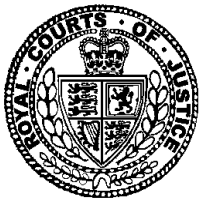

Neutral Citation Number: [2024] EWHC 1263 (Comm)

Case No: CL-2018-000226

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
COMMERCIAL COURT (KBD)

Royal Courts of Justice, Rolls Building
Fetter Lane, London, EC4A 1NL

Date: 24/05/2024

Before :

MR JUSTICE JACOBS

- -

Between :

(1) HOTEL PORTFOLIO II UK LIMITED (IN LIQUIDATION)
(2) ELIZABETH ALEXANDRA AIRD-BROWN
(as Liquidator of Hotel Portfolio II UK Limited (in Liquidation))

Claimants

- and -

(1) ANDREW JOSEPH RUHAN
(2) ANTHONY EDWARD STEVENS

Defendants

- and -

(1) PHOENIX GROUP FOUNDATION
(2) MINARDI INVESTMENTS LIMITED
(3) TANIA JANE RICHARDSON

Interested Parties

- -
- -

James Pickering KC and Samuel Hodge (instructed by **Spring Law**) for the **Claimants**
Sebastian Kokelaar (instructed by **Richard Slade and Partners LLP**) for the **2nd Defendant**

Hearing dates: 7th – 8th May 2024

- -

Approved Judgment

This judgment was handed down remotely at 9:00am on Friday 24th May 2024 by circulation to the parties or their representatives by e-mail and by release to the National Archives (see eg https://www.bailii.org/ew/cases/EWCA/Civ/2022/1169.html).

.....

MR JUSTICE JACOBS

MR JUSTICE JACOBS:

A: The parties and the application

1. This judgment concerns an application by the Second Defendant ("Mr Stevens") for an order discharging certain provisions of the order of Master McCloud dated 9 October 2023 ("the McCloud Order"). Under that order, an independent IT consultant is to make a copy of the hard drive of Mr Stevens' computer and mobile phone and search it in order to determine, amongst other things, whether it contains certain files belonging to 9 companies of which Mr Stevens was previously a director, namely Atlantic 57 Consultancy Ltd, Grenda Investments Ltd, Pascale Investments Ltd, Lenon Securities Ltd, Latimore Finance Ltd, Giotto Investments Ltd, Bluestone Securities Ltd, Grayview Overseas Ltd and Kilgore Securities Ltd ("the companies" or "the 9 companies"). All of the companies are incorporated in the BVI apart from Kilgore Securities Ltd which is incorporated in Belize. These companies are held within a trust structure called the JADES 2014 Trust ("the Jades trust").

2. The basis for the application is that the implementation of these provisions would expose Mr Stevens (and the IT consultant) to criminal liability in Italy, where Mr Stevens resides and where the computer and mobile phone are located.

3. The application is opposed by the Claimants ("HPII"). It contends that the implementation of the McCloud Order would not give rise to any real risk of a criminal prosecution in Italy. HPII also contends that compliance with the order would not in fact give rise to any criminal offence under Italian law. Even it did, HPII contends that the application should still be dismissed because it is a "dishonest ploy" designed to thwart enforcement of its judgment against Mr Stevens and therefore an abuse of the court's process.

4. The McCloud Order was made in the context of enforcement proceedings against Mr Stevens, and specifically in the context of an application under CPR Part 71 which contains rules providing for a judgment debtor to be required to attend court to provide information, for the purpose of enabling a judgment creditor to enforce a judgment or order against him.

5. Those enforcement proceedings themselves stem from a judgment of Foxton J dated 23 February 2023 following an 11-day trial: [2022] EWHC 383 (Comm). Foxton J held that Mr Stevens had dishonestly assisted in various breaches of fiduciary duty by Mr Ruhan, who was a director of HPII. Mr Ruhan had failed to disclose his interest in the sale of certain hotels by HPII in 2005. On 7 July 2022, Foxton J ordered Mr Stevens to pay HPII equitable compensation in the sum of £102.26m plus compound interest in the sum of £59.93m by 4pm on 1 August 2022. He also ordered Mr Stevens to pay HPII's costs of the proceedings with a payment on account of £2.162m to be made by the same date.

6. Mr Stevens did not make these payments. On 12 September 2022, HPII issued an application under CPR Part 71 for an order requiring Mr Stevens to attend court for questioning as to his means and to disclose documents that were, as HPII contended, relevant to enforcement of the judgment against him ("the Part 71 Proceedings"). The orders sought were made by Master Gidden on 11 October 2022. The Part 71 Proceedings are on-going. There have been multiple hearings, including three

examinations of Mr Stevens where he answered many questions, and Mr Stevens has disclosed a substantial number of documents in the course of them. The evidence given at those hearings, and the documents produced, have assisted HPII to advance aspects of its present case concerning abuse of process. This is substantially founded on an argument that Mr Stevens continues to control and is a de facto director of the 9 companies.

7. The McCloud Order was made in the course of the Part 71 Proceedings, described in more detail in Section B below.

B: Chronology of events leading to the McCloud Order and beyond

2022 – August 2023 and the order of Deputy Master Bard

8. The application for orders under Part 71 were made on 12 September 2022. On 11 October 2022, Master Gidden made Part 71 orders against Mr Stevens. He was required to attend, by video-link, for cross-examination as to his assets. He was also ordered to produce various documents.

9. HPII's application had been made without notice, and on 10 November 2022 Mr Stevens applied to set aside the orders made against him. That application was heard on 15 December 2022 by Deputy Master Kay, and was dismissed by order dated 28 December 2022. In so far as the set aside application was based on an argument that Master Gidden's order was disproportionate or oppressive, the application was certified as totally without merit. Mr Stevens' application had also sought a variation of the documents which were to be produced. This application was adjourned upon terms which included the provision by Mr Stevens of responses to certain questions. Deputy Master Kay subsequently produced a substantial written judgment, dated 28 December 2022, on the various issues raised by Mr Stevens on the set aside application (which included issues concerning service).

10. An application for permission to appeal against the orders of Deputy Master Kay was dismissed by Foxton J in trenchant terms on 17 January 2023. Amongst his reasons for refusing permission were the following:

> "…
>
> (2) However, the challenge to the alternative service order is not arguable. The question of whether the test for an alternative service order is met is context dependent (M v N [2021] EWHC 360 (Comm).
>
> (3) In this case, D2 has solicitors on the record and has participated in lengthy trial. He has been found to have acted dishonestly and assisted in a scheme to hide the ownership of assets. He has been coy before the court on previous occasions as to his address (at the Consequential Hearing in June 2022). D2 has also advanced a series of meritless objections to the CPR 71 application, which Deputy Master KC was right to conclude that "the primary purpose of the Second Defendant's

> applications … is at least to slow down if not prevent or frustrate the Claimants' endeavours to enforce the judgment".
>
> (4) Those factors provide ample grounds for the alternative service order made by Master Giddens and for Deputy Master Kay KC's refusal to set that order aside. There is simply no prospect of the court on appeal interfering with the exercise of that discretion, and the permission to appeal application can only be seen as a further attempt to frustrate or delay the enforcement process.".

11. On the same day as the hearing of the application before Deputy Master Kay, Mr Stevens resigned from 8 of the 9 companies. In early January, he resigned from the 9th company. In relation to their abuse of process arguments, HPII contended that the timing of these resignations was not coincidental. HPII argues that they were part of a ploy to frustrate enforcement of the judgment.

12. In consequence of the dismissal of the set aside application, a hearing date for the examination of Mr Stevens under Part 71 was fixed for 31 January 2023. Shortly before that hearing, which was the first of three examinations which have in fact taken place, Mr Stevens disclosed to HPII that he had resigned as a director of the 9 companies. In the case of each company, Mr Stevens had executed a "Deed of Resignation & Release". Clause 1.3 of that document was in the following terms (in the case of the deed relating to Pascale Investments Ltd):

> "Mr Stevens shall, forthwith, return to Pascale all its books and records in his possession and control and, where those books and records are in electronic form, he shall perform this obligation by providing copies of all documents in electronic form on an appropriate storage device and thereafter irretrievably removing, deleting and purging all such documents from his electronic systems."

13. Mr Stevens contends that, in accordance, with this obligation, he has indeed deleted documents from his devices. Following the first examination on 31 January 2023, Deputy Master Kay made an order on 9 February 2023. This required Mr Stevens to produce various further documents. It also required the parties' solicitors to liaise regarding potential arrangements for Mr Stevens' devices to be inspected in order see whether certain documents and files, said to have been deleted, could be retrieved. Mr Stevens gave an undertaking to preserve his devices and not to delete further files. The relevant part of the order concerning inspection of devices was as follows:

> "6. The Claimants' and the Second Defendant's solicitors shall liaise regarding arrangements (or potential arrangements) for:
>
> (1) the Second Defendant's computer, and his mobile telephone, to be examined by an independent forensic IT consultant (who is to be agreed if possible) to see if:

> (a) the documents and files said to have been deleted by the Second Defendant from his computer because of the "Deeds of Resignation & Release" (noted above) can be retrieved; and
>
> (b) in the event any Whatsapp conversations or communications between the Second Defendant and the First Defendant, or Dr Gerald Smith (from 14 February 2022 to the date of examination of the devices), have been deleted or otherwise lost, said conversations or communications can be retrieved;
>
> and
>
> (2) to the extent any such information can be retrieved: should the Second Defendant maintain a claim to privilege in respect of any such documents for whatever reason, for such documents to be privilege reviewed by a firm of independent solicitors.
>
> If no agreement can be reached between the parties about the way to proceed, the parties may seek directions from the Court on the point.
>
> 7. In the meantime, the Second Defendant shall as soon as reasonably practicable identify to the Claimants' solicitors the mobile phone(s) and computer(s) which are in his possession or control."

14. The companies then began civil proceedings in Italy. HPII contends that these proceedings were at the behest of Mr Stevens himself. On 20 March 2023, the companies issued an application for an interim injunction against Mr Stevens in the Milan court. The injunction sought to prevent Mr Stevens searching for and producing documents, and to require him to deliver up his devices to them. On 22 May 2023, the application was dismissed. The companies' appeal was dismissed on 31 July 2023. On 4 August 2023, the companies issued further proceedings in Milan against Mr Stevens, HPII, and its liquidator, seeking damages.

15. In the meantime, on 21 April 2023, Mr Stevens' second CPR Part 71 examination took place before Deputy Master Bard. It was adjourned to a later date. On 23 June 2023, Deputy Master Bard made an order consequent on the application. This order included orders for a further examination in November 2023, and for the production of various documents specified in paragraph 2 of the order. Paragraph 3 of the order is relevant to the present application and provides:

> "Without prejudice to the above paragraphs and in addition to those documents described at paragraph 6 of the Order of Deputy Master Kay KC dated 9 February 2023, by 4.00 pm on 15 September 2023, the Second Defendant's computer and mobile phone shall also be searched for documents (whether having been deleted or not) including any correspondence and electronic communications and other documents containing any of the following keywords:

> (a) "Gravity";
>
> (b) "Genii";
>
> (c) "Ikofin";
>
> (d) "Lopez";
>
> (e) "Lux";
>
> (f) "Peugeot";
>
> (g) "Lavrov"; and
>
> (h) "Vodka",
>
> for the period 1 December 2019 up until the date of the search which evidence or relate to (i) the receipts referred to at paragraphs 2(4) and 2(7) above, (ii) the payments referred to at paragraph 2(5) above, (iii) the loan referred to at paragraph 2(6) above, and/or (iv) the sale referred to at paragraph 2(8) above, but excluding any documents which set out or refer to any legal advice."

16. On 14 August 2023, HPII and Mr Stevens' solicitors agreed on a protocol, which was set out in a 3 page document. The steps set out in this protocol have not, however, been taken or completed as a result of the following developments.

17. On 29 August 2023, Mr Stevens filed a temporary stay application. This sought to stay the provisions of the order of Deputy Master Bard relating to the search of Mr Stevens' devices, pending a further hearing to determine whether those provisions should be implemented. Permission to adduce evidence on matters of Italian law was also sought. The application was supported by a witness statement of Mr Stevens' solicitor, Mr Richard Slade. That witness statement referred to the civil proceedings in Milan described above, and to possible liabilities under Italian civil law as well as criminal law. As matters have developed, Mr Stevens' argument on the present application, with which I am dealing, has been based on criminal law liabilities rather than civil law liabilities.

The decision and order of Master McCloud

18. The application for a stay came before Master McCloud on 13 September 2023. She refused to order a stay. In her ruling given orally that day she said that she was "deeply sceptical about the question of criminal liability". She considered that there had been plenty of time available for better evidence on that issue to have been adduced. She thought that there was more credibility to the case of civil liability (see below). As to how matters were then to proceed, her decision and reasoning was as follows:

> "However, I am not going to allow the court process to be completely frustrated simply because someone has issued a writ in Italy. That does not seem to me to be quite the proportionate approach. Nonetheless I do, I think, have to respect the fact that

there are some arguments here that perhaps cannot just be dismissed out of hand. What I am going to do is I am going to make a completely revised disclosure order in relation to para.3 of Master Bard's order. It is going to keep its search terms, but the storage devices that are referred to in the protocol must be forensically digitally imaged and two copies made. One copy must be lodged at the High Court where it will be kept securely and shall not be open to inspection under CPR Part 5 or by either party without further order of the court. The second copy shall be subject to a search by an independent forensic digital consultant with the second defendant having the right to have one of his own supervising. That search shall identify the locations of files or traces of files on those digital images, and that list of hits and sufficient data to locate the potential files with those hits shall be lodged at court in a digital form, and that shall be open to the parties.

When the matter returns to court next time, if so advised, argument will be heard as to the extent to which production and access to the documents which appear to be represented by those hits may or may not be given in these proceedings, and at that hearing the nine Italian companies shall have the right to be heard if so advised and may, if so advised, apply to join in and of course it goes without saying that each party may wish to apply to join those in as parties if necessary.

It seems to me that that reaches the point where nobody actually has these documents, if they still can be retrieved, or has access to them, but we do know whether there are traces suggestive of those documents existing and where they are on those drives (or whatever other media it is) which will have been imaged and kept at court so that it becomes a simple step then, if the court says "produce them" for that process to be done really very swiftly, because it is a simple question of running the necessary digital software to retrieve the files from the images. But that would be the first and only time that those files actually will have been reconstituted or accessed.

I think that is a position which, in my view, sufficiently respects what I can see from an English law perspective to be the potential interest of these nine companies, but also moves this case forward, respecting as I do the fact that Part 71 proceedings have to be got on with and that the judgment of the court must not be frustrated. Progress needs to be made next time. But it is necessarily the case that it may be necessary to have Italian law evidence and directions for that may need to be given next time or at least argument heard on the point in a more mature way next time, but it will at least be informed by some knowledge of what it is we are all talking about rather than proceedings in the dark. At least we will know whether there are hits at all. The

> second defendant is apparently accused, you know, of not having deleted these documents. We do not know whether he has. I mean, he says he has. Maybe he has. Maybe he has succeeded. It could be a flash in the pan or it may be in good faith he deleted them, but using forensic techniques it will be possible to reconstruct them, because it is incredibly difficult to delete in an absolute sense short of destroying the physical substrate of the recording medium. You can reconstruct files, as I mentioned earlier, from the indentations in the magnetic pits on the surface of the recording medium, if you really must, which is what they do in police pornography, child pornography reconstruction cases. To actually render a drive completely erasable, you have to re-write it, write it, re-write, re-write it, re-write it and keep doing it, which is tantamount to effectively destroying the disc. So it may well be that in good faith he has deleted it and maybe there are some traces. Whether that would be a breach in Italian law of the contract, we do not know. We will have some better information next time when we come to court as to whether this is something about nothing or whether there is something, and then it can be argued as to whether access to those documents, if they can be retrieved, is or is not likely to produce Italian law negative effects. That is the effect of the order I am going to make."

19. The McCloud Order was then made on 9 October 2023. This order provided as follows:

> "1. Paragraph 3 of the Bard Order is set aside.
>
> 2. By 4.00 pm on Thursday 26th of October 2023 the Second Defendant shall permit an independent IT consultant jointly engaged by the Claimants and the Second Defendants ("the Consultant") to forensically image the hard drive of the Second Defendant's computer and his mobile phone and make two copies ("the Copies").
>
> 3. As soon as reasonably practicable after making the Copies the Consultant shall provide one of them ("the Back-Up Copy") to the Second Defendant's solicitors to be held subject to the Undertaking.
>
> 4. The other copy ("the Search Copy") will be subject to a search by the Consultant ("the Search") that shall identify:
>
> (1) File types, the location of files or traces of files, or digital images of files including any correspondence and electronic communications and other documents which:
>
> i. which were said to have been deleted and contain the following keywords:
>
> "Pascale"

"Atlantic 57"

"Grenda"

"Grayview"

"Latimore"

"Lenon"

"Bluestone"

"Kilgore"

"Giotto";

ii. for the period 1 December 2019 up until the date of the search (whether having been deleted or not) and contain any of the following keywords:

"Gravity"

"Genii"

"Ikofin"

"Lopez"

"Lux"

"Peugeot"

"Lavrov"

"Vodka"

(2) File types, the location of files, traces of files, and/or digital images of files which relate to any WhatsApp conversations or communications between the Second Defendant and the First Defendant and/or Gerald Smith (from 14 February 2022 to the date of the search) that have been deleted or otherwise lost.

5. The Consultant shall prepare a list ("the List") of the results of the searches undertaken pursuant to paragraph 4 above, recording sufficient information to identify the locations and file types of any files, traces of files or digital images of files identified in the course of the Search, and provide copies of the List to the Claimants' solicitors and Second Defendant's solicitors.

6. For the avoidance of doubt, in carrying out the Search and preparing the List the Consultant shall not retrieve or access any

> of the files stored on the Search Copy nor permit any other person to do so."

20. The order also provided for a further hearing for the purpose of giving directions for the determination of any further issues arising on Mr Stevens' application, and hearing argument as to the extent to which production and access to documents identified through the search may or may not be ordered. Mr Stevens' solicitors were also required to give notice of the directions hearing to the legal representatives of the 9 companies. The companies were given permission to appear at the directions hearing and be heard on any matters before the court at that hearing. This latter order reflected something which Master McCloud had said in her ruling, namely:

> "In relation to civil, I think there is slightly more credibility there. There is clearly these release deeds that impose a duty to hand back documents and to destroy digital documents. That seems to be there in black and white. So, it is fair to say that these nine companies do, on the face of it, at least appear to have an interest of sorts. It is the sort of interest that would justify them being heard if they wished to assert what should be done in respect of protecting those interests, whether at human rights or in contract law or anything else."

The discharge application

21. On 23 October 2023, Mr Stevens filed the present application to discharge, alternatively stay, the order of Master McCloud. The basis of the application was that "its performance would expose [Mr Stevens] and the IT Consultant to criminal liability in Italy". The application also sought an interim stay pending the determination of the application, permission to call expert Italian law evidence, and a directions hearing in relation to the application. The application was supported by an expert report dated 18 October 2023, as to Italian criminal law, of Professor Fabio Fasani and Mr Marcello Elia. Professor Fasani has (as described in section D below) given evidence at the hearing of the present application to discharge or stay the McCloud Order, and the expert report has been relied upon in that context.

22. Before describing the procedural developments in relation to the discharge application, I will mention two other features of the chronology at around this time.

23. On 4 October 2023, the Court of Appeal allowed an appeal by Mr Stevens and set aside the award of equitable compensation against him: [2023] EWCA Civ 1120. Instead, it ordered him to account for the profits which he personally had made from his acts of dishonest assistance, and ordered him to pay HPII the sum of £ 1.5 million on account of his liability to account. The Court of Appeal ordered HPII to pay Mr Stevens' costs of the appeal, to be set off against the sums due from him to HPII), but otherwise left the costs orders made by Foxton J undisturbed. The Supreme Court has subsequently granted permission to appeal. Mr Stevens accepts that, following the Court of Appeal's order, he remains indebted to HPII in a sum of at least £ 3 million.

24. On 22 November 2023, Mr Stevens' third CPR Part 71 examination took place before Master Yoxall. He made an order for further production, and a further examination.

One of the matters which Master Yoxall recorded, in a "Master's Note" at the end of the order, concerned evidence which Mr Stevens had given at this third examination:

> "The Second Defendant's evidence that he had no record or ledger of monies in relation to various companies/ trusts is incredible – especially given the amounts of money passing into and out of his personal accounts".

25. Reverting now to the procedural developments in the application to discharge/ stay the McCloud Order: on 11 December 2023, HPII filed an expert report that they had obtained from Italian criminal law experts. The report was from Professor Federico Consulich and Mr Claudio Schiaffino. Professor Consulich gave evidence at the hearing before me, and again the expert report (dated 17 November 2023) has been relied upon in the context of the present application. In summary, Professor Consulich's evidence (contrary to that of Professor Fasani) is that compliance with the McCloud Order, whether inside or outside Italy, would not cause Mr Stevens or the consultant to contravene Italian criminal law.

26. The expert report was served as an exhibit to the 20th witness statement of Mr James Russell, a partner in the firm Spring Law instructed by the Claimants, HPII and its liquidator. The witness statement also went into considerable detail in relation to the procedural history of the case, the documents produced in the context of Part 71 Proceedings, and the evidence of Mr Stevens during his three examinations. This was in support of HPII's case that Mr Stevens has "at all material times, remained been interested and in control of the Companies (notwithstanding his purported resignation, and the Italian proceedings), and the Jades 2014 Trust into which the Companies were settled by Mr Stevens". This was the foundation of HPII's abuse of process argument.

27. On 31 January 2024, HPII filed an application seeking joinder of the 9 companies to the proceedings for the purposes of the Part 71 Proceedings and the discharge application, as well as applying for permission to serve out of the jurisdiction. Dias J granted permission. Her order was, however, subsequently set aside by Bright J on 12 April 2024, when Bright J also dismissed the joinder application. The companies have therefore not participated in the hearing before me.

28. On 15 February 2024, Foxton J approved a consent order. This granted an interim stay of the McCloud Order pending determination of the discharge application. It also gave directions as to the Italian law evidence. The parties were granted permission to rely on their respective experts' reports. The experts were directed to hold discussions for the purpose of identifying and narrowing the matters in dispute between them, and where possible reaching agreement on those issues. They were also directed to prepare and file a statement for the Court showing (a) those issues on which they are agreed, and (b) those issues on which they disagree and a summary of their reasons for disagreeing. Permission was also granted for further witness evidence, and this led to service of Mr Russell's 26th statement and Mr Slade's 13th statement.

29. On 2 April 2024, Mr Stevens' Italian law experts produced a second detailed report. No permission to produce such a report had been given in Foxton J's order of 15 February 2024. As at the time of the hearing before Bright J on 12 April 2024, the experts had not produced a joint report. Bright J ordered that the experts should produce a "joint statement compliant with paragraph 4 of the Foxton Order by no later than 4 pm on 26

April 2024". He declined to allow Mr Stevens' second expert report to be admitted in evidence. In the course of the hearing, Bright J emphasised that what was required was a "summary" of the experts' views:

> "What Foxton J wanted was a document, which in relation to the issues in which they disagreed, contained a, and this is the important word, "summary" of the reasons for disagreeing".

30. The experts produced their joint statement on 23 April 2024. It identified 5 issues to be addressed. Professor Consulich was faithful to both the letter and spirit of the orders of Foxton J and Bright J. The column which set out his opinion on the 5 issues contained a succinct summary of his views. Professor Fasani, in my view, disregarded both the letter and spirit of the two orders. The column containing his opinions was filled with lengthy texts and could not be called a "summary". This was, in substance and to a large extent, the further expert evidence which Bright J had declined to admit on 12 April 2024. In his written skeleton argument, Mr Pickering submitted that Professor Fasani had overloaded his statements in the joint statement, using it as an opportunity to write a full report. I agree. He also submitted that the court should in fairness disregard these entries. At the hearing, however, he did not press this latter point, and I have therefore had regard to Professor Fasani's entries on the joint statement. However, the clear disregard by Professor Fasani of the letter and spirit of the two orders is a matter to which I will return when considering his evidence.

31. On 25 April 2024, Foxton J approved a consent order giving permission to the parties' experts (one from each side) to give evidence and be cross-examined, remotely from Italy.

32. The hearing of the application took place on 7 – 8 May 2024. After brief "housekeeping", Professor Consulich and then Professor Fasani gave evidence on Day 1 by video link. Their evidence was given through an interpreter. The interpreter performed her task well, although there were times when both of the experts – who clearly had some ability to understand and speak English – indicated that a particular answer had not been interpreted quite correctly. The giving of evidence by video link through an interpreter is not particularly easy, particularly since some of counsel's questions were lengthy and complex. In considering the evidence of each witness, I have therefore considered it important to look at their evidence as a whole, rather than looking at the minutiae of any particular answer. It is fair to say that, on the critical issues on which the experts disagreed in their written reports, there was no substantial movement in the course of cross-examination.

33. Following the conclusion of the evidence, Mr Kokelaar made oral submissions on behalf of Mr Stevens, and Mr Pickering KC made oral submission on behalf of HPII. Mr Kokelaar focused his argument principally upon the Italian law evidence and its consequences, and spent comparatively little time on the abuse of process argument. In his submissions, Mr Pickering spent rather more time in explaining the procedural history and evidence which related to the abuse of process argument.

34. Mr Stevens' application was originally to discharge or stay the McCloud Order in its entirety. However, in the skeleton argument served on his behalf prior to the hearing, it was accepted that there was no basis for setting aside or staying the order insofar as it relates to the WhatsApp communications described in paragraph 4 (2) of the order. This

is because it is accepted that those communications belong not to the 9 companies, but to Mr Stevens, and so their retrieval and subsequent disclosure to HPII does not carry with it a risk of contravening Italian law. Mr Stevens contends however, that a risk of contravening Italian criminal law does arise in relation to the files described in paragraphs 4 (1) and 4 (2) of the McCloud Order. He contends that those files belong to the companies. Accordingly, the order sought on the present application is that the McCloud Order be discharged or set aside in so far as it relates to the files identified in paragraphs 4 (1) and 4 (2).

35. In this judgment, I will start by addressing the issues arising out of the Italian law evidence. I conclude (Section D below) that there is no basis, by reason of Italian criminal law or otherwise, to discharge or stay Master McCloud's order. It is therefore unnecessary to consider the abuse of process argument in detail. I will address the abuse of process arguments briefly in Section E below.

C: Legal principles

C1: Disclosure and breach of criminal law of another country

36. The decision of Henshaw J in *The Public Institution for Social Security v Muna Al-Rajaan Al Wazzan* [2023] EWHC 1065 paragraphs [43] – [51] contains a comprehensive summary of the applicable legal principles when a party contends that it should not be required to comply with a disclosure order because to do so would potentially involve an offence under the applicable criminal law of another country. The authorities have generally concerned the question of compliance with disclosure orders at the pre-trial stage, rather than (as here) the enforcement stage. However, neither party suggested that there was any material difference as to the principles to be applied. In order to avoid a very lengthy quotation – with internal sub-paragraphs, the following paragraphs substantially reproduce Henshaw J's judgment.

37. Ultimately, questions of disclosure and inspection are part of the law of procedure and are therefore matters of English law as the *lex fori* (*Bank Mellat v HM Treasury* [2019] EWCA Civ 449 paras [2] and [56]). Duties of confidentiality (which, if breached, may result in sanction) arising under foreign law do not provide an automatic basis to withhold disclosure and inspection. Whether to make an order for disclosure and production is a matter for the court's discretion: *Bank Mellat* para [16].

38. It has been stated that, whilst the English court has a discretion to excuse disclosure based on a proven actual risk of prosecution in the foreign state, "it will rarely be persuaded not to make a disclosure order on this ground" and only if the disclosing party shows that the foreign law is "regularly enforced, so that the threat to the party is real" (Matthews and Malek, *Disclosure*, 5th edn., para 8.26, quoted in *Bank Mellat* at para [62]). Neuberger J in *Morris v Banque Arabe et Internationale d'Investissement SA* [2001] ILPr 37 said:

> "Although not necessary to my decision, I agree…that the Court should normally lean in favour (probably heavily in favour) of ordering inspection, especially where a substantial number of important documents are involved. As I have mentioned, the question of discovery and inspection is obviously a question of procedure which, under

> international law, is to be determined in accordance with the lex fori." (para [73])

39. In *Morris*, the defendant French bank resisted inspection in BCCI-related proceedings on the basis that providing inspection would be a criminal offence under a blocking statute in France. Neuberger J declined to exercise his discretion to excuse disclosure (paras [68]-[74]): (i) the documents were highly material and their absence would "very substantially interfere with the liquidators' ability to pursue the case and would clearly hamper the Court's ability to try the case fairly"; (ii) the defendant had itself requested disclosure from the claimant; and (iii) even though the experts agreed that disclosure would infringe the French blocking statute (a criminal offence with penalties including up to six months' imprisonment), they were not aware of prosecutions where French companies had litigated abroad. For the French authorities to prosecute in the circumstances "would not correspond with generally accepted notions of comity".

40. Neuberger J also rejected an argument that disclosure should be sought by a letter of request under the Hague Convention, which would have created unjust delay and was not clear to succeed (paras [75]-[82]). The Court of Appeal in *Secretary of State for Health v Servier Laboratories Ltd* [2013] EWCA Civ 1234 similarly considered the "court to court" route "likely to be a slow, cumbersome and inadequate alternative" compared to a direct order between the parties (para 104).

41. Conversely, Neuberger J made clear in *Morris* that the court is not bound to order disclosure (paras [53] and [60]). Modern disclosure principles confirm that the court retains a discretion to refuse disclosure.

42. The Court of Appeal reviewed the law in *Bank Mellat*, in which it upheld an order against an Iranian bank requiring it to produce certain unredacted documents, even though doing so would breach Iranian criminal law. The court summarised the principles thus:

> "i) In respect of litigation in this jurisdiction, this Court (i.e., the English Court) has jurisdiction to order production and inspection of documents, regardless of the fact that compliance with the order would or might entail a breach of foreign criminal law in the "home" country of the party the subject of the order.
>
> ii) Orders for production and inspection are matters of procedural law, governed by the lex fori, here English law. Local rules apply; foreign law cannot be permitted to override this Court's ability to conduct proceedings here in accordance with English procedures and law.
>
> iii) Whether or not to make such an order is a matter for the discretion of this Court. An order will not lightly be made where compliance would entail a party to English litigation breaching its own (i.e., foreign) criminal law, not least with considerations of comity in mind (discussed in *Dicey, Morris and Collins*, op cit, at paras. 1-008 and following). This Court is not, however, in any sense precluded from doing so.
>
> iv) When exercising its discretion, this Court will take account of the real – in the sense of the actual – risk of prosecution in the foreign state.

> A balancing exercise must be conducted, on the one hand weighing the actual risk of prosecution in the foreign state and, on the other hand, the importance of the documents of which inspection is ordered to the fair disposal of the English proceedings. The existence of an actual risk of prosecution in the foreign state is not determinative of the balancing exercise but is a factor of which this Court would be very mindful.
>
> v) Should inspection be ordered, this Court can fashion the order to reduce or minimise the concerns under the foreign law, for example, by imposing confidentiality restrictions in respect of the documents inspected.
>
> vi) Where an order for inspection is made by this Court in such circumstances, considerations of comity may not unreasonably be expected to influence the foreign state in deciding whether or not to prosecute the foreign national for compliance with the order of this Court. Comity cuts both ways." (para [63])

43. The Court of Appeal in *Bank Mellat* held that the first instance judge (Cockerill J) had been right to exercise her discretion in the way that she did, having concluded that: (i) the "actual risk of prosecution" in Iran was more than "purely hypothetical" but "less serious" than the bank's expert had suggested noting also that, in any event, "an actual risk of prosecution of the Bank is not, ipso facto, determinative of the balancing exercise but is to be taken into account as part of it" (paras [72] and [89]); and (ii) the documents sought were needed "in the interests of the fair disposal of the trial" (paras 80-87). Equally, the judge had been entitled to order safeguards, in the form of a "confidentiality club" (paras [27], [88] and [91]-[93]).

44. Although each case turns on its own facts, the *Bank Mellat* principles were applied by Fancourt J in *Byers v Samba Financial Group* [2020] EWHC 853 (Ch), refusing to vary an order for disclosure on the basis that to comply with that order would force the respondent bank to act contrary to Saudi Arabian law, or to issue a letter of request to the Saudi Arabian authorities seeking a direction that the Saudi Arabian Monetary Authority allow the bank to give disclosure. Notwithstanding a risk of prosecution and regulatory action in Saudi Arabia, Fancourt J ordered disclosure given that the documents sought were likely to be "of the highest importance for a fair trial."

45. The *Bank Mellat* principles were also considered by Butcher J in *Tugushev v Orlov* [2021] EWHC 1514 (Comm), refusing a defendant's application to be relieved from disclosing documents that had been seized by a Russian investigator pursuing criminal proceedings in Russia, where the risk of prosecution was held to be real but not significant and the documents were centrally relevant to a fair trial of the English proceedings. Butcher J stated that:

i) the relevant question is as to the risk of prosecution:

> "It is not as to the risk of a sanction being imposed, but the question is one as to the actual risk of prosecution and not merely the question of whether the conduct which is relevant discloses a breach of foreign criminal law";

ii) the smaller or less significant the risk which the court considers that there is (even if it surmounts the threshold of being a "real risk"), the less weight it will be given in the balance; and

iii) the defendant applicant bore the burden of showing the reality of the risk of prosecution, and absence of evidence of any prosecutions in the circumstances weighed against him. (paras [32]-[38] and [49])

46. On the topic of comity, which is referenced in *Bank Mellat* in sub-paragraphs (iii) and (vi) of the above quotation. Dicey, Morris and Collins, *The Conflict of Laws* (16th ed., 2022) para 7-002 states:

> "The United [States] Supreme Court famously said in *Hilton v Guyot*, a case on the recognition of foreign judgments: "'Comity,' in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws."

47. After the above citation from Dicey, Henshaw J said the following:

> "In my view comity is capable of playing a freestanding part in the judicial decision-making process, and (contrary to a submission made by PIFSS) does not arise for consideration solely when a real risk of prosecution has been shown."

48. Mr Pickering submitted that this final sentence of Henshaw's judgment may be open to doubt. I am not persuaded that Henshaw J was wrong on this point. However, if the position is that no real risk of prosecution has been shown, then it is very unlikely that the balancing exercise would, because of comity considerations, come down against ordering disclosure.

49. In his skeleton argument in support of the application, Mr Kokelaar submitted it was sufficient, in order to discharge the McCloud Order, for the court to be satisfied on the evidence that its implementation would carry a real (i.e. not fanciful) risk of the commission of a criminal offence in Italy by Mr Stevens and the IT consultant. On this approach (for which no authority was cited), the existence or otherwise of a real risk of prosecution would be irrelevant. In the end, however, Mr Kokelaar did not pursue this line of argument, and he accepted that the applicable law was accurately stated by Henshaw J in *Public Institution*.

C2: Approach to evidence of foreign law

50. The approach to evidence of foreign law is summarised in paragraph [52] of the judgment of Henshaw J in *Public Institution*:

> "The proper approach to evidence of foreign law is well-established. In summary: (i) foreign law is a question of fact to be proved, generally, by a qualified expert in the law of the foreign country and whose

> expertise extends to the interpretation and application of the foreign law; (ii) the court will not undertake its own research but is not inhibited from using its own intelligence and common sense; (iii) where expert evidence is uncontradicted the court should be reluctant to reject it …"

D: The Italian law issues

D1: Overall conclusion

51. The case on Italian law for Mr Stevens was based on two provisions of the Italian Criminal Code, Articles 615-ter and 622. It was alleged that each of these provisions would be contravened if Mr Stevens were to comply with the McCloud Order. I address that argument in detail below, where I conclude that I am not persuaded that any offence under these articles would be committed by compliance with the McCloud Order. I consider that the evidence of Professor Consulich, that no offences would be committed, is far more persuasive.

52. However, it is not in my view even necessary to reach that stage of the argument in order to reject and dismiss the present application by Mr Stevens. There was, quite simply, no evidence in the present case of any real risk of prosecution for either of the alleged offences. There was nothing in Professor Fasani's written or oral evidence which asserted, let alone established, that there was a real risk of prosecution. Indeed neither expert had any knowledge of any actual criminal prosecutions in circumstances similar or equivalent to the present. There was no other evidence of a real risk of prosecution.

53. In my view, the complete absence of evidence of a real risk of prosecution means that the present application must fail. There is nothing which can be put into the balance to outweigh the considerations which favour compliance with the McCloud Order, which is to be seen in the context of various earlier orders for disclosure made by other KB masters who have considered this case. Those orders, taken as a whole, show the importance of document production in the context of HPII's attempts to enforce its judgment.

54. Mr Kokelaar submitted, relying on Henshaw J, that comity considerations would still be relevant and need to be considered. However, I cannot see that there are any considerations of comity which are of any significance in providing a counterweight to the factors which favour compliance with the McCloud Order. Indeed, arguments as to comity in my view vanish, for all practical purposes, in view of my conclusion below that no offence under Italian law would be committed by compliance with the McCloud Order. It is also important to remember that, as the Court of Appeal said in *Bank Mellat*, comity cuts both ways. In so far as considerations of comity do arise, particularly in the context of Article 622 discussed below, they favour compliance.

55. Mr Kokelaar also submitted, correctly, that the balancing exercise involves consideration of the importance of the documents whose disclosure is sought. I agree with that general proposition, but in my view it is unreal to suggest that the documents, which HPII seeks to obtain following compliance with the McCloud Order, are unimportant. A number of KB masters or deputy masters have made orders in the context of the Part 71 proceedings. These are designed to assist HPII in its enforcement efforts. The various court orders have been made in the context of applications which

generally have been hard fought, and also (at least in some cases) after KB deputy masters have had the opportunity to see Mr Stevens cross-examined in detail as to his assets. The various masters have been in the best possible position to assess the potential importance of the documents that HPII is seeking. Furthermore, the very hard-fought resistance to disclosure, following upon Mr Stevens' original deletion of the documents, tells its own obvious story as to the potential importance of the documents presently sought.

56. I reject Mr Kokelaar's argument in so far as it suggested that the documents are somehow of less significance because they are not being sought in order to prove a case at trial, but rather in the context of enforcement. Whilst it is true that the case-law (referred to above) has generally concerned orders for disclosure prior to trial, I do not consider that disclosure for the purposes of enforcement can be regarded as somehow less important. Indeed, it can fairly be said that they are even more important. Judgments of the court should in principle be enforced, and CPR Part 71 is an important part of the process in ensuring that a judgment which a party has fought hard to obtain does not remain unsatisfied. The importance of enforcement can be seen in other contexts: for example, it is usually easier to obtain a post-judgment freezing order than a pre-trial freezing order.

57. Accordingly, there is in my view nothing of any substance to put in the scales in favour of declining to enforce the order of Master McCloud.

58. Having reached that conclusion, I will however now address the principal issues of Italian law under Article 615-ter and 622 which. Before considering the detail, however, I will say something about the two experts.

59. In my view, Professor Consulich fully understood his role and duties as an expert, and his written and oral evidence was focused on explaining the relevant principles of Italian law including the case-law. He did so carefully and succinctly. By contrast, when I read Professor Fasani's report, and his statements in the joint report, prior to the hearing, I was concerned about a number of features of his approach. His reports contained various strong, but unsupported, statements as to what the evidence showed. For example, in his initial report, he referred to the "very serious harm that the Companies owning the confidential data would suffer as a result of their dissemination". There was, in my view, no evidence to support this statement. Similarly, he referred to the "profound business prejudice" which the companies would suffer if the confidential information was disseminated to Mr Stevens' adverse parties in the English litigation. Again, there was no evidence of such "profound business prejudice". In the joint report, as further described below, he declined to provide any views concerning the legal principles relevant to issue 5. He stated that the suggestion raised by that issue, namely that there was only a fictitious termination of the relationship between Mr Stevens and the 9 companies, was "entirely imaginative, lacking in even the slightest evidence". He declined to express any views as to the legal position concerning what he regarded as a "hypothetical scenario". For reasons briefly explained hereafter it is my view that, there was evidence, indeed reasonably substantial evidence, to support the suggestion raised in issue 5. I did not consider that it was for Professor Fasani to comment on the strength of that evidence, and still less to do so in such categoric terms. Furthermore, Professor Fasani's approach to the joint statement involved a disregard of what had been said by Foxton J and Bright J, namely that a "summary" of expert views was to be provided. Professor Fasani could see, from the

way in which Professor Consulich had approached the joint report, the way in which it should be done.

60. Despite my misgivings as to Professor Fasani's approach, I do not base my conclusions upon them. When he gave oral evidence and responded to questions in cross-examination, Professor Fasani did seek fairly to answer the questions. He accepted, at various stages, that he was not in a position to comment on certain aspects of the evidence. My overall impression was that he was seeking to assist the court in understanding of Italian law. From time to time, and in order to assist, he helped the interpreter so as to provide, what he considered to be, a better English translation of the point that he was seeking to get across. Accordingly, my conclusions on Italian law are based upon the substance of the evidence given by each of the experts on the important points, rather than upon any instinctive favourable or unfavourable view of their respective approaches.

D2: Article 615-ter

61. Article 615-ter provides as follows:

> "[I]. Anyone who unduly accesses a computer or telematic system protected by security measures or interferes with it against the wishes, implied or otherwise, of the person who has the right to exclude him shall be punished with imprisonment for up to three years."

The parties' arguments

62. The heart of the argument between the parties and their experts can be summarised as follows.

63. Professor Consulich, HPII's expert, argues that the only relevant "computer or telematic systems" relevant in the present case are the laptop computer and mobile phone of Mr Stevens. He accepted that these machines are, each, "a computer or telematic system". On the assumption that there are indeed security measures such as passwords or pin codes which protect against unauthorised access to these machines: Mr Stevens is the person, and indeed the only person, who is entitled to access those machines using the passwords or pin codes which he knows. Mr Stevens is the person who has the right to exclude others from those machines or systems. There is no evidence that anyone else (including the 9 companies) has the right to exclude Mr Stevens from his own machines. Accordingly, as and when he accesses his own machines, or data on those machines, or authorises another person to access them, he is neither "unduly" accessing a computer or telematic system nor interfering with it against the wishes of the person who has the right to exclude him. He would therefore commit no criminal offence under Article 615-ter if he were to comply with the McCloud Order.

64. Professor Fasani contends that this is too narrow an approach to Article 615-ter. He argues that the article is not confined to the case where a machine is accessed in an unauthorised way. He says (and indeed this much is common ground) that "a computer or telematic system" includes what is described in the case-law as a "virtual space". An illustration in the case-law is a "Dropbox" account which can only be accessed using passwords. But he says that it is not necessary for there to be any particular "account" for that purpose. Article 615-ter is concerned to protect the rights of a person in

confidential data which may be stored on a computer system. If, as in the present case, the owner of the confidential data (here the 9 companies) has made it clear to the owner of the computer (here Mr Stevens), that the data is confidential, and is not to be accessed, then Mr Stevens would commit an offence under Article 615-ter if he were to access the data (or authorise another person, such as the computer expert referred to in the McCloud Order) contrary to the wishes of the 9 companies. In his closing argument, and in reliance on Professor Fasani's evidence, Mr Kokelaar submitted that the relevant data in the present case was obviously located somewhere on the hard drive of the computer. The space on the hard drive which that data occupied was included in the idea of a "virtual space" described in the Supreme Court of Cassation case-law.

Discussion

65. I considered, in view of the wording of Article 615-ter, and the case law discussed below, that Professor Consulich's evidence was far more persuasive on this issue.

66. I was referred, in particular, to two decisions of the Italian Supreme Court of Cassation which explain the nature of the offence under Article 615-ter. Neither of them suggests that the offence is committed under 615-ter simply because a person accesses confidential data on that person's own computer system. It is clear from the authorities that the 615-ter offence can occur in different contexts. It can involve a person, without authority, wrongly using a machine, such as a computer or mobile telephone; for example, accessing the machine using the pin code or password in circumstances where that person had no authority to do so. Both experts were agreed, however, that the offence is not confined to wrongfully accessing a physical machine. Unsurprisingly, if an unauthorised person accesses or "hacks into" a computerised account which can only be accessed by using a password or pin code, an offence under Article 615-ter will be committed. Indeed, Professor Fasani used the word "hacking" to describe the offence committed under that section. It is of course common nowadays for people to have many different computerised accounts which can only be accessed with passwords or pin codes, including for example their online bank accounts and many other online services. These computerised accounts are regarded in Italian law as a personal "virtual space". Hacking into that virtual space does give rise to an offence under Article 615-ter.

67. The case-law shows that the offence can also be committed where the original access to the computer or the account is authorised, but the person with authorisation then exceeds the authority given by the owner of the system or virtual space.

68. In all of these cases, an offence is committed because a system (whether a machine or an account) is being used without any authority. The rationale in the cases is that the owner of the physical machine, or the account, has the right to exclude other people from his property or virtual space, or limit the terms on which access is granted. As Professor Consulich said in his oral evidence:

> "So the legislation wants to protect the owner of the digital space from third parties.
>
> …

> So this article protects the owner of the digital space and subsequently, also people that are inside the system. But this is not the meaning, this is not what that article wants. So what it says is only protects the owner of the digital space."

69. Professor Consulich disagreed when it was put to him in cross-examination that, in relation to data belonging to third parties stored on the system, it was the third party who had the right to exclude others from access to that data, and that Article 615-ter protects that right as well as the right to exclude others from the system as a whole. He said:

> "So the legislation is clear. So it says that the owner has the right of exclusion and we talk about the system, the whole system, the whole data, not the singularity"

70. A little later in cross-examination, he said:

> "We have to divide the owner of the data and the owner of the system. So we can have the owner of the system allowing third party entering the system and access the data. But you can't deny access to the data in this case. So the owner of the single file in this case, it can't prevent third party from entering the system. So – it can't prevent if a court ordered this."

71. I considered that Professor Consulich's evidence was consistent with the approach taken in the two cases in the Italian Supreme Court of Cassation to which I was referred, and that there was nothing in those cases which provided support for Professor Fasani's contrary argument.

72. Judgment 26604 of 7 June 2019 involved appeals against conviction lodged by a number of defendants. They had previously been employed by a company and by virtue of their employment had access passwords to (as described by the court) "data, information or programs contained in the computer system in use at the … company". They were convicted on the basis of circumstantial evidence that they had used these passwords to obtain the company's data for the benefit of a new company which they had created. The defendants argued on appeal that the courts below had confused the nature of the offence under Article 615-ter with another offence (described as "computer fraud") under Article 640-ter. The Supreme Court of Cassation disagreed, and held that the offence under Article 615-ter had indeed been committed. The court said:

> "Indeed, this Court (Division 5, decision number 1727 of 30/09/2008, Romano, file number 242938) has stated that the offence of unauthorised access to a computer system may occur concurrently with that of computer fraud, as the legal interests they protect and the behaviours they sanction are different. The first protects the digital domicile under the profile of "*ius excludendi alios* [right to exclude others]", including in relation to methods of access by authorised persons, while the second provides for alteration of the data stored in the system in pursuit of undue profit."

73. Accordingly, the nature of the offence is unauthorised access to a system, as Professor Consulich said. Article 615-ter provides protection for the "digital domicile" of the person who had the right to exclude others from that system. It therefore requires identification of the person who has that right, which is (as Professor Consulich's evidence indicates) the owner of that system. In the above passage, the court also refers to the "data stored in the system". This recognises that there is a distinction between the system and the data. The data is therefore described as being stored in the system. The data is not itself the computer system.

74. The judgment in case 27900 of 20 February 2023 was a longer and more detailed judgment. The defendants, Guido Bolsoni and Luigi Redolfi were two former employees of a company called Strabla owned by two brothers, Luca Strabla and Augusto Strabla. The defendants were convicted of an offence under Article 615-ter, and the conviction had been upheld by the Brescia Court of Appeal. The case arose from a change of the e-mail address associated with a Dropbox account from sts@strabla.com to gbolsoni@willsteel.it. The "willsteel" e-mail domain was that of a new company formed by the two former employees. The consequence of the change was that the Dropbox account could no longer be accessed by the managers of Strabla, when they had previously had access to at least some of the files held in that Dropbox account. The conviction, upheld by the Court of Appeal, was on the basis that actions taken by the employees "aimed at blocking the owner of the system from accessing that system – in the case in question, the Strabla brothers – is a violation of the limits imposed on third parties in possession of passwords".

75. The defendants' principal argument before the Supreme Court of Cassation was that there were insufficient grounds for rejecting their case that the "Dropbox storage space was the property of the defendants, who were its owners". They said that the space had been created by Mr Bolsoni, and Strabla could not claim that it had been prevented from using the space. In support of that argument, the defendants relied upon a number of matters, including that only Mr Bolsoni had the power to manage the Dropbox folder, and that Strabla did not know the login information and could not manage the account. They argued that they held the login details as owners of the folder, and not as "Strabla" employees, and therefore they were free to use their folder when they left the company.

76. The defendants' principal argument was accepted by the Supreme Court of Cassation, and the convictions were therefore overturned. The judgment provides, in my view, strong support for Professor Consulich's evidence as to the necessity to identify the owner of the system and thereby the individual with the right to exclude others from the system. There is again nothing in the judgment which suggests that, in that context, individual items of data stored on the system can be equated with the system itself, or indeed that it is appropriate to enquire into the ownership of those items of data.

77. In its judgment, the court explained the nature of the offence under Article 615-ter:

> "3.1. As has been observed in the legal literature and case law, the offence set out by Section 615-ter ICC comes under the category of computer offences, aimed at deterring illicit conduct with the object or instrument of information and data creation or storage systems or the automatic transfer of these. To ensure ever greater attention to the interest of confidentiality, protected under traditional criminal law by Law number 547 of 23 December 1993, the new offence outlined in

> Section 613-ter ICC was introduced, which considers the modern form of attack on or illicit interference with privacy, carried out by accessing or remaining connected to computer or telecommunications systems without authorisation, against the express or tacit wishes of the right-holder, with possible acquisition of data recorded electronically. Whether or not the offence in question is placed in the section for offences against the inviolability of the home depends, as can be seen from the report accompanying the relevant draft law, on whether computer systems are considered "an abstract extension of the area to be respected pertinent to the holder of the interest, guaranteed by article 14 of the Constitution, and the most traditional and essential aspects of which are protected in criminal law by Sections 614 and 615 ICC"."

78. The court then explained the nature of a "computer system":

> "From the outset, the case law of the supreme courts has clarified that a "computer system", according to the recurring expression used in Law number 547 of 23 December 1993, which introduced so-called "computer crimes" to the Criminal Code, is a set of devices aimed at serving any purpose useful to man, through the use (including partial use) of information technologies, which are characterised - through "coding" and "decoding" activity - by "recording" or "memorisation", via electronic impulses, on adequate storage media, of "data", i.e. of elementary representations of a fact, created using symbols (bits), in various combinations, and by the automatic creation of those data, so as to generate "information", consisting of a large or small collection of data organised according to a logic which permits them to express a particular meaning for the user. Assessment of the functioning of devices using these technologies constitutes a final decision on the facts at the cassation level when supported by adequate grounds and immune from logical errors.

79. Accordingly, in my view, the court was (as in the previous case) drawing the distinction (which to my mind is fairly obvious) between the computer system which was a "set of devices", and the data which was stored on the system or which could be generated by that system. I note in passing that a similar approach, and formulation of the legal position, can be found in another Supreme Court of Cassation case (11689 of 2007) to which Mr Kokelaar referred in his skeleton argument:

> "… a protected computer or electronic system is broken into whenever the (logical and/or physical) barriers safeguarding against access to the system's internal storage have been overcome, and therefore one is in a position to be able to refer to the data and programs contained therein … the criminal offence is consummated by merely accessing a computer or electronic system, regardless of the purpose".

80. The court (in case 27900/2023) then explained that the offence can be committed not only by a person without any authority to access a protected computer or telecommunications system, but also by persons who exceed their authority:

> "As clarified by a consolidated approach, which can already be defined in terms of "current law", the criminal offence of unauthorised access to a protected computer or telecommunications system, set out by Section 615 ter ICC, also covers the behaviour of accessing or remaining in the system not only (as is obvious on the part of someone unauthorised to access it, but also on the part of someone who, despite being authorised, violates the conditions and limits resulting from the set of rules laid down by the owner of the system to objectively delimit access thereto, or on the part of someone who puts in place operations different in essence from those for which access is permitted. For the offence to be committed, the aims and purposes which may have subjectively led to access to the system are irrelevant."

81. The court then continued (omitting internal citations):

> "The legal interest protected by the law in question is consistently identified by the case law of the supreme courts as the digital domicile, under the profile of *ius excludendi alios* [right to exclude others], also in relation to methods governing access by any authorised persons.
>
> In the reconstruction of the facts submitted for its examination, in particular, the court ruling on the merits must follow the approach indicated, in order to verify whether the accessing of or remaining in the computer system, including by someone with the right to access it, took place in compliance or against the wishes of the owner of the same system, whose wishes may be expressed explicitly or tacitly. Some applicable convictions of the Supreme Court fit into this approach. These emphasise that, for the offence in question to be committed, if a person with the login details to access it withdraws information from a confidential database, it is necessary to assert whether or not the defendant's conduct in copying/duplicating the files falls within the scope of their powers, in relation to their duties carried out within the organisation whose computer system it is, i.e. whether or not the copying and duplication fall outside the duties of the worker, going against the rules on accessing or remaining in the computer system, contained in organisational provisions imparted by the owner thereof.
>
> These principles outlined can also be seen in more recent cases, in which it is shown how the offence set out by Section 615-*ter* is carried out by virtue of the conduct of the person who, despite having authorised access and not breaking the formal rules set out by the owner of a protected computer or telecommunications system to delimit access thereto, accesses or stays in the system for reasons which are, in essence, extraneous to those for which they were given access powers.
>
> Therefore, criminal liability for that offence can be identified in the transfer, via "email", of confidential client data, from a bank employee to another employee not authorised to view said data or in the conduct of a collaborator with a law firm - only entrusted with management of a specific number of clients - who accesses the law firm's computer archives, proceeding to copy and duplicate, by transferring them onto

> other computer devices, files regarding all of the law firm's clients and, therefore, acting outside the duties with which they were entrusted.
>
> And yet again, in the case of access "*invito domino* [without the owner's consent]", carried out by using the access "passwords" known to the defendants by virtue of their previous employment relationship, of data, information and programs contained in the computer system of the company which had previously employed them, in order to divert away its clients and thereby obtain undue profit to the detriment of the aggrieved party.
>
> Finally, in reference to the psychological aspect of the offence, this is identified in the awareness and desire to access or remain in the electronic or computer system of others against the wishes of the holder of the exclusion right."

82. The above passage, in my view, supports Professor Consulich's evidence as to the significance of the owner of the system; i.e. the person with the right to exclude others.

83. The court then described the Dropbox system, and how it worked. It offered "cloud storage" and other services. The court concluded (again omitting internal citations):

> "After due consideration, it may therefore be maintained that "Dropbox", as a virtual space, used by the beneficiary of the service to collate "files" or folders containing "files", in order to facilitate access to them, view them and use them, is both a telecommunications system and, at the same time, a computer system, which contains digital documents.
>
> This has been maintained by the case law of the supreme courts, in affirming that email messages not sent by the user, but saved in the "drafts" folder of their "account" or in a virtual space for this purpose (such as Dropbox or Google Drive), only accessible by entering a username and password, constitute digital documents.
>
> It therefore seems clear (and it is also uncontested by the appellants) that the "Dropbox" service constitutes a digital domicile, the protection of which is provided for by Section 615-ter ICC.
>
> It should also be mentioned that in computer science, the term "account" indicates that set of functionalities, instruments and content attributed to a username which, in specific operating contexts, the system makes available to the user: an environment with content and functionalities that can be personalised, along with a convenient level of isolation from other parallel users."

84. In the light of this analysis, the court said that the "main question to be resolved, to assert whether or not the alleged offence in question is supported by sufficient grounds, involves identification of the persons who were entitled to exclusive access to the "Dropbox" space created by Bolsoni and by Redolfi, or to whom that virtual space belonged". In that context, it appeared decisive to "ascertain what the specific

applicable rules were governing use of the "Dropbox" space at the time of the abovementioned change" (i.e. when the previous email address was replaced with a new one):

> "In other words, it is a case of verifying, for the purpose of the decision on whether the objective aspect and psychological aspect requirements for the crime under discussion were met, whether the Dropbox" storage space belonged exclusively to the defendants, given that they created it, the use of which they temporarily granted to "Strabla" during their employment relationship, without this use reducing the power of Bolsoni and of Redolfi to amend the conditions of access to the space in question, making it belong exclusively to them; or if, on the other hand, once created, purely on the initiative of the defendants, that space became the exclusive property of "Strabla", then access by the appellants to the system to modify the account by changing the email address, to prevent it being used by "Strabla", must be considered to have been carried out for reasons, in essence, extraneous to those for which they were attributed powers to access and remain in the system; and whether, finally, the "Dropbox" space was shared between the defendants and "Strabla", by virtue of which each of these could deem themselves the holder of one *ius excludendi alios*, a shared use which, however, can no longer be considered shared after termination of their employment relationship and creation of the new company by Bolsoni and Redolfi."

85. The Supreme Court of Cassation considered that there had been insufficient consideration, by the lower courts, as to the factual position in relation to the key issue. The decision of the Brescia Court of Appeal was annulled, and the case referred back for reconsideration by another division of that court.

86. In relation to these cases, Professor Consulich said that the legal asset protected by Section 615-ter was the "IT confidentiality of the system owner". What was protected was the owner's interest in exclusive access to an IT space, regardless of the nature of the information stored, and the free availability of the same against unlawful interference by third parties. He concluded that it could not be claimed that Mr Stevens committed the offence under Article 615-ter, since he was not a third party to the system but was its owner who can therefore access the system without any restriction.

87. I considered that this analysis was convincing, and was in accordance with the Supreme Court of Cassation case-law and the wording of Section 615-ter. That section refers to a "computer or telematic system protected by security measures". It is clear from the case-law that this would cover both a physical machine which was password protected, and also a service (such as the Dropbox service considered in the 2023 case) where the "digital space" is also password protected. In either case, the offence is committed by someone who accesses the machine or the system in an unauthorised way, including a person who has initial authority to access a particular system but then exceeds the authority which has been granted by the owner.

88. In the present case, there is no evidence of any password protected "digital space" equivalent to the Dropbox account considered in the 2023 case. There is nothing in the case-law which supports the analysis that there is a protected "digital space" simply

because the data of the 9 companies occupied space on the relevant computer hard drive. In the above cases, the Supreme Court of Cassation does not equate the existence of confidential data on a system with a "computer or other telematic system" referred to in Article 615-ter. Rather, the description of a "computer system" in the judgment is upon the overall system which enables data to be recorded and stored, and there is no suggestion that data itself is a relevant computer system.

89. Furthermore, for an offence to be committed under Article 615-ter, there must be a "computer or telematic system protected by security measures". In my view, even if the companies' data itself could (contrary to my above views) be regarded as a "computer or telematic system" under Article 615-ter, there is no evidence that the data was "protected by security measures". Once Mr Stevens' computer was accessed, there was no further layer of protection, such as would exist when a person seeks to access an account such as a Dropbox account or other virtual space for which a password is required.

90. Mr Pickering argued that there was in fact no evidence that either of Mr Stevens' machines, the laptop and mobile, were protected by a password or pin code. There was force in that argument. The evidence served by Mr Stevens did not actually go so far as to state that either or both of these machines were indeed so protected. If there was no such protection on the machines themselves, then I cannot see how an offence under Article 615-ter could be committed. However, I will assume for present purposes that, despite the lack of positive evidence, the machines were both password protected, since (as Mr Kokelaar submitted) this is ordinarily the case with such machines. Even making that assumption, however, there is no basis for any argument that Mr Stevens, when accessing his own machines, would be committing an offence under Article 615-ter. He is clearly the owner of those computer systems, and he is the person who has the right to exclude others. There is no evidence that any of the 9 companies owned the machines, or that they were in a position somehow to exclude or limit Mr Stevens' access to his own machines. Even if Mr Stevens' intention, when he accessed his own machines, was to look at confidential data of the companies, or disclose it to another person, the case-law indicates that this would not amount to an offence under Article 615-ter. As the Supreme Court of Cassation said, "the aims and purposes which may have subjectively led to access to the system are irrelevant".

91. Unsurprisingly, I was referred to no case-law where a person had been convicted of an offence, under Article 615-ter, in circumstances where he had accessed his own machines, or had accessed data which was not itself contained in a virtual space which was password protected. Neither expert appeared to have heard of any case, similar to the present case, being prosecuted. I accept Professor Consulich's point that the "conduct enjoined on Mr Stevens by the English judicial authority does not appear to be in any way criminally typical under Italian law".

92. Accordingly, for the above reasons, I do not accept that compliance McCloud Order would give rise to an offence under Section 615-ter.

D3: Article 622

93. This article provides as follows:

> "[I] Anyone who, having knowledge, by reason of his status or position, or his profession or trade, of a secret, who then reveals it without just cause, or uses it for his own or another person's profit, shall be punished if the act can result in actual harm, with imprisonment for up to one year or a fine of € 30 to € 516,
>
> [II] The penalty shall be increased if the crime is committed by directors, general managers, persons responsible for preparing a company's financial statements, statutory auditors or liquidators, or if it is committed by the auditors of the company.
>
> [III] The crime shall be punishable upon legal action by the victim of the crime."

The parties' arguments

94. A number of points were made by Professor Consulich as to why compliance with the McCloud order would not involve an offence under Section 622. His principal point was that the offence of revealing secrets would only be committed if they were revealed "without just cause". Professor Consulich said that the instructions of the English court "appear to fully meet the requirement of just cause for the disclosure of confidential information". There were a number of different strands in his reasoning, as expressed in his oral and written evidence.

95. He referred to a doctrinal view that just cause would exist if the public interest in the disclosure of the secret outweighed the individual interest in secrecy. He said in cross-examination that there was here a public interest in the enforcement of justice.

96. Professor Consulich also said that the relevant legal framework for Master McCloud's order was the Brussels Regulation 1215/2012. Under Article 67 (2) of the EU-UK Withdrawal Agreement, judgments given in legal proceedings instituted before the end of the transition period (1 January 2021) remained entitled to recognition and enforcement in relation to legal proceedings commenced prior to that date. Master McCloud's order would be capable of making it lawful for any secrets to be disclosed. The order had binding legal force in Italy, and therefore Mr Stevens was obliged to comply with the order.

97. However, Professor Consulich ultimately did not consider that it was necessary for there to be an "obligation" to comply. In his written report, he said that what the crime requires is not that the disclosure is made in compliance with a legally binding order, but simply that there is a "legitimate right to do so on the part of the person bound to confidentiality". As he said in his oral evidence: just cause did not mean "that there is an obligation … but there is a reason". Here, the order of the English court was capable of placing the holder of the secret in the condition of having a legitimate right to comply with the request without fear of incurring sanctions.

98. Professor Fasani's view was that it would be hasty and simplistic simply to assume that there was just cause simply because there was compliance with orders made. He said that just cause, according to consolidated case-law, divided into two categories.

99. First, there were actual legal excuses, such as the exercise of a right or performance of a duty. However, this was of no application in the present case. Since Brexit, the rules governing mutual recognition of judgments in force among Member States were no longer applicable. The effect was that an English order, particularly an order of the present kind which did not have the nature of a decision but rather was in the nature of a search for evidence, would not be automatically binding. It would need to be subject to recognition procedures and formalities in Italy.

100. Secondly, there were situations where there was a need to protect conflicting interests, which rank higher than the one protected by the criminalising provision, within a reasonable balancing of values – provided that the means is appropriate for a lawful purpose that cannot be achieved otherwise. He said that this situation was inapplicable. The financial interests of Mr Stevens' adverse parties could not prevail over what he described as the "very serious harm that the Companies would suffer" as a result of the dissemination of their information. The requirement that the purpose could not otherwise be achieved was also not fulfilled. It would, he said, be "easy for English justice to find other instruments" to satisfy the economic claims of the claimants.

101. In cross-examination, Professor Fasani agreed that if an order, equivalent to that made by Master McCloud, had been made by a German court, then Mr Stevens in Italy would be obliged to comply with it. He was also asked whether compliance with an English court order would, but for Brexit, amount to just cause. He said that if the order could be considered binding, it would then be just cause.

Discussion

102. Here, again, I found Professor Consulich's views far more persuasive. I was not referred to any Italian case on the interpretation of "just cause" in Article 622. I was therefore not shown any case-law which indicated that the concept of "just cause" was rigidly defined.

103. It seemed to me that, as Professor Consulich said, the broad concept of "just cause" would provide a person, faced with an order of the English court and possible sanctions for contempt of court, of having "a legitimate right to comply with the request without fear of incurring sanctions".

104. Each expert did, however, identify various approaches to the concept of just cause under Italian law. Professor Consulich referred to a doctrinal view which involved considering whether the public interest in disclosure outweighed the individual interest in secrecy. As described above, Professor Fasani identified two other approaches.

105. I consider that each of the various approaches to "just cause", referred to by the two experts, would give rise to a "strong defence in the non-probable scenario of criminal proceedings based on alleged crimes pursuant to Articles 615-ter and 622 of the Criminal Code" (to use the language of Professor Consulich's response to question 4 in the joint report).

106. First, there is in my view a very strong argument that there is a public interest in (as Professor Consulich said) the enforcement of justice, and that this outweighs any individual interest in secrecy. In his submissions, Mr Kokelaar placed reliance on "comity", in relation to his argument that the English court should not enforce an order

which would involve a breach of Italian criminal law. However, as Mr Pickering submitted, comity does not simply operate in one direction in the context of the present case. Where Italian law permits a "just cause" exception, considerations of comity would point in the direction of the law recognising the need for a person to comply with orders lawfully made by a foreign court which (as in the present case) clearly had jurisdiction over Mr Stevens. This point that comity cuts both ways is also reflected in sub-paragraph (vi) in the Court of Appeal's summary of the applicable principles in *Bank Mellat* quoted above.

107. Secondly, it seems to me that Master McCloud's order is, notwithstanding Brexit, entitled to recognition and enforcement in Italy, or at least that there is a very strong argument to that effect. Professor Fasani accepted that there would be "just cause" in the case of a compliance with the order of a German court, because it would be binding. Article 67 (2) of the Agreement on the withdrawal of the United Kingdom of Great Britan and Northern Ireland from the European Union and the European Atomic Energy Community provides as follows:

> "In the United Kingdom, as well as in the Member States in situations involving the United Kingdom, the following acts or provisions shall apply as follows in respect of the recognition and enforcement of judgments, decisions, authentic instruments, court settlements and agreements:
>
> a) Regulation (EU) No 1215/2012 shall apply to the recognition and enforcement of judgments given in legal proceedings instituted before the end of the transition period, and to authentic instruments formally drawn up or registered and court settlements approved or concluded before the end of the transition period;"

108. The present legal proceedings were instituted in 2018, before the end of the transition period. I do not accept Mr Kokelaar's argument that the relevant "proceedings", for this purpose, were the Part 71 Proceedings which were only commenced after the transition period. An application under Part 71 is an application made, by application notice, within the context of existing proceedings: here, the proceedings commenced in 2018. Such an application is not the institution of new proceedings. Accordingly, the order of Master McCloud would appear to be entitled to recognition and enforcement in the same way as a German order to the same effect. Given the transitional provisions, there is therefore – in relation to just cause – no material difference between the McCloud Order and the German order described in this line of questioning.

109. Thirdly, there is also a very strong argument that this is a situation where a reasonable balancing of values results in Mr Stevens being permitted to comply with the order of Master McCloud, and without committing any offence. There has been a lawful order of the English court in a case which has long been dealt with in England, and where jurisdiction clearly exists. There is an obvious need for HPII to enforce its existing judgment, and the purpose of the order is to assist in enabling it to do so. It is owed substantial sums by Mr Stevens, and has hitherto not been paid anything even though judgment was obtained some time ago.

110. Professor Fasani submitted that it would be easy for English justice to find other instruments to satisfy the economic claims of the claimants. However, it is by no means clear to me that there are any such easy routes. I was not persuaded as to the ease of HPII being able to obtain equivalent relief by making an application to join the 9 companies for the purposes of obtaining disclosure, and the precise method by which such an application could successfully be made was not spelt out in the submissions on Mr Stevens' behalf. It seems to me that a far more straightforward and easy route is the one which HPII has initiated via the orders made by the various King's Bench masters in these proceedings, culminating in the order of Master McCloud. Professor Fasani also said that the 9 companies would suffer very serious harm if the order was complied with. However, it did not seem to me that there was any firm evidential basis for that assertion.

111. I therefore do not accept that the balancing of values would produce the result that there was, in the present case, no "just cause" on which Mr Stevens could rely, if prosecuted under Section 622.

112. Accordingly, for these reasons, I do not accept that compliance with the McCloud Order would give rise to an offence under Section 622.

113. It is not necessary for me to address the other reasons given by Professor Consulich as to why there was no offence under Section 622. Nor is it necessary to address the other arguments advanced by the parties in the context of Italian law; for example, HPII's argument that no offence would be committed if the devices were brought to England and then accessed here.

D4: Absence of real risk of prosecution – additional considerations

114. I have referred, at the outset of this section of the judgment (D1 above) to the absence of any evidence of a real risk of prosecution. My conclusions in Sections D2 and D3 above, namely that no offences under Articles 615-ter and 622 would be committed by reason of compliance with the order of Master McCloud, reinforce the conclusion that there is no real risk of prosecution in the present case. On any view, the legal difficulties in establishing the existence of any offence, and which would confront any such prosecution, mean that the prospect of any prosecution would be non-existent or at least negligible.

115. There is, however, a further point made by Professor Consulich which provides a further reason why there is no real risk of prosecution in the present case, and which also supports the above conclusion that no offences have in fact been committed.

116. The alleged offence under Article 615-ter involves the proposition that Mr Stevens commits a criminal offence by accessing documents on his own computer: a computer which he owns and to which only he has access. The alleged offence under Article 622 involves the proposition that Mr Stevens cannot access his own machine in order to obtain documents for the purposes of complying with an English court order. Leaving aside the very considerable legal difficulties in any argument that either offence would actually be committed (see D2 and D3 above), it is difficult to see how, realistically, a situation could come about where a criminal complaint against Mr Stevens was actually made to the prosecuting authorities in respect of compliance with the McCloud Order, or that the prosecuting authorities would be interested in pursuing a prosecution.

117. The alleged "victims" of the criminal wrongdoing, asserted by Mr Stevens, are the 9 companies of which he was (on his case) formerly a director. However, HPII was able to point to a variety of matters which, in my view, provide strong inferential or circumstantial evidence that Mr Stevens continues to exert control over those companies, and that he remains a de facto director of the companies.

118. That evidence was addressed in detail in the written and oral submissions of Mr Pickering. I do not consider it necessary to lengthen this judgment by discussing it in detail. However it includes the following: a significant finding of dishonesty against Mr Stevens made by Foxton J in the judgment which has given rise to the enforcement proceedings; further adverse comments, as to Mr Stevens' credibility, made in the context of the Part 71 proceedings; the absence of any coherent or convincing explanation as to why, if Foxton J's dishonesty finding was so concerning to the companies or the trustees of the trust which owned those companies that it required Mr Stevens' removal as a director, Mr Stevens would have nevertheless remained in post as a director for the best part of a year after the judgment; the fact that Mr Stevens' resignation as a director of the companies coincided with the first main contested hearing in Part 71 proceedings, when Mr Stevens sought to set aside the order of Deputy Master Gidden; the fact that, even since his resignation as a director, the documents disclosed in the Part 71 proceedings show that large sums of money were going from the trustees to Mr Stevens, and passing through his personal accounts, in order to pay the debts of the companies; the fact that this was happening even after the dishonesty finding of Foxton J, which is alleged to have been the reason for the (eventual) removal of Mr Stevens as a director of the companies; the absence of any documentary evidence which shows that anyone other than Mr Stevens is in fact taking decisions on behalf of the companies; the absence of any witness statements from any individual who alleges that he or she controls the companies, and that Mr Stevens does not; the fact that documents emanating from the Part 71 proceedings <u>against Mr Stevens</u> have been relied upon by the companies in the Italian civil proceedings; the comment by Master Yoxall, quoted above, as to the absence of any account or ledger recording the state of account between Mr Stevens and to companies or Jades 2014 Trust.

119. The strong inferential or circumstantial evidence that Mr Stevens continues to exert control over those companies, and that he remains a de facto director of the companies, has both practical and legal implications when considering whether there is a real risk of prosecution. On a practical level, it seems improbable that Mr Stevens would seek to procure that the companies, over which it appears that he continues to exert control, will actually make a complaint to the prosecuting authorities about his own conduct in complying with the order of Master McCloud. Although (albeit very shortly before the hearing of the present application), Mr Stevens provided evidence of a criminal complaint having been recently made by the companies, this was not a complaint against Mr Stevens himself but rather against the liquidator, Ms Aird-Brown.

120. Furthermore, one of the issues which the experts identified (issue 5), as a topic to be addressed in their joint report, was the following:

> "Whether there could be any effect on the above issues [principally, the legal issues concerning Articles 615-ter and 622] if there was an agreement between Mr Stevens and the 9 Companies of which Mr Stevens was director to only fictitiously terminate their relationship and

> allow those 9 Companies to take legal action in Italy for the sole purpose of allowing Mr Stevens to avoid compliance with the McCloud Order?"

121. Professor Fasani declined to address this issue, on the basis that it was hypothetical. He said in the joint report that this was a "scenario which is entirely imaginative, lacking in even the slightest evidence". For the above reasons, I disagree with Professor Fasani's conclusion as to the evidence. As already indicated, it is very surprising to find an expert opining as to the effect of the evidence on this issue at all, still less to do so in the categoric terms stated in Professor Fasani's report.

122. I also consider that Professor Fasani should have addressed the legal issue identified in this topic, at least if he was going to disagree with the opinion on the point expressed by Professor Consulich.

123. Professor Consulich did address the legal point as follows:

> "If these circumstances were proven, the conclusions surrounding the absence of criminally significant conduct would be strengthened.
>
> In truth, if Mr Stevens was still the de facto director of the nine companies which are formally against him, the consent given by these companies to the inspection and to the subsequent apprehensions of the data contained in his devices would a fortiori rule out the criminal significance of the conduct required by this High Court of Justice, insofar as he would have to be considered holder not only of the IT system to be accessed".

124. I consider that this conclusion is persuasive. Indeed, because Professor Fasani declined to address the point, there is no substantial challenge to Professor Consulich's evidence on this point.

125. I emphasise in this context that I am not in a position to reach a final conclusion as to whether or not Mr Stevens is in fact a de facto director of the 9 companies, notwithstanding his resignation. I do not consider that the nature of the present hearing – an interlocutory application without any cross-examination of Mr Stevens – is such as to enable me properly to reach a final conclusion. The significance of the present point is that it provides a further reason why there is, in the present case, no real risk of prosecution.

E: HPII's abuse of process argument

126. In view of my conclusion in Section D above, it is not necessary to consider the further argument, advanced by Mr Pickering, that Mr Stevens' application, and his resistance to the McCloud Order, is an abuse of process, and for that reason alone should be dismissed. Since Mr Stevens' application fails for the reasons set out in Section D, I will indicate what I would have likely decided if the "abuse of process" argument had been critical to the case.

127. HPII's argument was substantially founded upon the proposition that Mr Stevens remains a director of the 9 companies, and that he is the person who is orchestrating the actions of the companies in relation to the original deletion of documents/ data by Mr

Stevens, the subsequent procedural steps in the Part 71 Proceedings, and the civil actions in Italy.

128. As set out above, I accept that there is a strong case that Mr Stevens is a de facto director of the companies and is indeed orchestrating what has been happening. However, I did not think that the abuse of process arguments added anything of substance to HPII's case. If there had been a substantial case that compliance with the McCloud Order would give rise to a real risk of prosecution, such that the balancing exercise favoured a stay or discharge of that order, then I am doubtful that I would have concluded that, nevertheless, the application should fail on abuse of process grounds. If there was indeed such a real risk, then it seemed to me that this would provide a legitimate reason for Mr Stevens to resist enforcement of the order, and it is difficult to see why it would be abusive for him to do so. The mere fact that a party or person is resisting enforcement of a judgment, or orders made in the context of enforcement, does not in itself (in my view) constitute an abuse of process. Equally, the companies themselves are entitled to seek to protect their perceived interests, even if the decision as to what is in the companies' interest is being taken by Mr Stevens himself.

129. Mr Pickering also submitted that a further aspect of abuse was that the foundation of the present application was the proposition that the companies were acting independently of Mr Stevens, and that this was not in fact the case. Again, I did not consider that this argument carried matters further forward. The foundation of the present application was the argument (which I have rejected) that there would be a breach of Italian criminal law, if Mr Stevens were to comply with the McCloud Order. As Mr Kokelaar submitted, that argument was not premised on a separation between the companies and Mr Stevens.

130. Furthermore, whilst I consider that there is a strong case that Mr Stevens remains a de facto director of the 9 companies, I have not finally concluded that this is in fact the case. Even if I had reached that conclusion, I do not see that it would immediately or automatically lead to the conclusion that Mr Stevens' application was abusive. It would simply mean that I had not accepted one aspect of the factual case which was being advanced by him. It is common in litigation for aspects, including factual aspects, of a party's case to be rejected. That is inherent in the nature of litigation, where one party succeeds and the other party fails. But a case of abuse of process requires more than that.

CONCLUSION

131. Mr Stevens' application is therefore dismissed.