the general context of the statute.

Although Lord Bingham pointed out in *R (Jackson) v Attorney General* [[2005] UKHL 56, [30].] that 'the literal meaning of even a very familiar expression may have to be rejected if it leads to an interpretation or consequence which Parliament could not have intended', this passage indicates that the grammatical meaning is the starting point and may not be rejected without cause."

65. In *R v Bentham* [2005] 1 WLR 1057, Lord Bingham said**:**

"Rules of statutory construction have a valuable role when the meaning of a statutory provision is doubtful, but none where, as

> here, the meaning is plain. Purposive construction cannot be relied on to create an offence which Parliament has not created. Nor should the House adopt an untenable construction of the subsection simply because courts in other jurisdictions are shown to have adopted such a construction of rather similar provisions."

66. All of this supports the construction of 'act or omission' in s 5 as meaning 'all acts or omissions', without any restriction as to the nature of the act being read into it.

67. It seems to me that a further strong pointer that Parliament did not intend s 5 only to cover acts done *jure gestionis* is the fact that in a number of other sections in the Act, Parliament *did* choose to refer to sovereign authority in order to restrict exceptions to the general immunity conferred by s 1(1). So, s 3 provides (emphasis added):

> "3 Commercial transactions and contracts to be performed in United Kingdom.
>
> (1) A State is not immune as respects proceedings relating to—
>
> (a) a commercial transaction entered into by the State; or
>
> (b) an obligation of the State which by virtue of a contract (whether a commercial transaction or not) falls to be performed wholly or partly in the United Kingdom.
>
> (2) This section does not apply if the parties to the dispute are States or have otherwise agreed in writing; and subsection (1)(b) above does not apply if the contract (not being a commercial transaction) was made in the territory of the State concerned and the obligation in question is governed by its administrative law.
>
> (3) In this section 'commercial transaction' means -
>
> (a) any contract for the supply of goods or services;
>
> (b) any loan or other transaction for the provision of finance and any guarantee or indemnity in respect of any such transaction or of any other financial obligation; and
>
> (c) any other transaction or activity (whether of a commercial, industrial, financial, professional or other similar character) into which a State enters or in which it engages *otherwise than in the exercise of sovereign authority*;
>
> but neither paragraph of subsection (1) above applies to a contract of employment between a State and an individual."

68. Section 14 provides (again, emphasis added):

> "States entitled to immunities and privileges

> (1) The immunities and privileges conferred by this Part of this Act apply to any foreign or commonwealth State other than the United Kingdom; and references to a State include references to—
>
> (a) the sovereign or other head of that State in his public capacity;
>
> (b) the government of that State; and
>
> (c) any department of that government,
>
> but not to any entity (hereafter referred to as a 'separate entity') which is distinct from the executive organs of the government of the State and capable of suing or being sued.
>
> (2) A separate entity is immune from the jurisdiction of the courts of the United Kingdom if, and only if—
>
> (a) the proceedings relate to *anything done by it in the exercise of sovereign authority*;
>
> and
>
> (b) the circumstances are such that a State (or, in the case of proceedings to which section 10 above applies, a State which is not a party to the Brussels Convention) would have been so immune."

69. The canon of construction that is engaged here is the principle that where Parliament has omitted particular words used in one part of an Act from an equivalent context in another part of the Act, such an omission will generally be treated as deliberate and as connoting a different approach in the two contexts: *Bennion*, s 21.3; *R (M) v Gateshead Council* [2007] 1 All ER 1262, [19]. *Bennion* comments on that case as follows:

> "In *R (on the application of M) v Gateshead Council* Dyson LJ said of provisions in the Children Act 1989:
>
> > '… it is striking that the duties in ss 17, 18, and 20 are all owed by local authorities to children 'within their area', but that this qualifying phrase is absent from s 21. It would be striking if this omission were not deliberate.'
>
> This helped to show in relation to the s 21 duty (where those words were absent) that the duty applied to all children."

70. This is consistent with the approach adopted in *Shepherd v Information Commissioner* [2019] EWCA (Crim) 2, [44]:

> "The fact that the legislature has chosen one form of words on three occasions, and a different (and, as we have said, atypical)

> formulation on two, is a strong indicator that the intention of Parliament was to achieve different legal results."

71. In light of this, I find it impossible to construe s 5 in the narrow way contended for by Mr White. In these sections Parliament demonstrated that it well understood the dichotomy between acts done *jure imperii* and acts done *jure gestionis*. If, in s 5, it had intended immunity still to attach to the former in respect of personal injury, etc, it might have been expected to have used language such as, '… caused by an act or omission (other than one done by it in the exercise of sovereign authority) in the United Kingdom.' It did not do so. Hence, in my judgment, s 5 applies in respect of *all* acts and omissions of a foreign state, of whatever character, provided they occurred in the UK and caused personal injury, etc. This is the plain meaning of s 5 of the SIA 1978.

72. Strong support for this conclusion is to be found in the judgment of Ward LJ in *Al-Adsani (No 2)*, p549, which I quoted earlier, where he said that an action for damages for torture is a form of proceeding in respect of personal injury; that it was inconceivable that Parliament legislated for the loss of state immunity when the acts causing that person injury were committed in the UK without having borne in mind its clearest international obligations to recognize the fundamental freedom from torture which everyone should enjoy everywhere; and that a foreign state enjoys no immunity for acts causing personal injury committed in the UK.

73. As a matter of domestic and international law, torture can *only* be committed by a public official (or at their instigation) and those acting in an official capacity: see s 134, Criminal Justice Act 1988; Article 1 of the UN Convention Against Torture (considered at length in *R v Bow Street Magistrates Court ex parte Pinochet Ugarte (No 3)* [2000] AC 147); and Article 1 of UN General Assembly Resolution 3452 (1975), cited in *Al-Adsani (No 2)*, p540.

74. In that sense, therefore, torture is the very epitome of a sovereign or governmental act. In *Saudi Arabia v Nelson* 507 US 349 (1993), a decision of the US Supreme Court, Mr Nelson sued Saudi Arabia for torture committed in Saudi Arabia. Souter J wrote at pp361-2:

> "The conduct boils down to abuse of the power of its police by the Saudi Government, and however monstrous such abuse undoubtedly may be, a foreign state's exercise of the power of its police has long been understood for purposes of the restrictive theory as peculiarly sovereign in nature. See *Arango* v. *Guzman Travel Advisors Corp., 621* F. 2d 1371, 1379 (CA5 1980); *Victory Transport Inc.* v. *Comisaria General de Abastecimientos y Transportes,* 336 F.2d 354, 360 (CA2 1964) (restrictive theory does extend immunity to a foreign state's 'internal administrative acts"), cert. denied, 381 U. S. 934 (1965); *Herbage* v. *Meese,* 747 F. Supp. 60, 67 (DC 1990), affirmance order, 292 U. S. App. D. C. 84, 946 F.2d 1564 (1991); K. Randall, Federal Courts and the International Human Rights Paradigm 93 (1990) (the Act's commercial-activity exception is irrelevant to cases alleging that a foreign state has violated human rights). Exercise of the powers of police and penal officers is not the sort of action by which

> private parties can engage in commerce. "[S]uch acts as legislation, or the expulsion of an alien, or a denial of justice, cannot be performed by an individual acting in his own name. They can be performed only by the state acting as such." Lauterpacht, The Problem of Jurisdictional Immunities of Foreign States, 28 Brit. Y. B. Int'l L. 220, 225 (1952); see also id., at 237."

75. To like effect is Lord Bingham's statement in *Jones,* [19]:

> "It is, I think, difficult to accept that torture cannot be a governmental or official act, since under article 1 of the Torture Convention torture must, to qualify as such, be inflicted by or with the connivance of a public official or other person acting in an official capacity."

76. Hence, it seems to me that Ward LJ was indicating that a state would not have immunity in an action for damages for personal injury arising from torture because of s 5, and thus, because torture is by definition a sovereign act, s 5 extends to such acts.

77. I consider that the main act of which the Claimant complains in this case, namely installing spyware on his iPhones, is less obviously sovereign in nature than torture. Unlike torture, it is an act which *can* be carried out by a private individual. Such persons can, and no doubt sometimes do, install spyware on the devices of those whom they wish to target, for example, to commit industrial espionage, or for other nefarious reasons. However, I am prepared to accept in the Defendant's favour that the act of installing spyware in the present case was an act done *jure imperii*. However, for the reasons I have given, the Defendant does not enjoy immunity simply for that reason. The assault on the Claimant (*if* the Defendant can be shown on a balance of probabilities to have been responsible, which I discuss as issue (e)) similarly does not fall outside s 5.

78. Support for my conclusion that acts done *jure imperii* fall within s 5 is provided by Fox and Webb, *The Law of State Immunity* (3rd rev ed, 2015), p200, in relation to the s 5 exception:

> "This is a potentially wide exception, in that it covers the commission of torts in the course of sovereign as well as private activities …"

79. My view is also supported by Garnett, in *The Defence of State Immunity for Acts of Torture,* (1997) 18 Australian Year Book of International Law 97. The author concluded, after addressing *Al-Adsani (No 2)*:

> "However, what is interesting about this discussion is that it confirms that English courts will take a view similar to the US courts in the *Letelier* case, that is, the availability of the tort exception will not be premised on any distinction between sovereign and private or commercial acts. If, therefore, acts of

> torture have been committed in the forum which are attributable to a foreign State, a plaintiff will be entitled to sue."

80. The reference to *Letelier* is to the decision of the US District Court for the District of Columbia, *Letelier v Republic of Chile* 488 F Supp 665 (DDC 1980).

81. In 1973 General Augusto Pinochet overthrew the left-wing government of Salvador Allende in Chile in a *coup d'état* and installed a right wing military junta. The junta was accused of wide-spread torture and human rights abuses. At the time of the *coup* Orlando Letelier was Minister of Foreign Affairs. He eventually settled in the United States and became a leading critic of the Pinochet regime.

82. On 21 September 1976 Letelier and his co-worker Ronni Moffitt were killed by a car bomb as they drove to work in Washington DC. Investigations concluded that the bombing had been carried out by Chilean secret service agents on behalf of the Pinochet regime.

83. Letelier's and Moffitt's representatives sued Chile and named individuals for damages for conspiracy to deprive Letelier and Moffitt of their constitutional rights; assault and battery causing their deaths; as well as in other causes of action.

84. The plaintiffs obtained default judgment, and Chile asserted immunity. The Court therefore considered the question of sovereign immunity and whether the assassination was an act covered by immunity under the Foreign State Immunities Act 1976 (FSIA), contained in Title 28 of the United States Code (USC). Like the SIA 1978, the FSIA this sets out a general immunity for foreign states and then specifies exceptions to it. The one relied on by the plaintiffs was 28 USC 1605(a)(5), which provides that a foreign state is not entitled to immunity from an action seeking money damages 'for personal injury or death. caused by the tortious act or omission of that foreign state' or its officials or employees.

85. At p671 US District Judge Joyce Hens Green wrote:

> "… plaintiffs have set forth several tortious causes of action arising under international law, the common law, the Constitution, and legislative enactments, pp. 666-667 supra, all of which are alleged to spring from the deaths of Orlando Letelier and Ronni Moffitt. The Republic of Chile, while vigorously contending that it was in no way involved in the events that resulted in the two deaths, further asserts that, even if it were, the Court has no subject matter jurisdiction in that it is entitled to immunity under the Act, which does not cover political assassinations because of their public, governmental character."

86. She went on to note, by reference to legislative materials, Chile's argument that the exception to immunity in 28 USC 1605(a)(5) had been primarily intended to include only private torts, like automobile accidents. It is clear that Chile's argument was not wholly dissimilar to the argument advanced before me by the Defendant.

87. The judge said the flaw in Chile's argument was that it did not address the statutory language, which she said was 'plain', a view entirely in keeping with that of Ward LJ and Lord Bingham in relation to s 5 of the SIA 1978. The judge went to say at p671:

> "… a foreign state is not entitled to immunity from an action seeking money damages 'for personal injury or death . . caused by the tortious act or omission of that foreign state' or its officials or employees. Nowhere is there an indication that the tortious acts to which the Act makes reference are to only be those formerly classified as 'private,' thereby engrafting onto the statute, as the Republic of Chile would have the Court do, the requirement that the character of a given tortious act be judicially analyzed to determine whether it was of the type heretofore denoted as *jure gestionis* or should be classified as *jure imperii*. Indeed, the other provisions of the Act mandate that the Court not do so, for it is made clear that the Act and the principles it sets forth in its specific provisions are henceforth to govern all claims of sovereign immunity by foreign states."

88. I acknowledge that caution must always be exercised when placing weight on decisions of foreign courts in relation to different legislation (a point I will return to), but so far as it goes, I think this passage is helpful to the Claimant and supports his position.

89. I note that in *Benkharbouche*, [10], Lord Sumption said that the exceptions in the SIA 1978 'related to a broad range of acts conceived to be of a private law character'. Respectfully, I do not consider this observation provides any assistance to the Defendant. Firstly, as the following words of the sentence make clear, Lord Sumption was talking specifically of commercial transactions and commercial activities, as well as contracts of employment and enforcement against state-owned property used or intended for use for commercial purposes. Second, the case was not about s 5 and the *imperii/gestionis* dichotomy. The question at issue on the appeal, as Lord Sumption explained at [1], was whether two provisions of the SIA 1978 are consistent with the European Convention on Human Rights (ECHR) and the European Union Charter of Fundamental Rights. The two provisions are ss 4(2)(b) and 16(1)(a). In summary the effect of section 4(2)(b) is that a state is immune in respect of proceedings relating to a contract of employment between a state and a person who at the time of the contract is neither a national of the UK nor habitually resident there; and the effect of section 16(1)(a) is that a state is immune as respects proceedings concerning the employment of members of a diplomatic mission, including its administrative, technical and domestic staff. It was therefore concerned with a different issue to the one I am addressing, as Lord Sumption made clear at [39] when he said the case was not concerned with whether the acts in question were covered by an exception in the SIA 1978 (the issue before me), but whether the immunity they confer is wider than customary international law requires, 'and that raises different considerations.'

90. The conclusion I have reached on the construction of s 5 accords with the view of the authors of Dickinson et al, *State Immunity: Selected Materials and Commentary* (2004), [4.049]:

> "Section 5 corresponds broadly to Article 11 of the European Convention [on State Immunity]. Article 11 and s 5 are notable

> in representing, respectively, the Convention and the 1978 Act's clearest departure from the traditional distinction between sovereign and private acts. Conduct in the United Kingdom attributable to a foreign State causing death, personal injury or damage to property anywhere in the world may be the subject of proceedings in a United Kingdom court, however sovereign its character – for example, the actions of a foreign secret service or presidential bodyguard."

91. Article 11 of the European Convention on State Immunity 1972 (the Basle Convention) (ETS 74) provides:

> "A Contracting State cannot claim immunity from the jurisdiction of a court of another Contracting State in proceedings which relate to redress for injury to the person or damage to tangible property, if the facts which occasioned the injury or damage occurred in the territory of the State of the forum, and if the author of the injury or damage was present in that territory at the time when those facts occurred."

92. In *Benkharbouche,* [9], Lord Sumption described the Basle Convention as:

> "… a regional treaty drawn up under the auspices of the Council of Europe which identified specified categories of acts done by foreign states in the territory of the forum state which would not attract immunity. These treaties were concerned mainly with acts of a kind which would generally not attract immunity under the restrictive doctrine. But neither of them sought to codify the law of state immunity or to apply the restrictive doctrine generally. In addition, they have attracted limited international support. The Brussels Convention of 1926 [ie, the International Convention for the Unification of Certain Rules concerning the Immunity of State-Owned Vessels] has attracted 31 ratifications to date. The Basle Convention of 1972 has to date been ratified by only eight of the 47 countries of the Council of Europe.
>
> 10. One purpose of the State Immunity Act 1978 was to give effect to the Brussels and Basle Conventions, and thereby enable the United Kingdom to ratify them. It did this in both cases in 1979 …"

93. It is now time to consider the decisions of Laws J (as he then was) and the Court of Appeal in *Propend*. As I have said, Mr White contended these decisions were conclusive in the Defendant's favour on this issue, and that the Court of Appeal's decision was binding upon me.

94. The facts are somewhat convoluted, but in summary were as follows. In August 1993, the Attorney-General of Australia made a request to the Government of the United Kingdom, pursuant to the 1986 Scheme relating to Mutual Assistance in Criminal Matters within the Commonwealth (the Harare Scheme), to seek a Court order to search for documents relating to an investigation being conducted by the Australian Federal

Police (the AFP) into suspected tax evasion. The investigation concerned the plaintiff company, Propend Finance Pty Limited (Propend). In response to this request, the Home Secretary issued directions to the Metropolitan Police in London under the Criminal Justice (International Cooperation) Act 1990. Acting under these directions, officers of the Metropolitan Police applied for search warrants, which were issued by a judge at the Central Criminal Court on 26 October 1993. The first defendant, Superintendent Alan Sing, who was an officer of the AFP and an accredited diplomat with the role of police liaison officer at the Australian High Commission in London, gave evidence at the hearing at which the warrants were issued. The following day, the Metropolitan Police seized documents from the premises of a firm of solicitors and a firm of accountants in London. These documents were subsequently handed by the Metropolitan Police to the first defendant who took them to the premises of the Australian High Commission.

95. The plaintiffs sought judicial review of the decision to issue the search warrants, and on 29 October 1993 applied to the High Court for an interlocutory injunction restraining the first defendant from dealing with the documents. At the hearing of the application for an injunction before Potts J, the first defendant gave an undertaking to the Court that neither the documents nor copies thereof would be removed from the jurisdiction of the Court or from the High Commission and that copies of the documents would not be transmitted by fax. The decision to issue the search warrants was subsequently quashed by the Divisional Court in March 1994.

96. Several months later, the plaintiffs discovered that the first defendant had sent extracts from the seized documents to the headquarters of the AFP in Canberra shortly after giving the undertaking to the Court. The plaintiffs alleged that this communication was in breach of the undertaking and instituted proceedings for contempt of court against the first defendant, who by then had completed his appointment in the UK and returned to Australia, and the Commissioner of the AFP, who was sued as representing the AFP. The defendants maintained that the Court lacked jurisdiction, because the first defendant was entitled to diplomatic immunity and both defendants were protected by state immunity.

97. The plaintiffs were given leave by the Master to serve the contempt proceedings out of the jurisdiction, and he made other orders for service. The matter came before Laws J on the defendants' application to set the Master's orders aside, on the grounds of immunity.

98. After setting out the facts, Laws J turned to the law at p628. One of the issues he considered was whether the AFP was entitled to immunity under s 14 of the SIA 1978 as falling within the expression 'the government' in s 14(1)(b) or a 'department of that government' (in s 14(1)(c)), both of which are entitled to the general immunity conferred by s 1(1) and to which the exceptions to immunity in the Act apply.

99. The judge held that the AFP did not fall within either provision (at p651) and so was not entitled to immunity (at p653). After referring to a German case he said at p652:

> "The case throws no light on the question whether the AFP are, by the law of Australia, part of the executive federal government. In my judgment they are not. Certainly they exercise public power, but not all public power is the power of the executive.

> They owe, and perform, important obligations to the State, but not all such obligations are owed in right of executive government. The issue on this part of the case does not in my judgment depend upon the well-established distinction between acts done *jure imperii* and acts done *jure gestionis*. Obviously the police function is not a commercial one; but it does not follow that it is a function of the executive. The divide between acts *jure imperii* and acts *jure gestionis* may be critical in a case where it is plain that what has been done has been done by the government, or by a putative separate entity so as potentially to engage section 14(2)."

100. The plaintiffs had contended that the AFP did not fall within s 14(1)(b) or (c), but that if it did, then it did not have immunity (*inter alia*) because of s 5. As to this, Laws J said at pp651-652:

> "Mr Pleming [for the plaintiffs] had a number of submissions to the effect that, if he was wrong about the status of the AFP, nevertheless they were excluded from immunity on specific grounds … Secondly, by virtue of Section 5(b) of the Act of 1978 the AFP is deprived of immunity, because the proceedings before Potts J were in respect of damage or loss of tangible property caused by an act or omission in the United Kingdom. The property is said to be seized documents. I would not have upheld Mr Pleming's argument on this ground. It seems to me that Section 5(b) is concerned with what I may call ordinary private law claims. The section's flavour is given by para (a), the reference to death or personal injury. There is I think no authority on the point, but I incline to the view that the section's rationale may he lie in the fact that an accident causing personal injury, or some event causing damage to property (or its loss), is for the most part likely to involve acts or omissions by a servant of the foreign State in question which are incidental to the State's sovereign status, rather than integral to it. Where, as here, property is seized pursuant to an order of the court, obtained following a direction of the Secretary of State following a request made at the international level, neither the seizure nor the property's later retention can in my judgment fall within Section 5(b). It is true that the proceedings before Potts J fall to be regarded procedurally as part and parcel of the writ action which was issued after the hearing; and in form that was a private law claim. But in truth, as I have made clear, it was ancillary to the judicial review. In the alternative I would conclude the section 5(b) issue against the plaintiffs on the short ground (as submitted in Mr Mayhew's skeleton argument) that the 'loss' of the documents was not caused by an act or omission in the UK by Australia, but by the Metropolitan Police acting under Judge Goddard's order."

101. Laws J handed down his judgment on 14 March 1996. The decision of the Court in *Al-Adsani (No 2)* had only been handed down two days earlier, on 12 March 1996. Unsurprisingly, therefore, Laws J was not referred to it. I will return to this point later.

102. Laws J found that Inspector Sing (the first defendant) was entitled to immunity, and the plaintiffs appealed to the Court of Appeal against that finding. The Commissioner of the AFP (the second defendant) cross-appealed against the finding that the AFP was not entitled to immunity. There was a Respondents' Notice on the cross-appeal. This was summarised by the Court of Appeal at pp664-665:

> "They also rely by Respondents' Notice on three alternative arguments that the Commissioner has no immunity because (i) the present action constitutes 'proceedings in respect of … damage or loss of tangible property' within Section 5(b) of the 1978 Act; (ii) the Commissioner instituted the present action and is therefore deemed to have submitted to the jurisdiction and waived any immunity under Sections 2(1) and (3)(a); and (iii) the Commissioner had submitted to the jurisdiction, by the giving by the Superintendent of the undertakings on the cross-appeal that the action constituted 'proceedings in respect of … damage or loss of tangible property within s 5(b) of the SIA 1978 (at p664)."

103. The Court of Appeal dealt with the s 5 point in the briefest of terms at p664:

> "About the first two we need say no more than that they were succinctly rejected by the judge (at pages 52–3 of his judgment) on grounds with which we agree. To the third we shall refer at the end of this judgment."

104. I am, with respect, unable to accept the Defendant's submission that these passages are binding upon me as a matter of *stare decisis* in relation to the issue that I have to decide, namely the proper interpretation of 'act or omission' in s 5 of the SIA 1978. That is for the following reasons.

105. Firstly, Laws J was not concerned with the interpretation of that phrase. He was not addressed upon, nor addressed, the question whether s 5 extends to acts done *jure imperii* as well as acts done *jure gestionis*. The judge himself made this point in a passage at p652 ('The issue on this part of the case does not in my judgment depend upon the well-established distinction between acts done *jure imperii* and acts done *jure gestionis*.'). He did not lay down any general principle that an act or omission will fall outwith the scope of s 5 if it is sovereign in nature.

106. Second, it seems to me the Claimant is right to say that the passage in issue was, in any event, *obiter dicta*, given that the judge had already found that the AFP was not entitled to immunity as falling outwith s 14. Thus, the applicability or otherwise of s 5 on the facts of the case did not arise. That the passage in question was (and was intended) to be *obiter* I think is supported by the judge's phraseology (emphasis added): '*I would not have* upheld Mr Pleming's argument on this ground.' This does not seem to me to be a sign the judge was intending to reach a definitive conclusion on the issue. Added to this is the fact that he was much more definite on the basis on which he *did* determine

the s 5 point against the plaintiffs, namely, the act in question was not done by or on behalf of Australia in the UK, but had been done by the Metropolitan Police. He introduced his conclusion with the words, 'In the alternative I would conclude the Section 5(b) issue against the plaintiffs …'; not, it is to be noted, 'I *would have* concluded …' The judge's other, much more definitive conclusion, that the action did not fall within s 5 was grounded in the fact that the proceedings before Potts J were 'ancillary to the judicial review' and therefore not in reality an 'ordinary private law claim'. It was the true juridical nature of the proceedings in that case rather than a binary distinction between governmental and non-governmental acts which drove that conclusion.

107. Third, Laws J's language elsewhere smacks of a tentative *obiter dictum* and no more. I refer in particular to, 'There is I think no authority on the point, *but I incline to the view* that the section's rationale *may* be … *for the most part likely to involve*' (emphasis added).

108. Fourth, and with all due respect to a judge rightly regarded as one of the 20th century's greatest judges, Laws J's view that s 5 is '… for the most part likely to involve acts or omissions by a servant of the foreign State in question which are incidental to the State's sovereign status, rather than integral to it', cannot sit easily with *Al-Adsani (No 2)*, to which he was not referred. I therefore think that this statement was made *per incuriam*. Torture is, by definition, a sovereign act, and *Al-Adsani (No 2)* makes clear that such acts – which are not merely incidental to the State's sovereign status but are integral to it – fall within s 5 if committed within the UK.

109. It therefore seems to me that the central thrust of the reasoning underlying Laws J's decision on s 5 was that although the proceedings in question were, in form, a private law action, in substance they were part of the judicial review claim. The same is not true of the present case. As the Claimant rightly says, it is in substance *and* form a private law claim for damages.

110. I do not consider, again with respect, that the Court of Appeal's very brief approval of Laws J's approach can convert it into a binding *ratio*, given the way in which the judge expressed himself. The Court of Appeal's view was no more than a bare approval of a tentatively expressed *obiter dictum* which, in light of *Al-Adsani (No 2)*, was in my view *per incuriam*. Like Laws J, the Court of Appeal does not appear to have been referred to that decision. I also agree with the Claimant that the terms in which the Court of Appeal expressed itself indicates that no general rule as advanced by the Defendant in this case can be spelled out of the ratio of the case: see *Great Western Railway Co v Owners of SS Mostyn* [1928] AC 57, [73].

111. I also need to briefly mention the judgment of Stewart J in *Estate of Michael Heiser and 121 Others v Islamic Republic of Iran* [2019] EWHC 2074, [131]. The case was complicated, but at bottom it concerned the enforcement of judgments obtained by various claimants in the US Federal District Court for the District of Columbia. They arose out of a number of attacks around the world at various times in recent history in which citizens of the United States were either killed or severely injured. Very often the basis of the finding against the Government of Iran had been that it had conspired to cause the deaths or injuries concerned and had provided assistance by way of

resources to terrorist organisations, knowing that it was doing so, and that that assistance then led to the deaths or injuries of American citizens.

112. At [131] Stewart J said:

> "Although not argued before me, it occurs to me that there may possibly be a more fundamental objection to enforcement. This would be that when a foreign state commits an inherently sovereign or governmental act, section 5 has no application since it cannot deprive the state of its defence of state immunity. This is because in such circumstances customary international law provides a complete defence – see *Benkharbouche* at [17]; see also the reference at [10] that the exceptions in the 1978 Act 'relate to a broad range of acts conceived to be of a private law character' Obviously I do not rule on this, in the absence of argument. I merely mention it."

113. Whilst I note this paragraph, it plainly does not amount to a conclusion of law that I am required to consider further.

114. Before me there was extensive and impressive citation of public international law materials, in particular by Mr White on behalf of the Defendant. However, in accordance with *Lesa*, this material cannot assist the Defendant because s 5 is not ambiguous, as *Al-Adsani (No 2)* and *Jones* make clear. In *Lesa*, Lord Dipock said at p33:

> "Despite the fact that the resolutions (of the Council of the League of Nations) did not impose on the Government of New Zealand any obligation binding upon it in International Law, their Lordships agree with the Court of Appeal that the resolutions would be relevant in resolving any ambiguity in the meaning of the language ... They are, however, unable, for reasons already stated, to discern any ambiguity or lack of clarity in that language ..."

115. For similar reasons, I decline to consider the materials deployed by the Defendant under *Pepper v Hart* for the reasons given by the Claimant at [38]-[42] of his Skeleton Argument.

116. It follows that I determine the first issue in favour of the Claimant. The acts of which he complains do not fall outside s 5, even assuming that they are acts done *jure imperii*. Section 5 operates to remove the immunity otherwise conferred by s 1 on a foreign state in relation to all acts committed by it, whether sovereign or private, subject obviously to the other requirements of s 5 being satisfied.

117. The Claimant made submissions, in the event I was against him on his primary submission, that the restriction on his right of access to court contended for by the Defendant is not required by any rule of customary international law, and so violates Article 6 of the ECHR, applying by analogy the analysis in *Benkharbouche*. However, I need not consider those submissions further in light of the conclusion I have reached on his primary submission.

(b) Does the claim fail to meet the requirements of s 5 because the alleged personal injury resulting from the spyware claims was not caused by an act or omission in the UK ?

118. The questions here are whether: (a) s 5 only applies where the whole tort causing death, etc, is committed within the UK, as the Defendant contends, or (b) whether it applies so long as some substantial and effective act causative of the required damage has been committed within the jurisdiction (whether or not other substantial and effective acts have been committed elsewhere), which is the Claimant's contention.

119. The parties are agreed that there is no authority which is directly on point, or certainly none which is of clearly binding effect.

120. I start with the statutory language. For the reasons I have already explained, it is to be presumed that the grammatical meaning of an enactment is the meaning that was intended by the legislator. In my judgment, the grammatical meaning of s 5, and in particular the use of the indefinite article (death or personal injury caused by '*an* act or omission') (emphasis added) means what it says. There has to be *an* act or omission in the UK which is causative of the requisite damage on a more than *de minimis* basis. Parliament did not say '*the* act or omission', still less, 'acts or omissions occurring entirely within the UK', both of which would have been more supportive of the Defendant's interpretation of s 5. This suggests the Claimant's contention is the correct one.

121. Such domestic authority as there is on this question supports, in a limited way, the Claimant's interpretation. In *Heiser v Islamic Republic of Iran* [2012] EWHC 2938 (QB) (the same case which later came before Stewart J), on an *ex parte* application for permission to serve the claim form out of the jurisdiction, Singh J (as he then was) held that the claimants had a good arguable case that the s 5 exception applied in relation to international conspiracies causing death and injury to US citizens. He said at [6]-[7]:

> "6. The issue which may arise under the State Immunity Act is whether section 5 would apply if this were a case which arose in the United Kingdom. By way of analogy, the question will become whether the death or personal injury had been caused 'by an act or omission in the United States'.
>
> 7. The essential submission for the claimants at this stage is that there is a good arguable case that there would be jurisdiction if a similar action were to arise in the United Kingdom, on the basis of a conspiracy being regarded as a composite act. It is said that the conspiracies concerned could properly be regarded as being conspiracies not just against those individuals but their relatives and indeed the public more generally in the United Kingdom. So, by way of analogy, it is said in the present cases conspiracies can be analysed as being conspiracies not just to cause injury or death to American citizens, but also to damage their families and also to damage the public in the United States more generally. That, it is submitted, is one of the inherent features of the scourge of international terrorism, as it has been described by courts both in this country and elsewhere. In some of the other cases the analysis

> of the American court was to the effect that the material assistance knowingly provided to terrorist organisations which caused the death or injury in question. Again it is submitted on behalf of the claimants that it is at least arguable at this stage that section 5 of the State Immunity Act would not preclude an action in the United Kingdom if similar proceedings were brought here. I accept those submissions"

122. This reasoning was adopted in *Ben-Rafael v Islamic Republic of Iran* [2015] EWHC 3203 (QB). That case concerned an attempt to enforce a judgment from a US court for damages arising out of a bomb attack in Buenos Aires. Whipple J (as she then was) noted that the US courts had concluded that

> "… the proceedings were caused by an act or omission in the United States, to the extent that the US courts were considering a composite act (namely, one of conspiracy) at least one element of which had occurred within the territory of the US".

123. I accept the Defendant's point that these were short *ex parte* judgments, nonetheless they are judgments of exceptionally distinguished judges and are helpful so far as they go, and provide more support for the Claimant's contention than they do for the Defendant's position.

124. In his 2019 judgment in *Heiser* ([2019] EWHC 2074 (QB)) Stewart J considered s 5 at [134]-[160]. He concluded that, on the facts, s 5 could not apply because all but one of the cases with which he was concerned, '… involved acts or omissions committed in Middle Eastern states, not in the United States' ([146],[148]). He emphasised at [148] that:

> "The fact that either primary victims continued to suffer injury on return to the United States or that secondary victims never left the United States does not assist the Claimants. Section 5 does not permit eliding the act or omission causing the personal injury with where the personal injury occurs. I do not accept that section 5 can be construed with such flexibility as to permit the Claimants' submission to succeed.

125. At [160] he addressed the 'composite act' point. He emphasised that he made:

> "… no decision on the composite act submission e.g. whether firing a missile from country A into another country B is an act in both countries for the purposes of section 5. It is not necessary for me to decide that point since it does not arise on the facts of any of the cases before me."

126. As regards one of the judgements with which he was concerned, the *Acosta* judgment, which concerned an overt act occurring on the forum state's territory (ie, the US) (a shooting), Stewart J held that the case would have come within s 5: [166]-[174], [187(iii)]. His description of the *Acosta* judgment shows that some of the acts involved in the conspiracy occurred outside the US.

127. This series of cases supports the view that s 5 will not apply when *no* act or omission of a foreign state takes place in the UK. But they do not require that *all* acts or omissions must occur in the UK for s 5 to apply, and they indicate that composite acts may fall within s 5.

128. I find support for this interpretation from the cases on the tort jurisdictional gateway in PD 6B, [3.1(9)(b)]. I do not accept the Defendant's suggestion that these cases can readily be distinguished. True, the context is different, but the language is similar. Paragraph [3.1(9)(b)] provides (emphasis added):

> "3.1 The claimant may serve a claim form out of the jurisdiction with the permission of the court under rule 6.36 where –
>
> …
>
> (9) A claim is made in tort where –
>
> (a) damage was sustained, or will be sustained, within the jurisdiction; or
>
> (b) damage which has been or will be sustained results *from an act committed, or likely to be committed, within the jurisdiction*."

129. The approach of the English courts to the predecessor to [3.9(1)(b)] was that it was sufficient that a 'substantial and efficacious act', and not the entire tort, be committed within the jurisdiction: *Metall und Rohstoff AG v Donaldson Lutfin & Jenrette Inc* [1990] 1 QB 391, p437A-G, a case under the old RSC r 11:

> "As the rule now stands it is plain that jurisdiction may be assumed only where (a) the claim is founded on a tort and either (b) the damage was sustained within the jurisdiction or (c) the damage resulted from an act committed within the jurisdiction. Condition (a) poses a question which we consider below: what law is to be applied in resolving whether the claim is "founded on a tort"? Condition (b) raises the question: what damage is referred to? It was argued for ACLI that, since the draftsman had used the definite article and not simply referred to "damage", it is necessary that all the damage should have been sustained within the jurisdiction. No authority was cited to support the suggestion that this is the correct construction of the convention to which the rule gives effect and it could lead to an absurd result if there were no one place in which all the plaintiff's damage had been suffered. The judge rejected this argument and so do we. It is enough if some significant damage has been sustained in England. Condition (c) prompts the inquiry: what if damage has resulted from acts committed partly within and partly without the jurisdiction? This will often be the case where a series of acts, regarded by English law as tortious, are committed in an international context. It would not, we think, make sense to require all the acts to have been committed within the jurisdiction, because again there might be no single jurisdiction where that

would be so. But it would certainly contravene the spirit, and also we think the letter, of the rule if jurisdiction were assumed on the strength of some relatively minor or insignificant act having been committed here, perhaps fortuitously. In our view condition (c) requires the court to look at the tort alleged in a commonsense way and ask whether damage has resulted from substantial and efficacious acts committed within the jurisdiction (whether or not other substantial and efficacious acts have been committed elsewhere): if the answer is Yes, leave may (but of course need not) be given. But the defendants are, we think, right to insist that the acts to be considered must be those of the putative defendant, because the question at issue is whether the links between him and the English forum are such as to justify his being brought here to answer the plaintiffs' claim.'

130. In *Ashton Investments Ltd v OJSC Russian Aluminium* [2007] 1 All ER (Comm) 857, [62]-[63], the test under PD 6B, [3.1(9)(b)] was held to be satisfied in circumstances where a 'hack' of devices located within the jurisdiction emanated from abroad. Jonathan Hirst QC (sitting as a deputy judge of the High Court) said:

> "[62] Ashton's computer server was in London. That is where the confidential and privileged information was stored. The attack emanated from Russia but it was directed at the server in London and that is where the hacking occurred. In my view, significant damage occurred in England where the server was improperly accessed and the confidential and privileged information was viewed and downloaded. The fact that it was transmitted almost instantly to Russia does not mean that the damage occurred only in Russia. If a thief steals a confidential letter in London but does not read it until he is abroad, damage surely occurs in London. It should not make a difference that, in a digital age of almost instantaneous communication, the documents are stored in digital form rather than hard copy and information is transmitted electronically abroad where it is read. The removal took place in London. I also emphatically reject the proposition that the damages claimed are so trivial that the court should decline to bother the defendants with the claim. On the contrary, if the claimants make good the pleaded allegations at trial, then I think this is a very serious and substantial case indeed, with considerable potential ramifications. The cost of replacing the computer and the investigation/consultancy costs may not be very great, but the court will also have to consider what damages and other relief it should grant for the substantial injury caused—viz the improper obtaining of confidential and privileged information.
>
> [63] I also consider that substantial and efficacious acts occurred in London, as well as Russia. That is where the hacking occurred and access to the server was achieved. This may have been as a result of actions taken in Russia but they were designed to make

> things happen in London, and they did so. Effectively the safe was opened from afar so that its contents could be removed. It would be artificial to say that the acts occurred only in Russia. On the contrary, substantial and effective acts occurred in London.

131. To similar effect are *Vidal-Hall v Google Inc* [2014] 1 WLR 4155, [78], and *Lloyd v Google LLC* [2019] 1 WLR 1265, [47], both of which concerned alleged secret transnational tracking of internet users by Google in breach of data protection legislation. Although both *Vidal-Hall* and *Lloyd* were subject to appeal, the analysis on these issues was not revisited on appeal.

132. Where a computer device located in the UK is manipulated and made to perform operations as a result of electronic instructions sent from a computer/operator located abroad then there is authority for the proposition that this is to be regarded as an act within the UK.

133. In *R v Governor of Brixton Prison, ex p Levin* [1997] QB 65, the United States sought Mr Levin's extradition to face trial on 66 charges concerning his alleged unauthorised access to a bank's computer in the United States in order to transfer funds into various bank accounts controlled by him. He had gained access to the US computer by means of his own computer in Russia. The conduct alleged translated under English criminal law into offences of theft, forgery, false accounting and unauthorised modification of computer material. Because of how extradition law operates, there was an issue as to whether what happened in the US would, in equivalent circumstances, be regarded as having happened in the UK. The Divisional Court said at p81:

> "For the reasons we have already indicated, the operation of the keyboard by a computer operator produces a virtually instantaneous result on the magnetic disk of the computer even though it may be 10,000 miles away. It seems to us artificial to regard the act as having been done in one rather than the other place. But, in the position of having to choose on the facts of this case whether, after entering the computer in Parsipenny [New Jersey], the act of appropriation by inserting instructions on the disk occurred there or in St. Petersburg, we would opt for Parsipenny. The fact that the applicant was physically in St. Petersburg is of far less significance than the fact that he was looking at and operating on magnetic disks located in Parsipenny. The essence of what he was doing was done there. Until the instruction is recorded on the disk, there is in fact no appropriation of the rights of Bank Artha Graha
>
> …
>
> In the case of a virtually instantaneous instruction intended to take effect where the computer is situated it seems to us artificial to regard the insertion of an instruction onto the disk as having been done only at the remote place where the keyboard is situated."

134. Overall, the Defendant proposes a test for s 5 that requires 'each of the acts relied on as causing the personal injury [to have] occurred in the UK' (Skeleton, [43]). I consider that this test has no basis in the text of s 5, as properly interpreted, for the reasons I have given; the case law of the English courts; or international treaties. It appears to be modelled on the 'entire tort' doctrine in the United States, which is based on different statutory wording and legislative history. I will now turn to that.

135. Title 28 USC 1605(a)(5) (often known as the 'non-commercial tort exception' to immunity), which is part of FSIA, removes sovereign immunity in cases 'in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by *the tortious act or omission of that foreign state* …' (emphasis added).

136. As noted by Stewart J in *Heiser*, [98], most US court decisions on FSIA have taken the position that the *entire* tort (including the causative acts) must have occurred in the US for the non-commercial tort exception to immunity to apply under that Act. These cases include: *Smith v Socialist Peoples' Libyan Arab Jamahiriya* 101 F 3d 239, 246 (2nd Cir.1996) (The Lockerbie Bombing case); *Argentine Republic v Ameradi Hess Shipping Corp* 488 US 428, 421 (1989); *Persinger v Islamic Republic of Iran* 729, F 2d 835 (DC Cir); *Cabiri v Government of Republic of Ghana* 165 F 3d 193 (1999); in *Re Terrorist Attacks* 714 F 3d 109, 116 (2nd Cir 2013).

137. In the last of these cases, the US Court of Appeals for the Second Circuit summarised the 'entire tort' rule as follows:

> "As noted, the FSIA's non-commercial tort exception provides:
>
> A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case—... in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment. (28 USC § 1605(a)(5)).
>
> For this exception to apply, however, the 'entire tort' must be committed in the United States. This so-called "entire tort" rule was first articulated by the Supreme Court in *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 109 S.Ct. 683, 102 L.Ed.2d 818 (1989). In that case, the Supreme Court considered whether courts in the United States had jurisdiction over a suit brought by two Liberian corporations against the Argentine Republic to recover damages stemming from a tort allegedly committed by Argentina's armed forces on the high seas in violation of international law. *Id.* at 431, 109 S.Ct. 683. The Court held that the action was barred by the FSIA, holding that the noncommercial tort exception "covers only torts occurring within the territorial jurisdiction of the United States." *Id.* at 441, 109 S.Ct. 683.

> After *Amerada Hess Shipping Corporation* was decided, we described and explained the 'entire tort rule in *Cabiri v. Government of Ghana*, 165 F.3d 193 (2d Cir.1999), noting that "[a]lthough [the words of the statute are] cast in terms that may be read to require that only the injury rather than the tortious acts occur in the United States, the Supreme Court has held that this exception 'covers only torts occurring within the territorial jurisdiction of the United States.' " *Id.* at 200 n. 3 (quoting *Amerada Hess Shipping Corp.*, 488 U.S. at 441, 109 S.Ct. 683). At least two of our sister circuits have applied the "entire tort" rule as well. *See O'Bryan v. Holy See*, 556 F.3d 361, 382 (6th Cir.2009) ("We join the Second and D.C. Circuits in concluding that in order to apply the tortious act exception, the 'entire tort' must occur in the United States. This position finds support in the Supreme Court's decision in *Amerada Hess Shipping*...."); *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C.Cir.1984) ("Even if the [alleged tort] had the effect of retroactively rendering the prior acts on United States soil tortious, at the very least the entire tort would not have occurred here....")."

138. In light of the entire tort rule, the US Code was amended, and 28 USC 1605A inserted for terrorist attacks, in relation to which the said rule does not apply: see *Heiser*, [99]-[100].

139. Mr White placed particular weight on the decision of the US Court of Appeals for the District of Columbia in *Kidane v Ethiopia* 851 F 3d 7 (2017), whose facts were similar to the facts of the present case. In that case an Ethiopian corruption and human rights campaigner who had obtained asylum in the US claimed that he was tricked into downloading a computer program which enabled the Ethiopian government to spy on him from abroad and sought to bring a tort claim against Ethiopia in the US courts. The alleged trickery took place via the claimant in the US opening an attachment to an email he received from an acquaintance which infected his computer with a program known as FinSpy which, like Pegasus, clandestinely monitors and gathers information from electronic devices and is sold exclusively to government agencies. That program communicated with a server in Ethiopia and the text of the original email suggested that it had been sent by an individual located in London.

140. The District of Columbia Court found 28 USC 1605(a)(5)) was inapplicable (and so Ethiopia had immunity) because the entire tort did not occur in the US. It noted, by reference to *Argentine Republic v Amerada Hess Shipping Corp* 488 US 428 (1989) that the primary purpose of the Congress in enacting s 1605(a)(5), 'was to eliminate a foreign state's immunity for traffic accidents and other torts committed in the United States, for which liability is imposed under domestic tort law', and thus it was 'unsurprising' that transnational cyberespionage should lie beyond section 1605(a)(5)'s reach. In *Amerada Hess* the US Supreme Court had rejected an argument that s 1605(a)(5) could apply to a claim for injury to a ship which occurred on the high seas as the relevant tort did not occur 'in the US'.

141. The Court in *Kidane* went on to highlight that the phrase 'occurring in the United States' is no mere surplusage as '[t]he entire tort – including not only the injury but also the act precipitating that injury – must occur in the United States'. On the facts, it held:

> "… at least a portion of Ethiopia's alleged tort occurred abroad
>
> …
>
> … whether in London, Ethiopia or elsewhere, the tortious intent aimed at Kidane plainly lay abroad and the tortious acts of computer programming likewise occurred abroad. Moreover, Ethiopia's placement of the FinSpy virus on Kidane's computer, although completed in the United States when Kidane opened the infected e-mail attachment, began outside the United States. It thus cannot be said that the entire tort occurred in the United States.
>
> …
>
> Without the software's initial dispatch or an intent to spy – integral parts of the final tort which lay solely abroad – Ethiopia could not have intruded upon Kidane's seclusion under Maryland law …"

142. The tort which Mr Kidane alleged thus did not occur entirely in the United States, and so was a transnational tort over which the court lacked subject matter jurisdiction because of state immunity.

143. The Court distinguished *Letelier* on the basis that that case had involved actions 'occurring in the United States' that were tortious, without reference to any action undertaken abroad.

144. Despite the high authority of the American courts which have spoken on this issue, I remain unpersuaded that their decisions have a significant bearing on the issue I have to decide. As I have already remarked, English courts should be cautious before placing too much reliance on foreign decisions that are concerned with different legislation which has different wording and a different legislative history, as the FSIA does when compared with the SIA 1978. The decision in *Kidane* was further complicated by issues of Maryland state law. The following points strike me in particular as to why comparative and international materials do not offer much assistance on the present issue.

145. Firstly, differences exist among foreign States as to how and to what extent the territorial connection is established for the purpose of the exception to state immunity. As Yang observed in *State Immunity in International Law* (2012), 'the formulations of this requirement are as many as the instruments' (p216).

146. Second, it seems to me that the wording of the US provision ('*the* tortious act or omission of that foreign state') is critically different to s 5 of the SIA 1978, with its reference to '*an* act or omission in the United Kingdom' (emphasis added). As I have already indicated, the fact that Parliament specified only 'an act' suggests that not *every* wrongful act has to occur in the UK. By contrast, the use of the definite article conjoined to the word 'tortious' in the FSIA is a pointer to the conclusion that the

entirety of the tortious activity is governed by the territorial jurisdictional requirement (as the US courts have consistently held). Moreover, as set out above, English courts have accepted that s 5 may apply where only some acts occur in the UK.

147. Third, it is clear from the decision *In the Matter of the Complaint of Sedco Inc* 543 F Supp 561 (SD Tex, 1982), an early authority on the 'entire tort' theory under the FSIA, that this approach was based in large part on the specific legislative history of that legislation in the US:

> "Plaintiffs argue the tort may occur, in whole or in part, in the United States, and that the tort occurs in the United States if the acts or omissions directly affect this country. This argument may be correct in other circumstances, see *Ohio v. Wyandotte Chemicals Corp*., 401 U.S. 493, 91 S.Ct. 1005, 28 L.Ed.2d 258 (1971); however, legislative history appears to reject this theory with respect to the FSIA. In describing the purpose of § 1605(a)(5), the House Committee Report accompanying the House Bill, which ultimately became the FSIA, states:
>
> > 'It denies immunity as to claims for personal injury or death, or for damage to or loss of property caused by the tortious act or omission of a foreign state or its officials or employees, acting within the scope of their authority; the tortious act or omission must occur within the jurisdiction of the United States …
>
> House Report, supra at 6619 (emphasis added). The primary purpose of this exception is to cover the problem of traffic accidents by embassy and governmental officials in this country. Id."

148. There are statements to similar effect in later US cases on the entire tort doctrine: *Asociacion de Reclamantes v United Mexican States* 735 F.2d 1517 (DC Cir 1984) and *Jerez v Cuba* 775 F.3d 419 (DC Cir 2014), itself cited in *Kidane*, on which the Defendant relies. I agree with the Claimant's submissions that those circumstances particular to the FSIA are inapplicable to the SIA 1978.

149. In common with its submissions on the sovereign/private act issue (see above), the Defendant also seeks to place reliance on Parliamentary statements made during the passage of the State Immunity Bill (see Skeleton, [35] and [37]). I again consider the Defendant's submissions to be contrary to the principles in *Pepper v Hart* since the meaning of s 5 is clear. Further, the Parliamentary statements relied upon by the Defendant would not 'almost certainly settle the matter immediately one way or the other', which is one of the well-known *Pepper v Hart* requirements. So, the Parliamentary statement of Lord Wilberforce relied on by the Defendant at [35] of its Skeleton Argument ('… Lord Wilberforce described the mechanism of s 5 in relation to composite acts as 'unscientific' because it 'talks about an act or omission in the United Kingdom, whereas a great many acts or omissions are composite and sometimes occur partly inside and partly outside'. He stated: 'I have not sought to clarify or clear that because it would involve too radical a reconstruction'' …) is, to my mind, inconclusive on this point. Furthermore, the Defendant's reliance on it also contravenes

the third principle in *Pepper v Hart* since they were not the words of 'the Minister or other promoter of the Bill'.

150. The Defendant also seeks to support its adoption of an entire tort test by reference to scholarship and in particular to Dickinson, Lindsay and Loonam, *State Immunity: Selected Materials and Commentary*, 2004: OUP, pp. 369-370. (Skeleton, [34]). But I accept the Claimant's submission that Dickinson et al's comment at p370 that, 'if a claimant alleges a single legal wrong comprising more than one act or omission on the part of the state, each act or omission must have occurred while the actor was in the United Kingdom' was made was made in tentative and provisional terms and there is little by way of analysis.

151. I therefore find for the Claimant on this issue.

(c) Does the claim fail to meet the requirements of s 5 because there is insufficient evidence of the Defendant's responsibility for the persons responsible for the alleged spyware ?

152. The Claimant accepts, for present purposes, that the test to be applied to this aspect of the Defendant's application, at this *inter partes* stage, is whether, on the balance of probabilities, the claim falls within the exception in s 5 of the SIA 1978, in accordance with the approach adopted by the Court of Appeal in *Al-Adsani (No 2),* p545. However, he reserved the right to argue on any appeal that the approach to this issue taken in *Al-Adsani (No 2)* is incorrect. However, the Claimant submits that the evidence in this case amply meets that threshold in any event.

153. There is authority binding upon me, to which I have referred at the outset, which makes clear that I have to be satisfied on a balance of probabilities that an exception applies. The burden is on the Claimant. If I cannot decide the issue on the materials before me, then I can order a trial of the issue.

154. The Claimant has served expert evidence from Dr Marczak in support of his claim that his iPhones were hacked by spyware by the Defendant.

155. At [46] to [52] of its Skeleton, the Defendant argues that the Claimant's evidence is not capable of establishing on the balance of probabilities that his alleged personal injury arising from the spyware claim is properly attributable to the Defendant. However, the Defendant has not served any direct evidence in response to the Defendant's expert evidence. It relies on points made by its solicitor Ms Given in her first witness statement of 5 February 2021. It also makes a number of forensic technical points at [58] of its Skeleton Argument.

156. The reasons the Claimant says that the evidence shows that it was the Defendant who carried out the spyware attack on him, in summary, are: (a) the Defendant's history of using spyware products, including Pegasus; (b) the Claimant's profile and activities, and the targeting of him by the Defendant by means other than the Pegasus infection; and (c) the characteristics of the malicious text messages received by the Claimant.

157. Dr Bill Marczak is a Postdoctoral Researcher in Computer Science at the University of California, Berkeley (from where he holds a PhD). He is also a Research Scientist at the International Computer Science Institute (an independent not-for-profit research

organisation based at Berkeley), and he also works at Citizen Lab (CL), an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy at the University of Toronto. CL focusses on research and development at the intersection of information and communication technologies, human rights, and global security.

158. Both Dr Marczak and CL have extensive knowledge of, and expertise in, the field of cybersecurity in general, and in nation-state targeted digital attacks against dissidents and civil society groups in particular. In Marczak 1 at [4]-[5] he said:

> "4. At CL, I conduct research into nation-state use of spyware and hacking tools to conduct espionage against journalists, dissidents, and civil society targets. Spyware refers to any software or hardware component that is installed on a target's electronic device, without their consent, to facilitate third-party access to data stored on the device, or to the device's functions (e.g., turning on the device's microphone to record audio in the device's vicinity). I focus on companies that sell spyware and hacking tools and services directly and exclusively to governments, including FinFisher (based in Germany), Hacking Team (based in Italy), and Cyberbit and NSO Group (both based in Israel). These companies typically represent that their spyware products are intended to be used by governments for tracking serious organized crime or terrorists
>
> 5. These spyware tools, including NSO Group's Pegasus spyware, have a broadly similar method of facilitating government access to a target's devices, according to leaked documentation, as well as my own research. Once the operator implants the spyware on a device, the spyware causes the device to periodically contact Internet "Command and Control" ("C&C") servers included in the spyware's code. The purpose of this contact is for the spyware to receive commands from the operator (typically, a government agency), and to transmit any data captured from the device back to the operators."

159. Dr Marczak is sure there was spyware on the Claimant's phone, for the reasons he sets out in his witness statements.

160. Dr Marczak's qualifications and expertise are impeccable. In my judgment, his evidence demonstrates to the requisite standard that the Claimant's iPhones were infected with spyware, and that the Defendant and/or those for whom it was vicariously liable, were responsible.

161. In saying this, I acknowledge the points made by Ms Given on behalf of the Defendant, and the points made in its Skeleton Argument. However, with all due respect to her, she is not a computer scientist (as far as I know) and, at this stage at least, I am satisfied that Dr Marczak's evidence shows that: (a) there was a spyware attack on the Claimant's iPhones; and (b) there is good evidence that the Defendant was responsible,

and that this discharges the burden lying upon the Claimant on this aspect of the Defendant's application.

162. It should be said at once that much of Dr Marczak's evidence is very technical in nature. He uses terms such as 'command and control servers'; 'proxy servers'; 'zero-day exploits'; 'enhanced social engineering messages'; as well as many other technical terms. His statements need to be read in full for all of the detail, and it is not feasible to reproduce every aspect of his evidence here. I rely on everything which he says, whether or not it is mentioned in this section of my judgment.

163. Dr Marczak's central point is that he is satisfied that the Claimant's iPhones were infected by spyware sent by or on behalf of the Defendant, and that this spyware allowed the Defendant to monitor everything that was done on the Claimant's iPhones by way of internet and social media communications, and enabled the Defendant to manipulate them so that they operated as monitoring and listening devices. In the absence of any countervailing expert evidence on behalf of the Defendant, as I have said, I accept Dr Marczak's evidence in full.

The Defendant's history of using spyware products, including Pegasus

164. Between around 2012 and 2015 three of the Defendant's agencies used spyware produced by the 'Hacking Team', which is (or was) a commercial spyware company based in Italy. Further, in 2014 and 2015 various servers were found to be running software produced by FinFisher GmbH and/or the Gamma Group (other spyware companies) from within Saudi Arabia, which it can be inferred were used by the Defendant (see POC at [30-31]).

165. Furthermore, and perhaps more pertinently, it appears from Dr Marczak's evidence that the Defendant has used Pegasus against other individuals, in circumstances which (at least arguably) bear similarities to the conduct which the Claimant complains about, and which therefore indicates a propensity by the Defendant to engage in such activities.

166. Dr Marczak says this at [4]-[7] of Marczak 2 (which was primarily a response to points made on behalf of the Defendant in response to Marczak 1):

> "4. Having considered the points made by Ms Given, my conclusions on these matters, as expressed in my first witness statement, remain the same. I first provide a brief explanation of my conclusions, and then explore specific points raised by Ms Given.
>
> 5. I conclude with high confidence that a group of servers active in 2017 and 2018 that I referred to as KINGDOM in my first witness statement is linked to the Government of Saudi Arabia for the following summary reasons (developed further below):
>
> a. NSO Group only sells its Pegasus spyware to governments [BM2/1];

b. KINGDOM is linked to NSO Group's Pegasus spyware (paragraphs 15-19 of my first witness statement), and is likely to represent a single operator of NSO Group's Pegasus spyware (paragraphs 26-27 of my first witness statement);

c. the text messages that Mr al-Masarir received on his two phones in June 2018 contain links to the KINGDOM servers (paragraphs 33-34 of my first witness statement);

d. the Government of Saudi Arabia reportedly signed a deal to acquire Pegasus from NSO Group in the summer of 2017, and NSO Group's CEO appeared to tacitly acknowledge Saudi Arabia as a customer in October of 2018; and

e. the six publicly described KINGDOM targets, including Mr al-Masarir, show a clear nexus with Saudi Arabia; and no other Pegasus operator active during June 2018 showed a nexus with Saudi Arabia. This conclusion is consistent with my subsequent statement that I had a medium level of confidence that another group of servers active in 2019 and 2020 (which I referred to as MONARCHY) is linked to the Government of Saudi Arabia. In contrast to KINGDOM's six targets with a clear Saudi Arabian nexus, only two MONARCHY targets have been publicly described, and of these two targets, only one shows a clear nexus with Saudi Arabia.

6. I also conclude that the available technical evidence is consistent with the Pegasus spyware having been installed on Mr al-Masarir's two iPhones for the following outline reasons (some of which are explained in further detail below):

a. As stated in my first witness statement, I observed that both phones had received text messages with links corresponding to websites associated with the KINGDOM and the installation of Pegasus malware. One such message on each of Mr al-Masarir's phones was indicated as having been read.

b. I also observed that neither of Mr al-Masarir's phones were able to update the software for their operating systems. Disabling a phone's software update mechanism for its operating system is a known behavior of some versions of NSO Group's Pegasus spyware. In a 2016 version of NSO Group's Pegasus spyware analyzed by CL

> and Lookout, the phone's update mechanism was disabled only after the final stage of the spyware (Stage 3) had been successfully downloaded.
>
> c. While the operating systems of Mr al-Masarir's phones were slightly out of date when they received the SMS messages, this does not of itself indicate that the phones' update mechanisms had been disabled before receipt of the SMS messages. Updates may be deferred for various reasons (as discussed below)."

167. Dr Marczak's evidence about KINGDOM in Marczak 1 was this (at [27]):

> "I identified one group of servers indicated by Athena (which I believe was a single government agency operating Pegasus) that I called "KINGDOM", which I concluded with high confidence was linked to Saudi Arabia …"

168. The individuals referred to above at [5(e)] are Yahya Assiri (a former member of the Royal Saudi Air Force and Saudi human rights defender based in London), Omar Abdulaziz (a Saudi human rights defender based in Canada who is a prominent opponent of the government in Saudi Arabia), Ben Hubbard (the Bureau Chief of the New York Times who was writing a book about the rise to power of Saudi Crown Prince Mohammed bin Salman), a Saudi activist, and an Amnesty International employee working on issues relating to human rights issues in Saudi Arabia: see POC, [46]-[58] and Marczak 2, [10]. In that paragraph, Dr Marczak said this:

> "10. As of the date of this statement, CL and Amnesty International have publicly characterized six targets of KINGDOM: Ghanem al-Masarir, Omar Abdulaziz, Yahya Assiri, Ben Hubbard, a Saudi activist later targeted by MONARCHY, and an employee of Amnesty International. Mr Hubbard and the Saudi activist later targeted by MONARCHY had not been publicly described as Pegasus targets as of the date of my first witness statement. All six targets have clear links to Saudi Arabia. Mr al-Masarir has posted popular YouTube videos in which he criticized Saudi Arabia's royal family; Mr Abdulaziz hosted a popular satirical news show on YouTube and was a close associate of Saudi journalist Jamal Khashoggi; Mr Assiri is a former member of the Royal Saudi Air Force and the founder of ALQST, a London-based organization that advocates for human rights in Saudi Arabia; Mr Hubbard is the Beirut Bureau Chief of the New York Times, and was writing a book about the rise to power of Saudi Crown Prince Mohammed bin Salman while he was targeted (the text message containing the Pegasus link sent to Mr Hubbard said in translation: "Ben Hubbard and the story of the Saudi Royal Family"); the Amnesty employee was targeted with Pegasus via a text message that began (in translation): "Is it

possible for you to cover [a demonstration] for your brothers detained in Saudi Arabia in front of the Saudi Embassy in Washington [DC]?"

169. The principal response made by the Defendant to this evidence is set out in [46]-[52] of its Skeleton Argument:

> "46. For the reasons set out in the First Witness Statement of Davina Given ("DFG1") **…** the Defendant submits that the Claimant's case as to the alleged infiltrations being carried out by the Defendant and / or its employees, officials and / or agents acting on its behalf is entirely circumstantial. The Claimant has not established that the Pegasus operator designated by Citizen Lab as 'Kingdom' is a person or persons for whom the Defendant has vicarious liability.
>
> 47. First, the Claimant relies upon the fact that the text messages sent to his phone contained links corresponding to websites which have been identified by Citizen Lab as being used previously by 'Kingdom', a name allocated by Citizen Lab to what it hypothesises is a single operator of Pegasus **[21/474]** at [13]. However, it is unknown whether such websites are part of a bank of websites which might also have been used by other Pegasus operators.
>
> 48. Second, the Claimant relies on the use of domain names by the Pegasus operator in the text messages sent to him which have a theme related to an Arab Kingdom – 'kingdom-deals.com, kingdomnews.com, Mideast-today.com, muslim-world.info, akhbar-arabia.com, arabnews365.com **[21/472]** at [27]. But there are 8 Arab monarchies in the Middle East (Morocco, Jordan, Saudi Arabia, Kuwait, Bahrain, Qatar, Oman and the UAE). The domain names used are not specific to the Defendant, and do not advance the Claimant's case in this regard.
>
> 49. Third, the Claimant notes that the 'Kingdom' Pegasus operator is alleged to have targeted six persons with "clear links" to the Defendant **[5/113-114]** at [10]. However, two of these persons could be said to have links with other countries. One is a New York Times journalist focussing on the Middle East, and one is an unnamed Amnesty International employee about whom no other information is known **[5/168-170]**. Further, the evidence does not disclose whether the alleged infection of the "*unnamed Saudi activist later targeted by Monarchy*" related to the same version of Pegasus which was allegedly used to target the Claimant or whether that individual was allegedly targeted by an earlier iteration of Pegasus prior to the release of iOS 9.3.5 on 25 August 2016 **[3/35]**, **[3/41]**.

> 50. Fourth, the Claimant has himself alerted this Court to the possibility that one of the Pegasus operators that Citizen Lab has considered to be associated with the Defendant could be linked to an externally focussed security agency of the UAE **[3/36]**.
>
> 51. Fifth, in a Forbes article relied upon by the Claimant is it stated *(sic)* that there is "no clear evidence Saudi Arabian regime hackers are behind the spate of Pegasus attacks" **[21/690]**.
>
> 52. In short, the Claimant's evidence is not capable of establishing on the balance of probabilities that his alleged personal injury arising from the spyware Claims is properly attributable to the Defendant: compare *Al-Adsani v Government of Kuwait* (1996) 107 ILR 536 at 545, 551; *Al-Adsani v Government of Kuwait*, QBD, 3 May 1995 (Unreported) per Mantell J at 10."

170. These may be sound forensic points, and should there be a trial they can be made then, but at this stage they do not dissuade me from concluding that the Claimant has discharged the burden upon him, and especially since Dr Marczak specifically considered them and answered them in Marczak 2.

171. In other words, in light of the evidence advanced by the Claimant, and the relatively modest response by the Defendant, I think it overwhelmingly likely that there is a proper basis for concluding that the Defendant used Pegasus during the relevant period, and that it did so against individuals located outside Saudi Arabia involved in or working on matters of particular interest to the Defendant, in a manner which closely resembles the conduct sued on in this claim.

The Claimant's profile and activities, and his targeting by the Defendant by means other than the Pegasus infection

172. The evidence demonstrates to me that the only state which might have had any interest in hacking the Claimant's devices is the Defendant. I acknowledge the points made on its behalf, but it seems to me there is no other viable candidate than Saudi Arabia. If one asks the question which the great Roman judge Lucius Cassius would often ask (as quoted by Cicero), 'Cui bono fuisset ?' ('Who benefits ?'), then the answer is obvious.

173. There is, moreover, evidence that the Claimant was subject to various forms of online targeting not sued on in the claim which are attributable, either directly or as a matter of inference, to the Defendant, and which is consistent with the pattern of conduct which does form part of this claim.

174. I refer, here, to the Claimant's Skeleton Argument at [80]-[82]:

> "80. The evidence also demonstrates that the only state body which might have had any interest in hacking the Claimant's devices is the Defendant. Not only is the evidence on this point (again) undisputed by the Defendant, but the Defendant also fails to identify any other state body which might conceivably have been motivated to undertake that hack. There is moreover

> undisputed evidence that the Claimant was subject to various forms of online targeting not sued on in the claim which are attributable, either directly or as a matter of inference, to the Defendant, and which is consistent with the pattern of conduct which does form part of the claim.
>
> 81. In this context, it is not in dispute that the Claimant has a prominent profile as a critic of the Saudi royal family, resulting primarily from the videos posted to his Ghanem Tube and Ghanem Show YouTube channels. Those videos, many of which satirise the Saudi royal family and expose corruption within the country, are hugely popular, with the Ghanem Channel, for example, having garnered about 230,000,000 views, mostly by internet users within Saudi Arabia. These activities have resulted in (baseless) copyright complaints by the Saudi Broadcasting Corporation which have occasioned the removal from the Internet of the Claimant's material which is critical of the Saudi royal family …
>
> 82. In consequence of his online activities, the Claimant has also been subject to various other forms of online targeting. This has included a concerted mass "*spamming*" of the Claimant's Twitter account; the hacking of his Facebook account (such that his access to the account was reinstated only after Newsweek published an article entitled "Saudi Arabia's government might be getting help from social media giants to shut down dissent" on 22 December 2017); the hacking of his personal website (as a result of which photographs and messages relating to the Saudi royal family were added to his home page); and the transmission of a large number of threatening messages, comments and videos in Arabic to his YouTube channel and mobile telephone. This activity is consistent with the well-attested use by the Defendant, and its Center for Studies and Media Affairs in the Royal Court, of such online techniques for intimidation. See POC, paras 14-16 and 18 and 65 and 67 … "The CIA Sent Warnings to at Least 3 Khashoggi Associates About New Threats from Saudi Arabia", Time Magazine, 9 May 2019 **….** Again, these various allegations are not challenged by the Defendant."

The characteristics of the malicious text messages received by the Claimant

175. Pegasus spyware can be implanted on a device by various means including by the user of the device clicking on a link in a malicious text message formulated so as to provoke the user's specific interest. Once implanted and installed on the device, the spyware works by causing the device to communicate with a command and control (C&C) server operated by a Pegasus customer (eg, the foreign state which purchased it) so as to receive commands from, and transmit data to, the customer. Such communications are usually conducted via intermediate proxy servers so that it is not possible, by examining the spyware code, to identify the internet address associated with the C&C server (and thereby to ascertain the identity or location of that server and the customer). Marczak 1, [4]-[8].

176. Dr Marczak first publicly linked a case of spyware installation attributable to NSO by examining the behaviour of a device on clicking on a link in a malicious text message which had been sent to Ahmed Mansour, a human rights activist from the UAE. As a result of that examination, Dr Marczak was able to establish that the information received by the device when that malicious link was clicked on had certain 'fingerprints' which were also evident in responses communicated from a series of other IP addresses. Some of those IP addresses pointed to domain names registered to NSO. Dr Marzcak concluded that the set of servers linked to those IP addresses was associated with Pegasus: Marczak 1, [9]-[19].

177. By a means of a technique called DNS Cache Probing, Dr Marczak was able to search for other devices which had repeatedly looked up Pegasus C&C Servers and which had therefore probably been infected with the Pegasus spyware. This enabled Dr Marczak to identify that a device which belonged to Mr Abdulaziz had been infected in this way: Marczak 1, [20]-[24].

178. Dr Marczak then divided up the servers associated with Pegasus into 36 groups (which he terms 'operators'), with each group/operator representing proxy servers which communicated with a single Pegasus C&C server. By examining the traits of each group of servers/operator, Dr Marczak was able to identify that some of them were linked to a particular country. This identification was made by reference to: (a) the domain names relating to a particular operator; (b) the identities of targets who had received malicious text messages containing links to domain names relating to a particular operator; (c) country themes suggested by those domain names (eg where they impersonated websites relating to a particular country); and (d) DNS cache probing results showing the countries on which the operator was probably spying. See Marczak 1, [25]-[26].

179. Dr Marczak identified one operator which he concluded with high confidence was linked to Saudi Arabia, namely KINGDOM). He explains that the basis for this conclusion was that (a) this was the only operator whose domain names showed likely infections in Saudi Arabia based on Dr Marczak's DNS Cache Probing results; (b) Kingdom servers were associated with malicious text messages identified (at that stage) as having been sent to three targets associated with Saudi Arabia: Mr Assiri, Mr Abdulaziz and the Amnesty International researcher working on Saudi Arabia issues; and (c) the domain names employed by Kingdom included names thematically indicative of an Arab kingdom: Marczak 1, [27].

180. Furthermore, Dr Marczak is not aware of any additional targets of KINGDOM that are not clearly linked to Saudi Arabia, and he is also unaware of any individuals clearly linked to Saudi Arabia who were targeted in 2017 or 2018 by a Pegasus operator other than KINGDOM: Marczak 2, [11].

181. On 6 November 2018 Dr Marczak was contacted by Thomas Fox Brewster, a journalist at Forbes magazine, who alerted him to the Claimant's case. The following day Mr Brewster sent Dr Marczak a photograph of a text message on the Claimant's device containing a link to a website (sunday-deals.com) which was one of those Mr Marczak had previously identified as associated with KINGDOM: Marczak 1, [28]-[29].

182. On 16 December 2018 (after Mr Brewster had published an article about the Claimant's case in Forbes), Dr Marczak examined two of the Claimant's iPhones. He identified several

pieces of evidence which indicated that both devices had been subject to Pegasus infection by the KINGDOM operator.

183. Dr Marczak contrasts the 'high' confidence with which he attributes the KINGDOM operator to the Defendant with the 'medium' confidence with which he attributes a different operator, named MONARCHY, to the Defendant. This difference arises out of the fact that, based on its targets (of which Dr Marczak was able to identify only two in contrast to the six linked to the KINGDOM operator) and its method of operation, it is plausible that MONARCHY could be attributed to the UAE. By contrast, Dr Marczak does not believe that there is any plausible explanation other than that KINGDOM is linked to Saudi Arabia: Marczak 2, [12]-[17] .

184. Save in respect of a few narrow points, I do not think that the Defendant has mounted any significant challenge to Dr Marzcak's evidence. It makes the point that, 'it is unknown whether [the websites which have been identified by Citizen Lab as being used previously by 'Kingdom'] are part of a bank of websites which might also have been used by other Pegasus operators (Skeleton, [47]). I think that this point is, at this stage, speculative. Dr Marczak says at [25]-[27] of Marczak 1, that the KINGDOM operator (by which the alleged infection Claimant's hack was conducted) was formed part of a group of Pegasus proxy servers which communicated with a single C&C server. He has concluded that that operator was identified as uniquely linked to Saudi Arabia.

Conclusion

185. In light of the Claimant's evidence, and the Defendant's failure to respond in any persuasive way to it, I am satisfied that the Claimant prevails on the third issue.

(iv) Does the claim fail to meet the requirements of s 5 because there is insufficient evidence of the Defendant's responsibility for the persons responsible for the assault on the Claimant?

186. This issue concerns the alleged assault of the Claimant by two men. It is pleaded in the POC at [64] that he was assaulted in Knightsbridge on 31 August 2018 by unknown men. His case is that those responsible were working for or on behalf of the Defendant. These matters are said to have contributed to the Claimant's personal injuries. If, on a balance of probabilities the Defendant is responsible, then for the reasons given in relation to issue (a), the assault falls within s 5 notwithstanding it may be said to have been of a sovereign nature (an attack on a political dissident).

187. Again, the issue is whether I can be sure on a balance of probabilities that the Claimant's assertion of responsibility on the part of the KSA is right.

188. The Claimant's main evidence about this in his first witness statement at [6]-[11] is as follows:

> "6. I believe that the individuals who attacked me were acting on behalf of the Saudi government. The attack took place at about 6pm after I had met a new acquaintance of mine for coffee at a café. We left the café and continued our conversation as we walked. We did not realise that we were being followed by 2 men. They came up from behind us and one of them shouted at me

asking me who was I to talk about the family of al-Saud. I had not been speaking about the Al Saud royal family or the Saudi government at all, and it was clear to me that the men recognised me.

7. One of the men punched me in the face and continued to physically attack me. I tried to get away from the men. Both men followed me. The man who had not punched me was wearing a grey suit and a wire, either from headphones or from a headpiece. Passers-by intervened and attempted to restrain the second man preventing him from attacking me. During the assault, the men were calling me a "slave of Qatar" and said that they were going to teach me a lesson. If it were not for the people restraining the men, I know my injuries would have been a lot more serious. I remember the punches being very vicious and with intent.

8. After the attack I was sitting by a wall waiting for the ambulance and the police to arrive. The ambulance crew arrived first to tend to my injuries. When I was being seen to in the back of the ambulance my acquaintance was standing by outside. A man approached my acquaintance. He told him that he was a Saudi businessman, that he was an importer of rice in the UK and that he had seen what had been going on (meaning my attack) and it was in my acquaintance's interest to not get involved. He told my acquaintance, "Don't associate yourself with this son of a bitch!". He then warned him that "The police will not come for Ghanem, we are in charge here, we run the police and they will not come." My acquaintance told me everything when the man left. He also stated this exchange to the police in his statement to them.

9. I waited with the ambulance crew for the police to arrive for over 2 hours. The ambulance crew did not leave me, they contacted the police twice while we waited. The crew thought that it would be unsafe to leave me in the street to wait for the police to arrive. After this time the ambulance crew offered to drop me off at Notting Hill Gate police station. When I arrived at the station I was advised by the police officer at the desk to go home and that an officer would come to my home to take a statement from me. After what had happened and the warning that I had received via my acquaintance I was scared to go home. I decided to wait at the police station. I did not leave until after midnight.

10. Once my statement was taken, I was advised that an officer would be in contact. After a few weeks, I was contacted by a police officer from Kensington police station. I was invited in for an interview and again someone took down my statement, they also had an officer draw out profiles of my attackers from the video footage taken from attack. Bystanders had filmed the attack. I do not recall hearing anything further from Kensington

> or Notting Hill Gate police stations for some time after this. Before the end of the year, I was contacted by Kensington police station and informed that they would be closing my investigation. No one was arrested or charged in relation to the assault. I had done nothing to provoke the attack.
>
> 11. I do not accept Ms Given's statement [the solicitor for the Defendant] that the individuals acted independently. I believe they were acting on behalf of the Defendant. On reflection I believe I was under surveillance and had someone not restrained the attackers I would have ended up far more seriously injured if not killed. The Saudi government have a history of using people to act on their behalf covertly, and do not admit responsibility for such individuals."

189. I have watched and rewatched the video put in evidence by Ms Given on behalf of the Defendant (Ex DFG2/4). This is a spliced together montage of different clips. In brief, it shows two men, a larger man in a suit, and the Claimant, who is more diminutive, involved in a verbal altercation with two other men, one of whom is in a suit, and the other of whom is casually dressed and carrying a shopping bag. They are across the road from Harrods. The larger man is apparently attempting to shield the Claimant from the other two men by standing between him and them as they argue. There is arguing and then pushing and shoving and eventually punches are thrown and there is scuffling which goes into the road. It appears that third parties then intervene to break up the fight. Bystanders can be seen recording events on their phones. I am bound to say that: (a) I cannot readily see a wire being worn by anyone; and (b) the Claimant was not entirely passive, but takes an active part in what occurred.

190. In its submission in respect of this altercation, the Defendant alleges that the Claimant 'has no evidence beyond his mere assertion to that effect that the assault was committed by the Defendant's employees, officials and/or agents acting on its behalf' (Skeleton, [53]).

191. Circumstantial though the Claimant's case is, I am satisfied to the requisite standard at this stage that he has made out his case. That is because: (a) I am satisfied the altercation had a political component based on what the Claimant says was said, which at this stage I cannot discount; (b) he had at that stage already been targeted via spyware, in the way I have already described, and I am satisfied on a balance of probabilities that this was at the hands of Saudi Arabia; (c) of the timing of the altercation (which took place between the infection of his phone in June 2018 and his discovery of it in November 2018); (d) it can thus be inferred he may well have been put under surveillance (including by having his conversations monitored through his iPhones), as opposed to this being a random attack; (e) of the apparently unprovoked altercation; (f) the Claimant says that one of the men involved was wearing a wired ear-piece (as I have said, I cannot see this, but the footage is not wholly clear); (g) he had not, contrary to the threats made by the attackers, been discussing the Saudi royal family or government at all prior to being attacked: see [6] of Al-Masarir 1.

192. I also take into account what he says was said at the scene, namely, 'The police will not come for Ghanem, we are in charge here, we run the police and they will not come':

Al-Masarir 1, [8]. I reject any suggestion that the British police are somehow in the pay of the Saudis, but I think it a reasonable inference that if this was said (which I am satisfied to the requisite standard it was – I certainly cannot discount at this stage that it was), it can be inferred that the attack was connected to influential or powerful entities.

193. The broader context is that the Defendant is known to target dissidents and to use violence against them. The murder of the journalist Jamal Khashoggi is a case in point: see eg AP1/8 (Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi); and see also AP1/9 (Extract from *Vanity Fair*, 'No-one is safe: How Saudi Arabia makes dissidents disappear').

194. Although I consider the Claimant has probably over-egged what happened (for example, I do not think that 'vicious punches' really represents what occurred) I find that the Claimant's assertion as to who was responsible has not been challenged to any persuasive degree. In Given 1, Ms Given said at [33]-[34]:

> "33.The Defendant is aware that the Claimant was struck in a scuffle with two young men in August 2018 in London. The Defendant learned of this incident when the young men went to the Defendant's Embassy in London and explained what had happened after the event.
>
> 34. Although they were of Saudi nationality, the Defendant's Embassy in London has confirmed that the young men who struck the Claimant were not, and are not, agents of the Defendant and did not act directly or indirectly at the behest of the Defendant. When the young men attended the Embassy after the incident they explained to consular officials that they were, at the time, students in the UK attending a careers fair in London, who, by chance, overheard derogatory comments made by the Claimant in the street about the Defendant and its monarchy and took issue with them. They acted independently as private individuals out of their own sense of patriotism and the Defendant had no knowledge of their actions until after the event, when the young men voluntarily informed the Defendant's Embassy in London of what had happened."

195. There are shades of Mandy Rice-Davies in this explanation - 'They would say that, wouldn't they ?'. But there are further reasons why I do not regard either this, or what Ms Given said in Given 2, as sufficient to resolve the issue in the Defendant's favour at this stage.

196. In Given 2, Ms Given says at [9]-[10] that it was the mother of the two individuals who appealed for help from the Saudi Embassy, and by implication it was she and not them who first alerted the Embassy:

> "9. … I understand that it was this after-the-event publicity which prompted the mother of the relevant individuals to appeal for help

> from the Royal Embassy of Saudi Arabia in London (the Embassy) in 2018. She was angry because, in her view, the Claimant had provoked her sons and was wrongly using the incident to attack the Government of Saudi Arabia. I believe that it is not uncommon for the Embassy to assist Saudi citizens with miscellaneous legal matters arising in England and my firm has previous experience of supporting the Embassy in doing so.
>
> 10. In any event, on or around Friday 7 September 2018, the Embassy contacted me after receiving the mother's appeal. I met the individuals and their mother at the Embassy on Monday 10 September 2018; I have confirmed the date of this meeting from my firm's records. For the avoidance of doubt, I am not authorised to waive legal professional privilege or any immunity over any of the substantive communications involved …"

197. Without in any way casting any aspersions towards Ms Given personally, who is a well-known and well-regarded solicitor, there are, it seems to me, a number of problems and questions arising from the accounts she has been given.

198. Firstly, the two accounts Ms Given received from the Embassy seem to be different and contradictory, and I see the force of the Claimant's criticisms on this issue, in as much as in Given 1 at [33]-[34], it is said that the Defendant learned of this incident when the two men went to the Defendant's Embassy in London and explained to officials what had happened after the event. By contrast, in Given 2, [8]-[10], it was said that it was after-the-event publicity about the attack which prompted the *mother* of the relevant individuals to appeal for help from the Embassy, and that it was following the mother's approach that Ms Given was contacted, leading to the meeting between the various persons.

199. On the second account, therefore, it seems the Defendant learnt of the altercation before the men went to the Embassy (from their mother) and that the men then went on to speak to Ms Given rather than consular officials. There may be an explanation for all of this, but on its face it is striking that Ms Given was apparently not told of the mother's involvement until some time later. Given 1 is dated 5 February 2021. Given 2 is dated 16 April 2021.

200. Next, I am not wholly sure what 'help' the mother was seeking or expecting. Nor am I clear why these grown adult men needed to rely on their mother. Whatever the men heard, it was part of a private conversation between the Claimant and his friend, and so to say the men were 'provoked' seems to me to be far-fetched. There was no question of them requiring consular assistance, as all foreign detained people are entitled to under the Vienna Convention on Consular Relations 1963, as they had not been arrested nor were they likely to be (and so far as I know, were not). I am also not entirely sure what the mother feared the Claimant's dissident voice – or his statements about the attack referred to in Given 2 at [9] - could do to Saudi Arabia. Those who come to this country, on whatever basis, need to realise that here, there is a long and rich history of freedom of speech, especially when uttered privately.

201. Further, the Defendant has chosen to rely on a hearsay account from an unnamed Embassy source or sources. There are no first-hand accounts from the men involved

explaining either who they are, what they did, or why – for example, what exactly it was they heard the Claimant say which caused them such offence that it led to what happened. Because Ms Given met the men, there is no good reason I can think of why they, or their mother, could not have given statements. I will deal with privilege and immunity in a moment. But it follows that there is no explanation how they just happened to have overheard comments made by the Claimant in the course of a private conversation in a café or on a busy London street, who just happened to be a Saudi dissident and refugee. That the men could have done so just by chance is, *prima facie*, implausible. The video shows buses and much traffic going by, which it seems to me would have drowned out a private conversation, unless the men were intent on listening in and had the means to do so. On the other hand, if the Claimant's phone was being covertly monitored (which I have found it was), then it *is* plausible that they could have heard via that source and were acting on behalf of the Defendant when they confronted the Claimant and his larger friend in the suit.

202. I do not accept that there is any clear reason related to immunity or privilege that could properly operate to justify the absence of any direct evidence from the men involved. I quite accept that because Ms Given's client is the Defendant, any communications between her and Embassy officials would likely be covered by legal professional privilege. However, given on its own case the two men were nothing to do with the Defendant, it is hard to see how any privilege could arise in relation to them. They were private citizens acting as such. I recognise, of course, common interest privilege, but that has not been asserted (or not in terms, at any rate). For the same reasons, I do not readily see how any statements from them or their mother could have involved a waiver of immunity, any more than the statements from Ms Given relaying what she was told by the Embassy.

203. I do note the inconclusive finding of FtT Judge Eldridge of 25 October 2018 on the Claimant's asylum appeal ('I accept that he was so attacked but on the limited evidence available to me I cannot find whether this was at the direct behest of the Saudi government or merely by private individuals acting as such.') However, the position has moved on since then, because as at the date of that decision the spyware attack had not yet been discovered. That is potentially inter-linked to the physical attack, for the reasons I have given. It is also for me to make my own evaluation.

204. Overall, I conclude this issue in the Claimant's favour. Should there be a trial, then after proper disclosure and cross-examination the position might alter, but at this stage, circumstantial though the Claimant's case is, I am satisfied he has discharged the burden upon him.

(e) Does the evidence relied upon by the Claimant provide a coherent or realistic basis for his to advance his pleaded case such that the Court should stop the proceedings in any event ?

205. I can deal with this issue much more briefly. The conclusion largely follows from my earlier conclusions.

206. The Defendant contends under this head that the Claimant's case is of such a weak and/or speculative nature that it is one which it would be appropriate for the Court to exercise its inherent jurisdiction to ensure that its process is not used for purposes which are not explicable or do not make sense. It says the claim is misconceived, unviable

and/or is being conducted on an unrealistic hypothesis and the Court should take steps to halt the misuse of the proceedings. It relies on *Propend*, p662, per Leggatt LJ, which I quoted earlier.

207. Given I have resolved the first four issues in the Claimant's favour, it seems to me this fifth issue also must also be determined in his favour.

Conclusion

208. It follows the Defendant's application is dismissed. This case will proceed.