JUDGMENT : JONATHAN HIRST QC Deputy Judge, High Court. 18th October 2006.

1. In these proceedings, the Claimants make the fairly startling allegation that the Defendants have hacked into the Claimants' computer system in London in order to view confidential and privileged information in relation to litigation in which the parties are jointly engaged. The Defendants vigorously deny having engaged in any such improper conduct and contend that, if there was unauthorised access to the Claimants' computers (as it is fairly clear there was) it had nothing to do with them.

2. The Defendants now apply for a declaration that the English Court has no jurisdiction to try this action and for an order setting aside the issue and service of the Claim Form.

Background

3. The first Defendant, OJSC Russian Aluminium RUSAL ("Rusal") is the third largest aluminium producer in the world, producing about 9% of global output. The group has approximately 46,000 employees and in 2005 it had a sales revenue of some US$6.1 billion. Head office is in Moscow. The Group is privately owned. The Claimants contend that it is effectively solely owned ultimately by its Chairman, the third defendant, Mr Deripaska. That assertion has not been controverted before me. The Fourth Defendant, Mr Bulygin, is the Chief Executive Officer of the Group.

4. The Second Claimant ("Ansol") was incorporated in Guernsey in September 1998. It is controlled by Mr Avaz Saidovich Nazarov. The First Claimant ("Ashton") is an English company which provides consultancy services to Ansol. At the relevant time, it had offices at 6-10 Bruton Street, London W1.

5. According to evidence filed on behalf of the Claimants,[1] between 1999 and 2003, Ansol and Hydro Aluminium AS ("Hydro") entered into a series of barter arrangements with Tajik Aluminium Plant ("TadAZ") a state owned entity in Tajikistan which operated a large aluminium smelting plant. Tajikistan has large supplies of hydro-electric power but none of the raw materials (especially alumina) needed to produce aluminium. The barter arrangement was for Ansol to supply alumina (sourced from many parts of the world) and spare parts for the plant in return for which they received aluminium, which was exported by rail through Russia into Western Europe. This was a huge logistical operation.

6. In 2003, Ansol needed to find a new strategic partner to assist in financing this major enterprise. It claims that it entered into a joint venture with Rusal jointly to perform the barter arrangement that had previously been carried out by Ansol and Hydro. This joint venture operated successfully until December 2004. During that period, production at TadAZ continued to increase until it reached some 360,000 m.t., double what had been achieved in 1997. However, in December 2004, TadAZ suddenly stopped supplies under the existing arrangements and repudiated the barter arrangements. A few days later, it entered into a new arrangement with an off-the-shelf company registered in the British Virgin Islands, called CDH Investments Corp ("CDH"). It is alleged that CDH is really a front for Rusal. All this (including the existence of any joint venture involving Rusal) is hotly disputed.

7. On 12 May 2005, TadAZ applied to Etherton J. without notice for a world-wide freezing order and a search and seizure order against, *inter alios,* Ansol, Ashton and Mr Nazarov. It was alleged that Mr Nazarov had bribed the director of TadAZ, Abdukadir Ermatov, by gifts made to Mr Ermatov and his son over many years.

8. On 13 May 2005 Etherton J. granted wide ranging orders which included worldwide freezing orders against Ansol, Ashton and Mr Nazarov limited to the value of US$178 million and a search and seizure order against Mr Nazarov and Ashton. Execution of the order began on the same day. An application was made to Lewison J to stay further execution and he directed that the search should continue but all documents seized and all copies of computer hard disc drives were to be taken to the offices of DLA Piper Rudnick ("DLA"), who acted as the supervising solicitors. Between 1,500 and 2,000 files were removed from Ashton's offices and stored at DLA's offices.

9. Rusal was promptly joined to the proceedings by Ansol as an additional party under CPR Part 20. Ansol's case is that Rusal, TadAZ and others in Tajikistan have conspired together to steal the business formerly done by the joint venture by diverting it to Rusal. Mr Deripaska and Mr Bulygin were also joined as additional parties on the grounds they were necessary or proper parties. In circumstances to which I shall return, they were removed from the action by Cresswell J. following a judgment delivered by him on 28 July 2006 – [2006] EWHC 2374 (Comm). The application by Rusal to be released from the proceedings failed.

10. In the meantime, applications were made by all Defendants to discharge the orders made by Etherton J. On 27 May 2005, there was a hearing before Laddie J. during which concerns were expressed as to the adequacy of the cross-undertakings given to preserve the confidentiality of documents seized. An undertaking was given by counsel on behalf of TadAZ that none of the documents or other information disclosed by the Defendants (including Ashton and Ansol) should be made available to Rusal or its employees. The judge directed that TadAZ should not have access to the documents held at DLA's offices until the applications had been determined.

11. The applications came before Blackburne J. for a five day hearing in late July 2005. In his judgment delivered on 21 October 2005, he discharged the freezing injunction and the search and seizure orders,[2] although he left a proprietary injunction intact.[3] He directed that the files taken from Ashton's offices be returned to their solicitors,

[1] This is a bare summary. For a much more detailed exposition, see the Judgment of Blackburne J in ***Tajik Aluminium Plant v. Abdukadir Ganievich Ermatov & ors*** [2005] EWHC 2241 (Ch) delivered on 21 October 2005

[2] §193

[3] This was subsequently discharged by Blackburne J. on 11 January 2006.

Clyde & Co., so that they could first identify what needed to be disclosed in the proceedings, and to "minimise the risk of any of the documents, following their return [to their clients] being overlooked or going astray". He was critical[4] of the failure by TadAZ to highlight sufficiently the extent of Rusal's involvement in TadAZ's affairs, in particular that Rusal was funding the litigation and that day to day instructions to Herbert Smith, TadAZ's solicitors, came via Rusal. At §191 of his Judgment he said as follows: *"Pulling these various strands together, the strong overall impression which I have gained is that, notwithstanding the joint venture, Rusal has decided to further its own interests through the exploitation of TadAZ's aluminium production capacity, intends to do so shorn of any participation by Ansol through the joint venture, and, to that end and acting in conjunction with those who now control TadAZ, is backing these proceedings both by providing Herbert Smith with day to day instructions and by underwriting some or all of the cost to TadAZ of bringing them. In short, from once being Ansol's partner, through Hamer, in their joint dealings with TadAZ, Rusal has now become Ansol's rival and, as part of the pursuit of its commercial interest, is promoting this litigation. It does so while denying this court's jurisdiction to try Ansol's related cross-claims against it. This may turn out on closer examination at the trial to be a wrong conclusion but that is how it presently appears to me."*

12. This bitterly contested litigation continues.

13. There is also an arbitration proceeding in the London Court of International Arbitration between Hydro and TadAZ under the 2003 barter agreement. The case was due to be heard on 19 September 2005. On 22 August 2005 (with the permission of the Tribunal) TadAZ obtained from the Chancery Registry orders that Ashton produce at the hearing a wide range of documents and a number of witness summonses including one against Mr Nazarov. A further set of orders was obtained from the Admiralty and Commercial Registry on 5 September 2005. These orders would have encompassed many of the documents held at DLA's offices and covered by the undertaking offered to Laddie J (§10 *supra*).

14. On 13 September Mann J. heard applications to set aside the witness summonses and the orders to produce documents. He refused to set aside the witness summonses, but set aside the orders to produce documents on the grounds that the documents were not properly identified. TadAZ appealed but its appeal was dismissed on 24 October 2005 – see [2005] EWCA Civ 1218, reported at [2006] 1 Lloyd's Rep 155. Moore-Bick LJ said at the conclusion of his judgment: "*One such matter does deserve further mention, however, and that is the order made by Laddie J, to which TadAZ consented, restricting its access to the very same documents pending the outcome of the witnesses' challenge to the search and seizure order. Mr Doctor QC submitted that these witness summonses were little more than an attempt by TadAZ to circumvent that order to obtain immediate access to the documents for purposes unconnected with the arbitration. Miss Reffin submitted that TadAZ would be entitled to have access to them sooner or later in any event when the time came to give disclosure in the High Court proceedings and that the effect of obtaining production under the witness summonses would merely accelerate that process. However, since Laddie J's order was designed to ensure that the process of disclosure was not accelerated, at least until the dispute surrounding the search and seizure order had been resolved, I did not find that a very satisfactory answer. It was difficult to see how TadAZ could realistically hope to make much use of such a large body of material in the arbitration if it was only presented with the documents at the opening of the hearing, which leads one to suspect that it may have had an ulterior motive for issuing the witness summonses.*"

15. There is other litigation and also arbitration proceedings in various jurisdictions involving a number of parties, including TadAZ and Ansol and corporations said to be affiliates of Rusal.

The circumstances leading up to the issue of these proceedings

16. Ashton maintains a computer system in its offices in London. On 24 January 2006, Mr Vlad Sinani, the IT administrator employed by Ashton and Mr Makarov of Westbridge Associates, Ashton's then independent IT consultants, were carrying out what Mr Sinani described as a routine security scan on the Ashton server. In the course of it, they used a new security product called "F-Secure Blacklight" – this product had not yet been released on the market and was still in the process of development. The evidence did not reveal why Mr Sinani and Mr Makarov had decided to do this. At all events, the scan revealed a hidden software product often called "spyware". Further investigation showed that it was a product called "Perfect Keylogger" produced by a software company called Blazing Tools. The programme was designed to be installed surreptitiously on a computer – often via an innocent looking e-mail sent from a remote computer. The software manufacturers claim that the software is "absolutely undetectable".[5] Having been installed, the spyware makes a log of everything typed on the computer. It can also carry out "visual surveillance" by taking a snapshot of the computer screen and any information saved on file. This information can then be secretly transmitted to the person who installed it.

17. Records showed that the spyware had been installed on Ashton's server at about 4 a.m. on 20 January 2006. As administrator of the system, Mr Sinani is the only person authorised to have access to the server. His access is protected by a password which is (allegedly) only known to him.

18. Mr Sinani and Mr Makarov disabled the spyware (having taken a copy of it) and deleted it from the list of processes set to run on start-up. The administrator's password was re-set.

[4] See §207 of the Judgment.

[5] Miss Dohmann pointed out that this was a boast too far, because it *was* detected. It is in dispute whether the spyware can be detected by standard security products

19. This led to further investigations the next morning. An earlier version of the Keylogger software called KS.exe was found on Workstation 12, which is operated by Ashton's receptionist and secretary. The domain user or "owner" of the KS.exe file was called "Oroosinovich". The software appeared to have been installed on either the 11 March or 3 November 2005 (depending on the dating system used).[6] The workstation was not normally used to store confidential information. The spyware had been transmitting information to an internet number "smtp.list.ru/194.67.23.115". Mr Sinani had carried out a routine service on the workstation on 8 December 2005. In order to gain access he would have had to enter his administrator's user name and secret password. Mr Sinani and Mr Makarov disabled the KS.exe spyware on the workstation.

20. Mr Sinani and Mr Makarov examined the internet traffic incoming to Ashton's server between 19 and 24 January 2006. When a computer is accessed from a remote location, the user will usually leave a trace of information which includes details of the internet address from which access was obtained. The address is a unique number allocated to all users of the internet by an internet registrar, such as ICANN, Nominet or Réseaux IP Européens ("RIPE"). The latter maintains a searchable database of internet addresses.

21. This examination revealed that there had been two attempts to gain unauthorised access to the system on 19 January 2006. The first was at 5.44 a.m. from an internet address 213.248.20.172. It was made manually but was unsuccessful due to one mistake in the spelling of the word "remote" in the internet URL. A second attempt was made at 5.46 a.m. This was successful. The remote user appears to have entered the administrative account using the administrator's username and the administrator's secret password. The log on was for 38 seconds but the administrator user ID and password were not entered until 32 seconds into the event. The user appears to have signed out as soon as the successful log-in screen was completed.

22. Further at 3.31 a.m. on 20 January 2006, remote access was made from the internet address 83.237.37.9. And at 8.38 p.m. on 21 January via internet address 213.87.88.1. Changes made to the active directory of the server on 20 and 22 January 2006 also suggested that there had been further successful attempts to log into the server using the administrator's username and Mr Sinani's password.

23. The RIPE database revealed the following:
    i) Address smtp.list.ru/194.67.23.115 to which the spyware on the workstation was transmitting was registered to Mail.ru a large free e-mail provider in Russia, similar to Hotmail or Yahoo.
    ii) Address 213.248.20.172 from which the Ashton server was accessed (successfully on the second occasion) was one of the internet addresses registered to Rusal.
    iii) Address 83.237.37.9 from which Ashton's server was accessed on 19 January 2006 was registered to to ZAO MTU-Intel, an internet provider in Moscow.
    iv) Address 213.87.88.1 from which Ashton's server was accessed on 21 January 2006 was registered to MTS/Mobile Telesystems, one of the two main mobile phone operators in Moscow.

24. On about 1 February 2006, Ashton retained Mr James Kent, the retired head of Suffolk Police's hi-tech crime unit, and a senior forensic investigator and head of forensics at 7Safe Limited, an IT firm specialising in penetration testing, computer forensics and risk management to assist in the enquiry. In his report, Mr Kent records that the actions taken by Mr Sinani and Mr Makarov to secure the system, whilst entirely understandable, had resulted in important files and information being removed. "Subsequent forensic examination of original evidence has been made very difficult due to changes made to the system. The changes will not have affected the information contained within the log files."

25. Amongst many other things, Mr Kent examined the logs of the Ashton server from 14 January 2006. He confirmed the information that I have already set out. However, his investigations also revealed that on 14, 17, 18, 20, 21 and 22 January there were numerous successful attempts to gain access to the Ashton server from an internet address in Austria, addresses registered to ZAO MTU-Intel in Moscow and Mobile Telesystems OJSC in Moscow, using the administrator's username and password. In most cases it was not possible to work out the duration of the log on, but in one case it was for 37 minutes and in another 22 minutes. Of the indeterminate log ons, the potential duration was in some cases several hours.

26. There were also indications that, in many cases, a remote desktop was being used. This is a facility whereby the user can control a computer from another remote computer, just as if the user was sitting in front of the computer. It is a service legitimately used by an administrator. In the hands of a hacker, it is of great value. He has full remote control of the machine. If the user closes the session by logging off at the web workplace, this will be recorded on the local web log. If he closes the session without logging off, there will be no record in the web log of the length of the session.

27. Mr Kent also examined the monthly summary logs going back to January 2005. These appear to reveal that (probably)[7] in March 2005 and August 2005, there were attempts to communicate with the server from IP addresses 213.248.20.196 and 213.248.20.1. Both these addresses are registered to Rusal. If these were attempts to log on – there were "web requests" which might indicate this was being attempted – they were prevented.

[6] §14.1 of Mr Kent's 1st report rather suggests that it was probably on 11 March 2005.

[7] The summary file numbers are SUMM200503 and SUMM200508. The convention for file naming suggests these are for these months.

28. On 3 February 2006, a full port scan was conducted on the Ashton server from a remote location. The remote computer was trying to scan every port or entry point to discover which was open. This scan would have taken several hours to complete.

29. I have set out the information extracted by Mr Sinani and Mr Makarov and Mr Kent without comment. Most is I think not really in dispute at least for the purposes of this application. However, it has led to very differing conclusions being drawn by the parties.

The Claimants' Case against Rusal and the commencement of proceedings.

30. The discovery that someone from an IP address registered to Rusal had attempted to log on and then successfully logged on to the Ashton server on 19 January 2006, using the administrator's user name and password, was viewed by the Claimants with the utmost gravity in the context of the bitter disputes with Rusal. They concluded that by leaving its registered address 213.248.20.172 on the Ashton server, Rusal had left the equivalent of a finger print at a crime scene. They drew the inference that, in all probability, Rusal was behind the other attempts, successful and unsuccessful, to gain access to the Ashton system and that Rusal had managed to obtain secret and privileged information about the litigation. The chronology they suggested was as follows:
    i) Back as long ago as March 2005, Rusal had been attempting to communicate with the Ashton server.
    ii) Either in March or November 2005, Rusal had succeeded in installing Keylogger spyware onto Workstation 12. This was done remotely probably using an innocent looking e-mail. The spyware transmitted information to an internet address controlled by Rusal. Free internet addresses are not subject to many security checks and in practice are anonymous, so ideal for hackers.
    iii) On 8 December 2005, Mr Sinani serviced Workstation 12. In order to do so he entered the administrative account and used the administrator's password. These keystrokes he used were recorded by the spyware and subsequently transmitted to Rusal.
    iv) Having obtained the key information needed to access the server, Rusal did so from 14 January using various accounts in Russia and one in Austria. Mobile telephone accounts are also fairly anonymous and it is difficult to discover who the user actually is.
    v) On 19 January 2006, after one unsuccessful attempt, Rusal logged on from a Rusal registered address using the administrator's username and password.
    vi) Using this username and password, the spyware was also successfully installed on the main server on 4 a.m. on 20 January 2006.
    vii) The Claimants cannot say what files (if any) Rusal accessed, viewed and/or downloaded to their own computers, but it had ample opportunity to do so, and it is pretty obvious that they must have been looking for confidential and privileged information in connection with the litigation and other disputes involving Rusal and TadAZ.

31. On the basis of this case, on 8 February 2006, the Claimants issued a claim form "not for service out of the jurisdiction" in the Chancery Division against the Defendants. The brief details given of the claim were that the claims against each defendant "arise from unauthorised access gained by one or more of the Defendants (or others acting on their behalf and with their authority) to the computer system of the First Claimant which contains confidential and legally privileged information belonging to both Claimants)". The following relief was sought:
    i) Damages/equitable compensation/restitution for breach of confidence;
    ii) Damages for unlawful interference with business;
    iii) Damages for conspiracy by unlawful means;
    iv) An injunction;
    v) Further or other relief;
    vi) Costs.

32. On the previous day, the Claimants had issued an application notice in the Part 20 proceedings seeking wide ranging injunctive relief against the Defendants. The application notice also sought an order for substituted service on Bryan Cave & Co. and "in so far as necessary, there be permission to serve out of the jurisdiction by a method specified by the court". The application was supported by the 3rd witness statement of Julian Connerty and the 1st witness statement of Andrei Makarov both dated 8 February 2006. It came before Park J. on 9 February 2006. With admirable expedition, the Defendants were able by that date to produce a statement from Dennis Willetts, a computer expert who gave an initial report, and a statement from Paul Hauser, a partner in Bryan Cave. Mr Connerty had also filed a 4th witness statement in which he clarified that the Claimants were seeking permission to serve the Claim Form on the four Defendants in Russia and that the paragraphs in CPR Part 6.20 on which they relied were:
    i) CPR 6.20(2) – *"This is a claim for an injunction ordering the Defendant to do or refrain from doing an act within the jurisdiction".*
    ii) CPR 6.20(8) – *"claim made in tort where the damage is sustained within the jurisdiction".*

    Mr Connerty confirmed that the Claimants believed that the claim had reasonable prospects of success.

33. Very sensibly, the parties reached agreement as to how this application was to be dealt with. The agreement was contained in a consent order made by Park J. on 9 February, and entered on 10 February 2006. Essentially,
    i) The Defendants gave undertakings, without prejudice to their objection to the jurisdiction of this Court and without prejudice to their contention that none of the Claimants' allegations were well founded, *inter alia*, not to enter into, view, or modify Ashton's computer systems.

ii) The proceedings were to be served on all the Defendants by fax to Bryan Cave, on the clear understanding that no point would be taken by the Claimants based on the agreement for service of the claim form in this way, and that no point would be taken by the Defendants based on the absence of service in Russia.
iii) Directions were given for the service of further evidence.

34. The Claimants served their Particulars of Claim on 27 February 2006. They advanced the following causes of action:
i) Breach of confidence;
ii) Wrongful interference with the Claimants' businesses with intent to injure and by using unlawful means;
iii) Unlawful means conspiracy.

35. On 5 May 2006, Cresswell J. ordered by consent that the action be transferred to the Commercial Court and he directed that any jurisdictional challenge was to be issued by 8 May. On 8 May, the Defendants duly issued their application for an order declaring that the English Court had no jurisdiction to try these proceedings, alternatively that it should not exercise any such jurisdiction, and setting aside the issue and service of the Claim Form.

The hearing

36. I heard this application on 27 September 2006. It was accompanied by very extensive written argument and evidence. It was agreed that, although service of the proceedings had been effected in this jurisdiction, I should proceed on the basis that permission had been required to serve them out of the jurisdiction and that service had been effected in Russia – i.e. that in accordance with the spirit of the consent order made by Park J., the Defendants should in no way be prejudiced by their agreement to short-cut service. I have proceeded on the basis that the Defendants' application is to be tested by asking whether the Claimants could justify obtaining permission to serve out under CPR Part 6.20 in the light of all the evidence before the Court.

37. In the course of her argument, Miss Barbara Dohmann QC for the Defendants developed the following primary submissions:
i) The Claimants had failed to demonstrate that there was a serious issue to be tried in relation to each cause of action.
ii) The claims did not come within the relevant sub-paragraphs of CPR Part 6.20, let alone the letter and spirit of those paragraphs.
iii) The Claimants had failed to show that England was the *forum conveniens* for the dispute. Russia was another available jurisdiction and it was the natural and appropriate forum for the resolution of the dispute.

I will deal with the arguments in the same order.

The Defendants' factual case.

38. First, however, it is right that I should set out the factual case advanced before me on the basis of evidence filed by the Defendants. In addition to the preliminary evidence filed from Mr Willetts and Mr Hauser, the Defendants also filed witness statements from Elina Klimova, Paul Hauser (2nd), Mikhail Erenburg (1st and 2nd), and Dennis Willetts (2nd).

39. In their factual evidence, the Defendants vigorously dispute that they or anyone acting on their behalf ever sought to gain access to Ashton's server, let alone successfully did so. As to the crucial log-ons on 19 January (one successful and the other unsuccessful) their evidence is as follows. The IP address 213.248.20.172 is one of the 782 internet addresses registered to Rusal, of which only 84 have ever been used. Of these, only 2 are in regular use. One is used by computers physically connected to the Moscow system. The other – 213.248.20.172 – is allocated exclusively to the wireless connection to the net (so called "wi-fi"). Radio transmitters were installed at Rusal's head office at 13/1 and 15 Nikoloyamskaya Street in Moscow in November 2004. Computers with a "wi-fi" card and software could pick up the signal and connect to the internet. The radio beam had a range of about 100 metres outside the office, but this could be extended to about 5 kilometres if an antenna was used.

40. Despite warnings from Rusal's IT department that, unless security measures (such as passwords) were put in place, third parties would be able to use the system to gain free access to the internet, the wi-fi system was not protected at first. It soon became apparent that the level of unauthorised use was so high that it was starting to cost Rusal money. A system of MAC numbers (short for media access control) was introduced. A MAC number is a unique number assigned to a computer. A wi-fi system can be programmed only to allow access to computers with recognised MAC numbers. As from April 2005, anyone wishing to use the wi-fi system had to register their computer's MAC number with the IT department.

41. As at 19 January 2006, only two computer MAC numbers were authenticated for use with the IT department.[8] One was operated by Ms Elena Klimova, Director of the Treasury Department of the Second Defendant. Mr Willetts examined this machine on 26 May 2006. It had not accessed the Ashton system on 19 January. Ms Klimova confirmed this, and added that she only ever connected the machine to the main system and did not use the wi-fi connection. The other had been operated by Mr A. Myshkin, but he was no longer employed by the Second Defendant. The machine had been handed back to the IT department in September 2005, since which time it had been left dormant in a locked cupboard. Mr Willetts examined the machine on 13 March 2006, and he confirmed that it was not in use on 19 January 2006.

[8] As I understood it, the primary purpose of having the wi-fi system was to allow guests within the building to gain access to the internet using their laptops. But it seems that no guest computers were enabled to do this.

42. Yet, Mr Erenburg discovered that these two MAC numbers had appeared with very great frequency in Rusal's web authentication logs. So for example, on 8 September 2005, the number assigned to the dormant machine was authenticated to the wi-fi system over 100 times. Mr Erenburg and Mr Willetts consider that this is highly unusual behaviour for an individual and they believe that the MAC numbers must have been cloned and used by third parties. Rusal's Moscow headquarters are only about 100 metres from the Moscow State Aviation Technological University, known as MATI. The most likely explanation was that the MAC numbers were obtained and distributed amongst university students, although they could have been used by someone much further away using an aerial attached to their computer. Anyone using the wi-fi system to access another computer via the internet would leave the Rusal IP address on the other computer, so that it would appear (falsely) that it was a Rusal employee who had obtained the unauthorised access, whereas in fact it was someone misusing the Rusal wi-fi system.

A serious issue to be tried?

43. On the basis of this evidence, Miss Dohmann submitted that there was really no evidence to connect the unauthorised log-ons onto Ashton's server with Rusal. The only "grain of sand" which supported the edifice of the Claimants' case was the discovery of the log-on on 19 January 2006 using the Rusal internet address. Once this grain of sand was removed, there was nothing left of it. The remainder of their case was anyway based on impermissible and unsupportable inference. Miss Dohmann also emphasised that there was no evidence that anything was ever viewed or downloaded, or that any spyware or other malign programmes installed. It was obvious that in the 6 seconds on 19 January 2006, during which access was gained to the Ashton server, nothing could have been downloaded. As a result of the steps taken by Mr Sinani and Mr Makarov to prevent further unauthorised access, the alleged "crime scene" had been trampled over and any relevant foot prints were no longer discernible. There was no evidence of what, if anything, had been downloaded or viewed on any other occasion of unauthorised access.

44. On this basis, Miss Dohmann submitted that the Claimants had failed to surmount the first hurdle – to establish that there was a serious case to be tried. In considering this submission, I will deal first with the case against Rusal and Rusal Management Company (the "Rusal Defendants") as to which no distinction was drawn in argument, and then with the case against Mr Deripaska and Mr Bulygin.

45. Counsel disagreed as to the right test to apply. Miss Dohmann relied on what she called the gloss introduced by Waller LJ in ***Canada Trust Co. & ors v. Stolzenberg & ors (No. 2)***[1998] 1 WLR 547. She submitted that the Claimants had to show that they had a much better argument on the material available. She founded this submission on the following passage in the judgment (at p.555 b-g): *It is I believe important to recognise, as the language of their Lordships in Korner's case demonstrated, that what the court is endeavouring to do is to find a concept not capable of very precise definition which reflects that the plaintiff must properly satisfy the court that it is right for the court to take jurisdiction. That may involve in some cases considering matters which go both to jurisdiction and to the very matter to be argued at the trial (eg the existence of a contract), but in other cases a matter which goes purely to jurisdiction (eg the domicile of a defendant). The concept also reflects that the question before the court is one which should be decided on affidavits from both sides and without full discovery and/or cross examination, and in relation to which therefore to apply the language of the civil standard of proof applicable to issues after full trial, is inapposite. Although there is power under Ord 12, r 8(5) to order a preliminary issue on jurisdiction, as Staughton LJ pointed out in the* ***Attock Cement case*** *[1989] 1 All ER 1189 at 1197, [1989] 1 WLR 1147 at 1156, it is seldom that the power is used because trials on jurisdiction issues are to be strongly discouraged. It is also important to remember that the phrase which reflects the concept 'good arguable case' as the other phrases in Korner's case 'a strong argument' and 'a case for strong argument' were originally employed in relation to points which related to jurisdiction but which might also be argued about at the trial. The court in such cases must be concerned not even to appear to express some concluded view as to the merits, eg as to whether the contract existed or not. It is also right to remember that the 'good arguable case' test, although obviously applicable to the ex parte stage, becomes of most significance at the inter partes stage where two arguments are being weighed in the interlocutory context which, as I have stressed, must not become a 'trial'. 'Good arguable case' reflects in that context that one side has a much better argument on the material available. It is the concept which the phrase reflects on which it is important to concentrate, ie of the court being satisfied or as satisfied as it can be having regard to the limitations which an interlocutory process imposes that factors exist which allow the court to take jurisdiction."* [my emphasis]

46. Mr Brian Doctor QC responded that Lord Goff's speech in ***Seaconsar Ltd. v. Bank Markazi Jomhouri Islami Iran*** [1994] 1 AC 438 remained the leading authority. He cited these passages at pp. 455F-456E and 456G-457B:

> *"… it is difficult to see why the fact that the writ is to be served out of the jurisdiction should have any particular impact upon the standard of proof required in respect of the existence of the cause of action. On this point, I find myself in respectful disagreement with the opinion expressed by Lloyd L.J. to the contrary in the Court of Appeal [1993] 1 Lloyd's Rep. 236, 242. I prefer the approach of Stuart-Smith L.J. when, at p. 248, he commended his preferred view as consonant with common sense and policy, and continued: "It seems to me to be wholly inappropriate once the question[s] of jurisdiction and forum [conveniens] are established for there to be prolonged debate and consideration of the merits of the plaintiffs' claim at the interlocutory stage."*
>
> *It has been suggested that, since both the assessment of the merits of the plaintiff's claim and the principle of forum conveniens fall to be considered as elements in the exercise of the court's discretion, these should be regarded as*

interrelated in the sense that "the more conspicuous the presence of one element the less insistent the demands of justice that the other should also be conspicuous:" see ***Societe Commerciale de Reassurance v. Eras International Ltd.(formerly Eras (U.K.)*** *[1992] 1 Lloyd's Rep. 570, 588, per Mustill L.J. This approach originated in the speech of Lord Oaksey in Korner's case, at pp. 881-882, to the effect that the strength of the evidence in that case as to forum conveniens was such that only the slightest evidence was required of there having been a breach of contract within the jurisdiction. Lord Oaksey's speech also provided the inspiration for an expression of opinion by Parker L.J. to the effect that, if there is overwhelming evidence that England is the appropriate forum, it will be enough that, on the merits, the plaintiff's case is worthy of serious consideration: see* ***Overseas Union Insurance Ltd. v. Incorporated General Insurance Ltd.*** *[1992] 1 Lloyd's Rep. 439, 448, and see also. [1991] 2 Lloyd's Rep. 19,* ***Banque Paribas v. Cargill International S.A 25****. I must however express my respectful disagreement with this approach. Suppose that, for example, the plaintiff's case is very strong on the merits. If so, I cannot see that a case particularly strong on the merits can compensate for a weak case on forum conveniens. Likewise, in my opinion, a very strong connection with the English forum cannot justify a weak case on the merits, if a stronger case on the merits would otherwise be required. In truth, as I see it, the two elements are separate and distinct. The invocation of the principle of forum conveniens springs from the often expressed anxiety that great care should be taken in bringing before the English court a foreigner who owes no allegiance here. But if jurisdiction is established under rule 1(1), and it is also established that England is the forum conveniens, I can see no good reason why any particular degree of cogency should be required in relation to the merits of the plaintiff's case. …*

Once it is recognised that, so far as the merits of the plaintiff's claim are concerned, no more is required than that the evidence should disclose that there is a serious issue to be tried, it is difficult to see how this matter, although it falls within the ambit of the court's discretion, has not in practice to be established in any event. This is because it is very difficult to conceive how a judge could, in the proper exercise of his discretion, give leave where there was no serious issue to be tried. Accordingly, a judge faced with a question of leave to serve proceedings out of the jurisdiction under Order 11 will in practice have to consider both (1) whether jurisdiction has been sufficiently established, on the criterion of the good arguable case laid down in ***Korner's*** *case, under one of the paragraphs of rule 1(1), and (2) whether there is a serious issue to be tried, so as to enable him to exercise his discretion to grant leave, before he goes on to consider the exercise of that discretion, with particular reference to the issue of forum conveniens.*

47. Waller LJ was not seeking to change the principles established in ***Seaconsar,*** nor could he. Properly interpreted, he was referring to the case where jurisdiction was founded on a disputed factor that only went to jurisdiction – eg the alleged domicile of the Defendant. In such cases, where the issue would never be argued again, there was much to be said for the proposition that a Claimant should have to establish that he had much the better of the argument.

48. This submission gained considerable support from the judgment of Rix LJ in ***Konkola Copper Mines v. Coromin Limited*** [2006] EWCA Civ 5; [2006] 1 Lloyd's Reps 410, where he said:

> *[80] The present case, however, while closer to the former variety, is either an extreme form of it or, as I would prefer to think, a third variety where the jurisdictional factor is part and parcel of the ultimate merits of trial. On the structure of the argument presented before Colman J and in the parties' original skeleton arguments for appeal, the issue, Zambian or English jurisdiction clauses, was simply one aspect of the broader issue: KCM wording (named perils cover) or CCIP wording (all risks cover). But that is the issue at trial between these parties (and the 'collapse' issue only becomes relevant if the reinsurance contract is on the KCM wording). In such a case it seems to me that Waller LJ's warnings about avoiding even the appearance of pre-trying the central issue move to centre stage.*
>
> *[81] What is to be done in such a case? One possibility is that the Canada Trust gloss ('a much better argument') of the 'good arguable case' test is not really appropriate in such circumstances. It is quite possible, especially at the opening, jurisdictional, stages of a dispute for both sides to have a good arguable case as to the central merits of a dispute. I would regard the present case as being a good example of just such a dispute. It is after all familiar enough, even at the end of a trial, for a judge to think that the merits of the opposing parties are fairly evenly balanced. If a court, in applying the good arguable case test, as well as taking account of the opposing arguments as it has always done, in addition had to decide and rule as to which side had the 'much better argument', I fear that, however much the judge couched his reasoning in terms of the provisional nature of his decision on the material available, he would inevitably be drawn into a trial of the merits. This is plainly undesirable. Is it necessary? I am doubtful that it is, especially in circumstances where, as was generally the case under the old RSC Ord. 11 or is now the position under CPR 6.20, the power to give leave to serve out of the jurisdiction is at the end of the day a discretionary one. However important the proper disposition of a jurisdictional challenge is, it is not something which should be allowed to subvert the merits of a potential trial.*

49. After Mr Doctor had handed up his submissions on this part of the case, I gave Miss Dohmann the opportunity to respond in writing, but she did not avail herself of that opportunity.

50. In my judgment, Miss Dohmann's arguments would require me to do exactly what Lord Goff warned against – to enter a prolonged consideration of whether the Claimants had a much better overall case than the Defendants. This would go to the heart of what the trial court will have to decide. I think the right question for me to ask is whether the Claimants have shown that there is a serious issue to be tried. In considering that question, I bear in mind that the Claimants are making extremely serious allegations against the Defendants, involving conduct which would be criminal under sections 1 and 2 of the Computer Misuse Act 1990, and which would constitute an

outrageous attempt to gain access to privileged information held by the other party to litigation, and will have to produce commensurate proof.

51. I am satisfied that the Claimants have shown that there is a serious issue to be tried. They have done more than just scrape over the hurdle. Without (I hope) trespassing excessively on the merits of the case:

i) I agree with Miss Dohmann that it is absolutely critical for the Claimants to show that the two attempts to access Ashton's server on 19 January 2006 were by Rusal. That is the peg on which the rest of the Claimants' case must hang. The Defendants may turn out to be right at the end of the day that these attempts were actually by other people who had cloned the MAC numbers, so appearing to be from Rusal when they were not. And it is fair to say that if Rusal were trying to gain access, it was a considerable blunder to leave behind the computer equivalent of a fingerprint. However, as against that, it is an extraordinary co-incidence that, say, a student should happen, whilst using the Rusal wi-fi, to gain access to the Ashton server using the administrator's username and password. There is a dispute about how public the Ashton website is – Mr Connerty says the URL address is not readily available publicly but this is challenged. Whatever the position, why should a Russian student have any interest in the Ashton website or go to the considerable trouble to obtain the password? Why should students or other people wish to enter the system repeatedly? By contrast, Rusal undoubtedly had a motive to gain access to the server, although that is a long way from saying that it did so. It will not be the first time that a perpetrator has been found out as a result of a stupid mistake.

ii) Whilst Miss Dohmann is right that the events of 19 January 2006 are critical, there is other evidence, which I have summarised at paragraphs 14 and 27, which, on one interpretation, show an unhealthy interest on the part of Rusal in the documents held by the Claimants and on Ashton's server, and which could be seen as consistent with Rusal having obtained access on 19 January.

iii) If Rusal did obtain access on 19 January 2006 using the administrator's username and password, then I think that a judge could infer that the other incursions were also by or on behalf of Rusal. It might be seen as a surprising coincidence that there should be someone else doing the same thing at the same time. Further, why should Rusal go to the trouble of gaining the means of achieving unauthorised access and then do so for only a very short time (something which it had no legitimate reason for doing) and just leave it at that?

iv) Miss Dohmann is also right that there is no direct evidence as to what the hackers were doing. It seems fairly clear that no further information is likely to be obtained from Ashton's computer logs, so it will be a matter for inference,[9] unless other evidence becomes available. I agree with her that it seems improbable indeed that anything can have been viewed on 19 January 2006, but if Rusal were behind the other instances of unauthorised access, there seems to have been plenty of time to have a very good look for privileged and confidential material. It is difficult to conceive of what other motive Rusal could have had. It would be open to the Court to conclude that Rusal must have improperly obtained highly confidential and privileged information stored on the server and belonging to Ashton and Ansol with the intent of gaining an advantage in the litigation – I stress that there is, of course, not the slightest suggestion that the team of counsel led by Miss Dohmann or Bryan Cave would conceive of making use of any information so obtained.

Ultimately, as the evidence stands,[10] the trial judge will have to decide whether the Claimants are right that the necessary inferences can properly be drawn. I make it clear that I am certainly not saying that a Court would draw these inferences. It is enough for me to say, after a review of the evidence and having heard counsel, that I am satisfied that they have a good arguable case. So do the Rusal Defendants.

52. The position of Mr Deripaska and Mr Bulygin is very different. The Claimants' pleaded case against them is as follows:

47. All strategic decisions are taken by Messrs Deripaska and/or Bulygin, who are in complete control of the entire group and all affiliates. They are also intimately involved in the Main Proceedings and Mr Bulygin has given evidence therein.

48. It is to be inferred that the unauthorised access to the System … took place with the knowledge and express consent of Messrs Deripaska and Bulygin …, alternatively with their implicit consent.

49. In the premises:

49.1 The Hackers were acting with the authority of Mr Deripaska, Mr Bulygin and Rusal Management Company .

49.2 All of the Defendants together with the Hackers were, and each of them was, acting in concert and/or as mutual agents for each other and/or under the control and direction of each other and the knowledge of each was the knowledge of all and communication to one was communication to all.

49.3 Each of the Defendants is therefore jointly and severally liable for the breach of confidence, unlawful interference with business and breach of Articles 6 and 8 of the ECHR.

53. In evidence the Claimants added that Rusal is an unidentifiable and amorphous group which cannot be definitely identified. Its international trade was carried out by a complex, impregnable and impenetrable web of offshore entities, registered primarily in the BVI and other offshore jurisdictions such as Gibraltar and Cyprus.

[9] There is a dispute about whether Mr Sinani and Mr Makarov unwittingly damaged the logs and records on the Ashton server. At this stage, I am doubtful that they did.

[10] It may have developed by trial

54. The Claimants mounted a similar argument in the Part 20 proceedings.[11] Cresswell J. held (at §181) that Mr Deripaska and Mr Bulygin were not proper defendants. He considered that the case against them had not been properly particularised.

55. In my judgment, the case that the individual defendants were behind the hacking into Ashton's server goes beyond what might be a legitimate inference and enters the realms of conjecture. Rusal is a very large group with thousands of employees which, on the evidence, is ultimately owned and controlled by Mr Deripaska and in which Mr Bulygin plays a very senior role. Even assuming that it is amorphous and operates through a number BVI companies – and I should note that it was a group with which Ansol was willing to do business on a large scale – and that these two individuals do take the major strategic decisions in the business, I do not think that it follows that it can be reasonably inferred that they were personally party to gaining improper access to the Ashton server. The Claimants have failed to establish on the evidence that they have a seriously arguable case against the individuals that they committed the substantive torts. I will revert to the additional question argued before me whether they can nevertheless be joined as necessary and proper parties to the action.

CPR Part 6.20

56. The Claimants submitted that they could establish the following causes of action against the Rusal Defendants:
i) Breach of confidence, and/or inducing or procuring the same;
ii) Unlawful interference with business;
iii) Unlawful means conspiracy.

I did not understand Miss Dohmann to submit at this stage, assuming (as she strongly contested) the Claimants could establish the facts they allege, there would not be an arguable cause of action for breach of confidence and unlawful interference. However she submitted that the case in conspiracy was not adequately pleaded. I have already indicated that the Claimants have completely failed to demonstrate a sufficiently arguable case that Mr Deripaska and Mr Bulygin were involved in any impropriety. What is left of their conspiracy plea, which adds very little to the case? Not much in my judgment, and certainly not enough to justify service out as the pleading stands. The Particulars of Claim completely fail to set up the sort of overt acts from which it could properly be inferred that the remaining Defendants were a party to a conspiracy. However, I am can see that it might well be possible to plead a conspiracy involving a number of unknown individuals and the Rusal Defendants, given (on the Claimants' case) the way in which the spyware was originally installed and activated and multiple attempts made from Russia and Austria to gain access to the Ashton server. I therefore consider that the right course is to give the Claimants a further opportunity to re-plead this part of the case against the Rusal Defendants.

57. On the basis of these causes of action, the Claimants asserted that they could justify service out of the jurisdiction on the Rusal Defendants through the following gateways of CPR Part 6.20:
i) 6.20(8) on the basis that the claims for unlawful interference and conspiracy were claims made in tort and
(a) damage was sustained within the jurisdiction; or
(b) the damage sustained resulted from an act committed within the jurisdiction.
ii) 6.20(10) on the basis that the claim for breach of confidence related to property located within the jurisdiction.
iii) 6.20(15) on the basis that the claim for breach of confidence also amounted to a claim for restitution where the Defendants' liability arose out of acts committed within the jurisdiction.
iv) 6.20(2) on the basis that an injunction was being sought ordering the Defendants to do or refrain from doing acts within the jurisdiction.
v) As against Mr Deripaska and Mr Bulygin, 6.20(3) on the basis that they are necessary and proper parties to the claim against the Rusal Defendants.

58. Miss Dohmann challenged each of these propositions.

6.20(8) Tort

59. Miss Dohmann argued that the tort was committed in Russia. The issue was where the substance of the tort was committed – see the Privy Counsel's Judgment in ***Distiller's Co (Biochemicals) Ltd v. Thompson*** [1971] AC 458, 468: *"It is not the right approach to say that, because there was no complete tort until the damage occurred, therefore the cause of action arose wherever the damage happened to occur. The right approach is, when the tort is complete, to look back over the series of events constituting it and ask the question: where in substance did this cause of action arise?"*

Here the substance of the acts occurred in Russia – that is where the intention was formed to gain unauthorised access, where the electronic installation of the software occurred and where the administrator's username and password were improperly entered. Further the damage was caused where the confidential information was received. That is where the tort was complete.

60. Miss Dohmann also argued that no real damage was caused to the Claimants. The Particulars of Claim plead as follows:

53. As a result of the said breach of confidence and/or unlawful interference and/or conspiracy by unlawful means and/or inducement of breach of confidence the Claimants have suffered loss and damage in a sum to be fully particularised following disclosure and/or expert evidence herein, but including:

[11] See §150 of the judgment of Cresswell J.

53.1 the cost of a new server … ;

53.2 the costs of investigations and ancillary work carried out by Ashton's IT consultants … ;

53.3 the cost of investigations by the forensic computer experts … .

These claims could not be sustained. Ashton's computer system was so inadequately protected from outside interference, that costs would have to be incurred anyway to upgrade the system to an adequate configuration. Further the cost of the new server, £3,231.25, was so trivial that it was utterly disproportionate to bring foreign defendants in.

61. The applicable legislation in *Distillers* was section 18(4) of the New South Wales Common Law Procedure Act 1899. The Court would have jurisdiction over the foreign Defendant if the cause of action arose within the jurisdiction. The test under CPR 6.20(8) is not the same. More relevant guidance was given by the Court of Appeal in ***Metall & Rostoff v. Donaldson Inc.*** [1990] 1 QB 391,437: *"As the rule*[12] *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 A.C.L.I. 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 common sense 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."*

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 costs 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.

64. So both limbs of CPR Part 6(20)(8) are satisfied.

Breach of confidence: CPR 6.20(10) and (15)

65. The Claimants did not originally seek permission to serve out on these grounds, but Mr Connerty put forward these additional grounds as justification for service out in his 6th witness statement. No application was issued prior to the hearing, but after considerable prodding from Miss Dohmann, Mr Doctor made an oral application in the course of the hearing to add these grounds. This is not a case where the Claimants are seeking to add a cause of action for which permission has not previously been obtained for service out: the breach of confidence claim was included as the first of the potential causes of action listed by Mr Connerty in paragraph 123 of his 3rd witness statement. Rather, on the basis of facts set out in the original witness statements and in the pleadings, the Claimants are now saying that there are further gateways available under Part 6.20. I cannot see that any

[12] RSC Order 11 r.1(1)(f) which is for all intents and purposes identical to CPR 6.20(8)

prejudice is caused to the Defendants and I give permission for the Claimants to rely on these grounds, subject to the appropriate application notice being issued. So I turn to the substance of these grounds.

66. CPR Part 6(20)(10) permits service out where "the whole subject-matter of a claim relates to property located within the jurisdiction". Mr Doctor submitted that property was not confined to real property, but extended to personal property, intellectual property and confidential information. Here the property to which the claim related was the Ashton computer system and the confidential information contained thereon.

67. Support for this argument is given by ***In Re Banco Nacional de Cuba*** [2001] 1 WLR 2039, where Lightman J. said (at §33): *"The critical differences between RSC, O 11, r 1(1)(g) and CPR 6.20(10) is the substitution for the words "land situate within the jurisdiction" of the words "relates to property located within the jurisdiction". The implications are that: (1) the rule is no longer limited to land and now extends to personal property; and (2) instead of the whole claim having to be confined to a claim to a proprietary or possessory interest, it is sufficient that the whole claim relates to property. The evident purpose of the new rule is to lay down a single rule in place of the three earlier rules which embraces and extends beyond the contents of those rules. It is to be noted that at p 128 of the Autumn 2000 Civil Procedure ("White Book") the comment is made on CPR 6.20(10): "This wide and new provision is no longer confined to land and the old cases are redundant." In my view on its proper construction the rule cannot be construed as confined to claims relating to the ownership or possession of property. It extends to any claim for relief (whether for damages or otherwise) so long as it is related to property located within the jurisdiction. This construction vests in the Court a wide jurisdiction, but since the jurisdiction is discretionary the Court can and will in each case consider whether the character and closeness of the relationship is such that the exorbitant jurisdiction against foreigners abroad should properly be exercised."*

Briggs & Rees on Civil Jurisdiction and Judgments (4th ed.) suggests at §4.46 that property includes intellectual property rights. Dicey, Morris & Collins on Conflicts of Laws (14th ed.) at §11R-230 offers no assistance on the point.

68. Miss Dohmann did not seek to challenge this argument. In my judgment, Part 6.20(10) extends to claims in respect of confidential information if it can be established that the information was really located in the jurisdiction. Information contained in digital form on a server in London satisfies this test.

69. Part 6.20(15) allows service out where the claim is made for restitution and the Defendant's alleged liability arises out of acts committed within the jurisdiction. Mr Doctor cited ***Douglas & ors v. Hello! Limited*** [2003] EWCA 139 [2003] EMLR 585 at §§23-26 for the proposition that paragraph 15 has been successfully relied upon for service out of claims for equitable relief for breach of duty. That is a pretty frail foundation – the focus of the Court of Appeal was whether there was a sufficient case of tortious conduct to justify service out. It is far too sweeping an assertion that any claim for equitable relief in respect of a breach of confidence is a claim in restitution. Some may be, but each case needs to be looked at closely on its own facts. The Particulars of Claim includes a claim for an account of profits but that does not seem a very realistic remedy on the facts of this case – it seems improbable indeed that the Defendants will have sold any ill-gotten information. This case is not in substance a claim in restitution and I am not satisfied that Part 6.20(15) can be properly invoked.

Injunction: CPR Part 6.20(2)

70. Part 6.20(2) permits service out where a claim is made for an injunction ordering the Defendant to do or refrain from doing an act within the jurisdiction. In the Particulars of Claim, the Claimants seek a permanent injunction restraining the Defendants from using or disclosing any information unlawfully obtained and an order for delivery up of any documents containing such information. Rather oddly, no injunction is sought restraining the Defendants from interfering with the Ashton server, although undertakings were obtained in these terms.

71. The Claimants do not need to rely on Part 6.20(2) to obtain relief restraining use of information improperly obtained, or for delivery up. That relief can be granted (if appropriate) in connection with the claim for breach of confidence and, possibly, the claim for wrongful interference. The information is now presumably in Russia and any documents are likely to be there. I am not satisfied that the injunction would in substance be ordering the Defendant to do or refrain from doing an act in the jurisdiction.

72. By contrast, if a claim were added for an injunction restraining the Defendants from interfering with the server (as I anticipate it will be), that would be restraining the Defendants from doing an act in the jurisdiction. Miss Dohmann submitted that in order to rely on this as a ground for jurisdiction, the Claimants would have to show that there were real grounds on which to anticipate a repetition: ***Watson v. Daily Record Ltd*** [1907] 1 KB 853 where Cozens-Hardy LJ held, in the context of an unusual libel action: *"Now it seems plain that the Court has a discretion, and that a plaintiff cannot acquire a right to serve a defendant out of the jurisdiction by the mere fact that his writ claims an injunction. The Court must at least be satisfied that the claim for an injunction is made in good faith. This was decided by the Divisional Court in **De Bernales v. New York Herald**, where Lopes L.J. said: "I do not believe the claim for an injunction is made bona fide, but merely to bring the case within Order XI. There is no evidence of any apprehended repetition of the libel, and indeed, having regard to the circumstances, it is most improbable that it will be repeated. ... The giving leave to serve notice of writs out of the jurisdiction is a matter of judicial discretion." It must not be inferred from the language used by Lopes L.J. in that case that want of good faith is a complete or exhaustive statement of the grounds for refusing to order service out of the jurisdiction. If the Court is satisfied that, even assuming the plaintiff to have a good cause of action, there is no reasonable probability that he will obtain an injunction, the Court ought not to consider the insertion of a claim for an injunction as sufficient to justify service on a*

person resident out of the jurisdiction. The Court is bound to consider all the circumstances disclosed by the affidavits, and to take care that a Scotchman, or it may be a foreigner, is not improperly made amenable to the orders of an English tribunal."

Miss Dohmann submitted that there were no grounds to anticipate a repetition and, anyway, now that Ashton had taken steps to improve the security of its server, there was no need for an injunction.

73. If the Claimants succeed in making good the allegations they have pleaded, I think it is quite likely that the Court would grant a permanent injunction: what will have been established is a persistent campaign on the part of Rusal to gain access to the Ashton server by use of secret passwords. The Court might take some considerable persuasion that there was no risk in the future. It is not necessarily a complete answer to such an injunction that the Claimant now has improved its security. So that sort of injunction would in my view come within Part 6.20(2), although the remedy would be available without need to rely on this ground on the basis of the torts alleged.

CPR Part 6.20(3): Necessary and proper party

74. Mr Doctor submitted that, even if there was no sufficient case against Mr Deripaska and Mr Bulygin (as I have held), nevertheless they should be joined under Part 6.20(3) on the basis that they were necessary or proper parties, because they were the only persons with the authority and position to give instructions to the whole of Rusal. The injunction would be much more effective if it enjoined them as well.

75. In my view that does not make Mr Deripaska and Mr Bulygun necessary or proper parties. They have not been shown to be arguably liable to the Claimants: cf. ***Unilever Plc v. Chefaro Proprietaries Ltd***. [1994] FSR 135, 139. If the Claimants wish to bring home to them their potential liabilities should an injunction be disobeyed, this can be achieved by serving on them a copy of any order with an appropriately drawn penal notice: see White Book (2006) sc45.7.6. at p. 1974.

Forum Conveniens

76. Finally, Miss Dohmann submitted that the Claimants had failed to demonstrate that England was clearly the appropriate forum. She reminded me of the well known principles in ***Spiliada Maritime Corp v. Consulex Ltd*** [1987] AC 460. The Court should first consider the natural forum for the trial of the action – the country with which the action has the most real and substantial connection. Factors to be taken into account included convenience, expense and the proper law applicable to the dispute. Where another forum appeared to be as suitable or more suitable than England, then the Court should refuse permission, unless there were exceptional circumstances.

77. She submitted that in this case:
    i) The most natural and appropriate forum was Russia, where all the Defendants were resident and where the substance of the acts committed occurred.
    ii) The acts alleged to have been committed would give rise to civil and criminal liability in Russian law.
    iii) No adequate case had been raised as to the competence and efficacy of the Russian legal system to deal with the case.
    iv) Russia was altogether the more convenient forum.

78. In response, Mr Doctor contended:
    i) England is the obvious forum – that is where the computer system was attacked, all the Claimants' witnesses are here as are the experts. The damage was sustained here.
    ii) There is a strong connection with the TadAZ action and there is an urgency in resolving the issues in these proceedings.
    iii) Any proceedings in Russia would be difficult and cause delays.
    iv) The applicable law is English law.

79. I think the first question is whether Russia is an alternative forum for the resolution of this dispute. Expert Russian legal evidence was given on behalf of the Defendants by Colonel Anatoly Osipenko, Head of Department of the Omsk Academy of the Internal Affairs of the Russian Federation, and Gainan Avilov, Deputy Chairman of the Council of the Private Law Research Centre in Moscow. In response, evidence was filed by Professor William Elliott Butler, the John Fowler Distinguished Professor of Law at the Dickinson School of Law at Pennsylvania State University and Emeritus Professor of Comparative Law at London University. He has specialised in the legal systems of the former Soviet Union, including the Russian Federation. These witnesses were well qualified to assist the Court.

80. Colonel Osipenko explained that the acts complained of could give rise to criminal liability under Articles 183, 272 and 273 of the Russian Criminal Code. A civil claim could also be made under Article 3 of the Federal Law on Commercial Secrets of 29 July 2004 No. 98-Ф3. In cases where a civil action was based on facts which could also give rise to criminal proceedings, normally a civil action would be brought within the criminal proceedings. This would have the advantage that the burden of proof was on the State. Separate civil proceedings could however be brought without commencing criminal proceedings. They could however be stayed under Article 215 of the Russian Civil Procedure Code if it were not possible to resolve the case before the conclusion of criminal proceedings.

81. Mr Avilov considered that a civil cause of action could be brought under Article 1064 of the Civil Code which sets out general grounds for liability for causing harm to arise as a result of unlawful conduct and fault on the part of the wrongdoer. A claim might also be possible under the Law on Commercial Secrets but that rather depended on whether the information stored on the computer had been protected in accordance with the statutory regime for a

commercial secret. He confirmed the possibility of criminal proceedings and a stay. He emphasised the advantages gained by having a law enforcement body collect the evidence – they had considerably more authority.

82. Professor Butler largely concurred but he thought that criminal proceedings were rather unlikely. There were, in his view, real difficulties in pursuing civil proceedings, arising from the legal status of information, whether held on computer or otherwise, in Russian law. It was controversial whether you could "steal" information as opposed to the carrier – the paper on which it is written or the disc on which it is stored. That is why the Russian legislators introduced the Law on Commercial Secrets, but it is a cumbersome, complicated and often unrealistic regime.

83. In my view, it would be possible for the Claimants to bring civil proceedings in Russia against the Rusal Defendants, but those proceedings would not be without considerable difficulty due to the state of Russian law on the legal status of information and the technicalities of the Law on Commercial Secrets.

84. Given the availability of an alternative jurisdiction, have the Claimants clearly established that England is the proper place to bring the claim (CPR 6.21(2A)), that is that it is clearly the appropriate forum where the case can most suitably be tried for the interests of all the parties and the ends of justice? In my judgment, they have for the following reasons:

i) The unauthorised access occurred to a server that was physically situated in London. In my view that is where the tort was in substance committed and the breach of confidence occurred.

ii) There are other important connections with England. If the Rusal Defendants really did hack into the Ashton server and obtain confidential information, one inference that might be drawn fairly readily is that their principal motive was to find out about the privileged and confidential information held on the server in relation to the TadAZ proceedings to which Rusal had been joined as third party by Ansol. These proceedings are continuing in the High Court.

iii) It seems likely that, under s.11(2)(c) of the Private International Law (Miscellaneous Provisions) Act 1995,[13] the applicable law to be applied to the tort claim is English law. The most significant element of the events occurred in London – I regard the unauthorised access to the server as being by far and away the most significant element of the events which occurred. Events which occurred abroad were all directed at the server in London. The confidential information was also held in London and English law is probably the applicable law.

iv) All the Claimants' witnesses are here, as are both experts, as is Ashton's server. As against that, the Defendants' factual witnesses are in Russia as are their main computers. The Claimants' witnesses are no strangers to Russia. The comparative ease of imaging hard drives onto disc mitigates, but does not eliminate, any inconvenience caused by the fact that the Rusal Defendants' computers are in Russia. In my view overall these factors more or less cancel each other out. However, I do think it will be more expensive to have proceedings conducted in Russia rather than here, where there are extant proceedings in which London lawyers are already instructed.

v) If the Claimants had to litigate in Russia, even if they were able to establish that the Rusal Defendants had hacked into Ashton's computer in London and obtained privileged and confidential information, there would be considerable and uncertain technical Russian legal difficulties in their way.

vi) I think it is clear that any Russian proceedings would be likely to be rather slow. That is not a criticism of the Russian legal system. However, it is a highly significant factor in this case. It is vital that the present issue is resolved as soon as possible and before the TadAZ trial starts in October 2007. Either way, the result may very well have an impact on that litigation. The parties have recognised this in the consent order made by Cresswell J. on 5 May 2006, where it is recorded that, if the jurisdictional challenge fails, the parties will co-operate with the aim that this action is determined before the TadAZ trial. This Court will wish to accommodate that desire and to have an early trial of this action. There is no evidence that it would be possible to have a swift determination of this case in Russia. I have the opposite impression that the proceedings would be rather tortuous.

85. For these reasons in my judgment the *forum conveniens* for this litigation is clearly in London.

Discretion

86. In the light of all these considerations, and also drawing back to consider the justice of the position overall, I am satisfied that, as a matter of discretion, this case against the Rusal Defendants ought to proceed in this Court.

Conclusion

87. I will set aside the proceedings against Mr Deripaska and Mr Bulygin. Of course, if evidence were to arise on disclosure which implicated them personally, an application could be made to re-join them to the action.

88. The proceedings against the Rusal Defendants will continue. However, the claim in conspiracy must be re-pleaded if it is to be maintained. I will reconsider it if that occurs. Otherwise, I will set aside that claim.

89. I will hear counsel on costs and on whether any further directions should be made at this stage.

Barbara Dohmann QC, Nick Cherryman and Shaheed Fatima (instructed by Bryan Cave) for the Defendants
Brian Doctor QC and Rosalind Phelps (instructed by Clyde & Co.) for the Claimants

[13] If the claim could be categorised as in respect of damage to property, the position would be even clearer under s.11(2)(b).