Neutral Citation Number: [2024] EWHC 423 (TCC)

Case No: HT-2021-000363

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

Royal Courts of Justice
Rolls Building
London, EC4A 1NL

Date: 28/02/24

Before :

Mrs Justice O'Farrell DBE

- -

Between :

IBM UNITED KINGDOM LIMITED	**Claimant**
- and -	
(1) LZLABS GmbH **(a company incorporated in Switzerland)** **(2) WINSOPIA LIMITED** **(3) LZLABS LIMITED** **(4) MARK JONATHAN CRESSWELL** **(5) THILO ROCKMANN** **(6) JOHN JAY MOORES**	**Defendants**

- -

- -

Nicholas Caddick KC & **James Weale** (instructed by **Quinn Emanuel Urquhart & Sullivan UK LLP**) for the Claimant
Roger Stewart KC & **George McDonald** (instructed by **Clifford Chance LLP**) for the Defendants

Hearing date: 16th February 2024

- -

APPROVED JUDGMENT

This judgment was handed down by the court remotely by circulation to the parties' representatives by email and released to The National Archives. The date and time for hand-down is deemed to be 28 February 2024 at 10.30am

Mrs Justice O'Farrell**:**

1. The matter before the court is the claimant's application dated 13 February 2024, seeking directions and/or guidance from the court in respect of the designation and management of confidential documents for the purposes of the trial listed to start on 29 April 2024.

Background

2. This claim arises out of the development by the first defendant ("LzLabs") of software, known as the 'Software Defined Mainframe' ("the SDM"), which is said to enable its customers to take applications developed for IBM mainframe systems and run them in their object level form on x86-based computer architectures without the need for source code changes or recompilation.

3. On 9 August 2013 the claimant licensed ICA programs to the second defendant ("Winsopia") pursuant to an IBM customer agreement ("the ICA") and subsequent agreements. On 24 February 2021 the claimant purported to terminate the licence agreements for contractual breach; alternatively at common law.

4. On 21 September 2021, the claimant issued these proceedings, in which it seeks a declaration and injunctive relief, an account of profits and/or damages.

5. The claimant's case is that the defendants breached, conspired with each other to breach, or procured the breach of, the ICA, using Winsopia's access to the IBM mainframe software to develop the SDM to run software systems without an IBM mainframe or the IBM mainframe software stack by reverse assembling, reverse compiling or reverse engineering the software.

6. The defendants dispute the claims and counterclaim injunctive declaratory relief, damages for breach of the ICA and specific performance of the same.

7. The defendants' case is that the SDM was developed by LzLabs through its own research and development. No IBM material was used, other than in compliance with the terms of the ICA and through acts of observation, study and testing, or to achieve interoperability of an independently created computer programme with other programmes, within the defendants' statutory rights.

8. The defendants also rely on defences of contractual and statutory limitation. The claimant's response is that limitation does not provide a defence in the circumstances of this case, where among other matters the relevant causes of action raise issues of dishonest conduct and/or deliberate concealment.

9. It is apparent from the pleadings that preparation for, and presentation of the parties' respective cases at, trial will include:

    i) interrogation of the source code of both IBM and LzLabs, and deconstruction of the software development process for the SDM, to ascertain whether it involved reverse assembling, reverse compiling or reverse engineering of IBM software;

ii) analysis of contemporaneous technical and non-technical communications within and between the defendants to determine whether development of the SDM was in breach of the ICA or permitted by virtue of the Copyright, Design and Patents Act 1988; and

iii) analysis of contemporaneous communications within and between the claimant, IBM Corp and customers to determine when the claimant knew, or ought to have known, of relevant matters said to give rise to an actionable claim.

Confidentiality Order

10. Given the commercial sensitivity of many of the documents, the parties agreed that a confidentiality ring would be required to facilitate disclosure in these proceedings. Following negotiation and agreement by the parties to the terms on which a confidentiality ring would be established and operated, an order dated 21 December 2022 was made by Waksman J ("the Confidentiality Order").

11. The Confidentiality Order (as amended) contains the following provisions:

> "1.1.2 'Confidential Customer Information' means:
>
> (a) any information contained or identified in any document:
>
> (i) which relates and/or refers to Source Code Information of a customer, potential customer, business partner, or third party; or
>
> (ii) which is otherwise proprietary or confidential to, and/or protected by confidentiality arrangements in place with customer, potential customer, business partner, or other third party.
>
> …
>
> 1.1.9 'Inner Confidentiality Ring Information' means:
>
> (a) documents (or any part thereof) that have been or are to be disclosed by a Party to these Proceedings and that (i) are designated by the disclosing Party as Inner Confidentiality Ring Information in writing in accordance with paragraph 7 of this Confidentiality Order, or (ii) are designated as Inner Confidentiality Ring Information by the Court; and
>
> (b) documents (or any part thereof) which contain or otherwise disclose Inner Confidentiality Ring Information falling within paragraph 1.1.9(a), above, but excluding a redacted version or copy of such a document which does not contain or otherwise disclose any such content
>
> Inner Confidentiality Ring Information shall include but shall not be limited to:

(c) all copies, extracts and complete or partial summaries of the Inner Confidentiality Ring Information, together with portions of transcripts or any Confidential Proceedings Document and exhibits or annexes that contain or otherwise disclose the Inner Confidentiality Ring Information;

(d) portions of Inner Confidentiality Ring Information filed at Court or served on another Party;

and

(e) any information, findings, data or analysis containing or otherwise disclosing the Inner Confidentiality Ring Information or the substance of the Inner Confidentiality Ring Information,

provided that in all instances set out above: (i) Inner Confidentiality Ring Information is information which by its nature is highly sensitive commercial information that is reasonably necessary and proportionate to designate as Inner Confidentiality Ring Information in accordance with the terms of this Order and (ii) the designating Party has an honest and reasonable belief as to the designation acting in good faith.

…

1.1.12 'Outer Confidentiality Ring Information' means:

(a) documents (or any part thereof) that have been or are to be disclosed by a Party to these Proceedings and that (i) are designated by the disclosing Party as Outer Confidentiality Ring Information in writing in accordance with paragraph 7 of this Confidentiality Order, or (ii) are designated as Outer Confidentiality Ring Information by the Court; and

(b) documents (or any part thereof) which contain or otherwise disclose Outer Confidentiality Ring Information falling within paragraph 1.1.12(a), above, but excluding a redacted version or copy of such a document which does not contain or otherwise disclose any such content.

Outer Confidentiality Ring Information shall include but shall not be limited to:

(c) all copies, extracts and complete or partial summaries of the Outer Confidentiality Ring Information, together with portions of transcripts or any Confidential Proceedings Document and exhibits or annexes that contain or otherwise disclose the Outer Confidentiality Ring Information;

(d) portions of Outer Confidentiality Ring Information filed at Court or served on another Party;

> (e) documents which contain special categories of personal data within the meaning of Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation); and
>
> (f) any information, findings, data or analysis containing or otherwise disclosing the Outer Confidentiality Ring Information or the substance of the Outer Confidentiality Ring Information.
>
> …
>
> 1.1.18 'Source Code Information' means:
>
> (a) any Confidential Information insofar as it consists of computer source code (whether written in a high-level language, low level-language, Assembler or other instructions) and related instructions and associated metadata;
>
> (b) Winsopia Responses; and
>
> (c) Requests sent from the First Defendant to the Second Defendant through the DR System,
>
> unless upon the agreement of the Parties or an application to the Court it is determined that some or all of the information in paragraphs (b) and (c) above should not be treated as Source Code Information.
>
> 1.1.19 'Winsopia Response' means any information sent from the Second Defendant to the First Defendant through the 'Discovery Request system' (as provided for in the Services Agreement dated 4 December 2013 between the First and Second Defendants (the "DR System")) and any attachments to a Winsopia Response (including any attachment that was sent separately from the corresponding Winsopia Response due to attachment size constraints in the DR System)."

12. Source Code Information was disclosed by the parties on purpose built and configured source code computers, to which access was strictly limited in secure rooms at Clifford Chance's offices. Source Code Information, Confidential Customer Information and Inner Confidentiality Ring Information is made available only to the Inner Confidentiality Ring members or, in the case of Source Code Information and Confidential Customer Information, a sub-set of Inner Confidentiality Ring Members.

13. Inner Confidentiality Ring members include: (i) external legal advisers, counsel and in-house lawyers who have signed a confidentiality undertaking; (ii) necessary secretarial and/or other support personnel working under supervision of such legal advisers; (iii) external testifying and non-testifying technical experts, who have signed a confidentiality undertaking; and (iv) necessary

support personnel working under the supervision of the external experts who have signed a confidentiality undertaking.

14. Outer Confidentiality Ring members include: (i) Inner Confidentiality Ring members; (ii) for each of the claimant and first to third defendants, up to two named officers who have signed a confidentiality undertaking; (iii) the fourth, fifth and sixth defendants; and (iv) necessary secretarial and/or other support personnel working under the supervision of the external legal advisers.

15. Paragraph 5.6.4 of the Confidentiality Order provides that where confidential documents are required to be included in any hearing bundle, the bundle will comprise: (i) an unredacted confidential hearing bundle for the court, external solicitors and external counsel who are Confidentiality Ring members; (ii) appropriately redacted bundles for those who are permitted to access Inner Confidentiality Ring Information or Outer Confidentiality Ring Information; and (iii) a fully redacted, non-confidential hearing bundle for use by those outside the Confidentiality Ring.

16. Paragraph 7.3 requires the parties to keep the designation of confidential documents under review and to de-designate documents as soon as reasonably practicable where appropriate.

17. Paragraph 10.8 provides that the parties shall be at liberty to apply to vary the terms of the Confidentiality Order.

18. Various amendments have been made to the Confidentiality Ring by consent or on application to the court. These included the parties' agreement to increase the number of support personnel to whom Source Code Information and Confidential Customer Information would be made available. In-house lawyers for the parties were added to the Inner Confidentiality Ring. Further, the parties agreed the addition of specified non-members who have access to certain confidential information for the purpose of considering the pleaded case.

19. The Confidentiality Order includes a procedural mechanism for disputes to be referred to the court. A number of applications have been made to the court by both parties in respect of disputes concerning the de-designation or re-designation of documents. The court has ruled on those applications based on submissions and by reference to the documents subject to challenge.

20. Neither party has sought to change the framework of the Confidentiality Order, which has governed the disclosure process to date. It is too late to re-visit the basis on which disclosure has been made, given the proximity of the trial. That does not preclude an exercise to review and revise the designation of specific documents or categories of document for the purpose of the trial. Very sensibly, the parties have commenced that process well in advance of the trial.

The Application

21. By application dated 13 February 2024, the claimant seeks an order that each party should reconsider the confidentiality designations applied to any documents in the trial bundle over which such party seeks to maintain

confidentiality restrictions at trial, in accordance with principles set out in Quinn Emanuel's letter dated 9 February 2024, subject to any modifications made by the court.

22. The principles proposed by the claimant identify categories of information that may be designated as confidential, namely: (A) Source Code Information, including IP addresses; (B) Customer Confidential Information, limited to customer names and descriptions of customers, which are sufficiently detailed to identify those customers, such as the address of the customer or name of the customer's representative; and (C) trade secrets as defined in the Trade Secrets (Enforcement etc.) Regulations 2018. It is proposed by the claimant that (D) all other information, not in categories (A), (B) or (C), may not be designated as confidential.

23. In carrying out the review, it is proposed by the claimant that regard must be had to the guidance in the practice direction 1/2024 of the Competition Appeal Tribunal Rules 2015 and set out by Cockerill J in *Aurora Cavallari & Ors v Mercedes-Benz Group AG & Ors* [2024] EWHC 190 (Comm). The guidance which the claimant seeks to incorporate includes the EU rule of thumb that documents older than five years will normally have lost their secret or confidential nature unless, exceptionally, the party relying on that nature shows that, despite its age, that information still constitutes essential elements of its commercial position or that of interested parties.

24. The defendants agree that a review of the confidentiality designation of documents should be carried out; indeed, they have already embarked on such a review of the pleadings and factual witness statements, and are producing a sample set of documents indicating their approach. However, their position is that there is no basis for re-writing the Confidentiality Order to incorporate the claimant's principles paper; any dispute should be crystallised by reference to specific documents rather than abstract principles; and the extent of the review should be by reference to documents to be referred to at trial rather than the entirety of the trial bundle.

25. They propose that the court should set a timetable for the parties to carry out a review of the pleadings and witness statements. The defendants anticipate that any disputes about the designations will be extremely limited and it is likely that they can be resolved consensually. In the event that the parties are unable to resolve any dispute as to designation, the dispute can be referred to the court for decision on the papers or at a further hearing.

Applicable legal principles

26. A comprehensive and helpful review of the relevant authorities, which I gratefully adopt, is contained in *Oneplus Technology (Shenzhen) Co, Ltd v Mitusbishi Electric Corp* [2020] EWCA Civ 1562 (CA) per Floyd LJ at [21]-[40]; *JC Bamford Excavators Limited v Manitou UK Limited* [2023] EWCA Civ 840 per Arnold LJ at [71]-[97]; and *Cavallari v Mercedes-Benz* (above) per Cockerill J at [22]-[50].

27. There is no material dispute as to the applicable legal principles in this case, which can be summarised as follows.

28. First, the principle of open justice is a fundamental aspect of English law. It demands that the public is entitled to attend court proceedings to see what is going on; to hold the judges to account for the decisions they make and to enable the public to have confidence that they are doing their job properly: *Attorney General v Leveller Magazine Ltd* [1979] AC 440 Lord Diplock at p.450; *Al Rawi & Others v The Security Service & Others* [2011] UKSC 34 per Lord Dyson at [11]; and *R (Guardian News and Media Ltd) v City of Westminster Magistrates' Court* [2012] EWCA Civ 420 per Toulson LJ at [1].

29. Second, in furtherance of the principle of open justice, the evidence and argument before the court should be made public so that the parties, the public and the media can understand the issues for determination, the evidence and legal arguments on those issues, the procedural rules applied and the basis on which the court reaches its decision. This includes the documents and their contents deployed in court during the trial.

30. Third, the principle of open justice is not absolute. An established basis for derogation from the normal rule of open justice is the protection of confidential information, where the effect of publicity would be to destroy its value or cause harm. The court has power to order that part or all of a hearing should be held in private; alternatively, to restrict access to documents adduced in evidence by an order that their confidential contents should not be recited in public. However, such powers may be exercised only where the court is satisfied that, it is necessary and proportionate to do so to protect the private rights of parties in respect of their confidential information, and it is necessary in the interests of justice: CPR 39.2.

31. Fourth, the facts of the particular case may require the court to carry out a balancing exercise, taking into account competing interests of the parties, when ordering disclosure. The general rule is that each party should have unrestricted access to relevant documents held by the other party for the purpose of the proceedings, to enable it to consider, prepare and present its case at trial. But disclosure of information and documents carries with it an inevitable invasion of privacy and confidentiality: *Riddick v Thames Board Mills Limited* [1977] QB 881 per Lord Denning at p.896. Those competing interests are particularly acute in cases such as this where the allegations concern unlawful misuse of proprietary software. Both the claimant and the defendants seek to protect their respective source code, technical secrets and customer confidential information. In managing the disclosure of such confidential information in the litigation, the court must balance the interests of the receiving party in having the fullest possible access to relevant documents against the interests of the disclosing party in the preservation of their confidential commercial and technical information.

32. For the purposes of disclosure in these proceedings, the parties agreed an appropriate and proportionate approach, balancing those competing interests, by establishing a confidentiality ring, subject to the terms of the Confidentiality Order.

33. Fifth, the designation of documents as confidential for the purpose of disclosure through the Confidentiality Ring is not conclusive for the purpose of the trial. A conservative approach to the designation of documents as confidential during disclosure may be understandable, when the extent of public knowledge and significance of the information may then not be apparent. But the court must be astute to the potential for a party to misuse the Confidentiality Ring, deliberately or inadvertently. The burden is on the party seeking to maintain the level of confidentiality designated within the Confidentiality Ring to produce clear and cogent evidence to explain and justify the same, particularly where the documents have been designated as Inner Confidentiality Ring.

34. Sixth, although CPR 31.22 provides protection against misuse of documents disclosed between the parties, it may not necessarily provide sufficient protection where documents justified as confidential and commercially sensitive are deployed in court during trial. CPR 31.22 (which remains applicable alongside PD57AD), provides:

> "(1) A party to whom a document has been disclosed may use the document only for the purpose of the proceedings in which it is disclosed, except where—
>
> (a) the document has been read to or by the court, or referred to, at a hearing which has been held in public;
>
> (b) the court gives permission; or
>
> (c) the party who disclosed the document and the person to whom the document belongs agree.
>
> (2) The court may make an order restricting or prohibiting the use of a document which has been disclosed, even where the document has been read to or by the court, or referred to, at a hearing which has been held in public."

35. I emphasise that in most cases, it is not necessary for the court to make any order restricting or prohibiting use of a document referred to in open court. Even where confidential information is referred to in open court, sufficient protection may be afforded to the affected parties by an order under CPR 31.22(2). However, such orders can be difficult to police and, once confidentiality has been breached, the information is in the public domain. The parties agree in this case that, on both sides, there is confidential information that is so commercially sensitive that it requires additional protection, through restricted access to the documents.

36. Seventh, in this case, a material factor for the court to consider is the administration of justice. The parties must be able to understand the evidence that is deployed in the case against them so that they can respond to the allegations, give instructions and follow the proceedings. The court must also have regard to the practicalities of cross-examination and oral argument based on confidential documents, and any impact on the smooth running of the trial. This is a highly technical case. It would be relatively straightforward to restrict

references to confidential technical information during argument in open court by placing them in confidential written submissions; it would be challenging to require counsel to cross-examine without referring orally to the technical detail in the documents. It may be necessary to hold parts of the trial in private but that must be kept to a minimum for the reasons set out above. The parties should endeavour to avoid these difficulties by limiting the restricted or redacted documents referred to at trial to the necessary minimum.

37. Finally, it is stressed that the appropriate order is specific to the circumstances arising in each case. The categories of confidential information are broad, ranging across private, security and commercial matters. The approach of the court in considering whether such information is so sensitive such that it demands additional protective measures during the trial will be driven by the facts of the particular case and the context in which the relevant documents are said to be material.

Approach to review

38. There have already been a number of exchanges between the parties in correspondence and in a "without prejudice" meeting. A significant degree of common ground has been reached:

    i) It is agreed that the parties should engage in a review of documents in the trial bundle to consider whether some of the documents can be de-designated as confidential.

    ii) It is agreed that the same principles, approach and exercise should apply to all parties.

    iii) It is agreed that: (a) source code and references to descriptions of source code and/or information that reveals source code or proprietary information; (b) the identities of customers; and (c) IP addresses relating to internet domains used by the parties should remain in the Inner Confidentiality Ring or as Source Code Information.

    iv) It is agreed that where confidential information appears in a document, only that part of the information that is confidential should be redacted, rather than the whole document.

39. There remain differences as to the scope of the exercise to be undertaken and whether any other principles or presumptions should apply.

Scope of the exercise

40. As to the scope of the exercise, the claimant has prepared a draft trial bundle index, which includes approximately 900 documents that have been designated as confidential. It is proposed by the claimant that the designation of all those documents should be reviewed in line with the principles set out in the attachment to the letter of 9 February 2024.

41. The defendants position is that it has already embarked on an exercise to review the confidentiality designation of the pleadings and factual witness statements. However, a review of the entirety of the trial bundle is unnecessary, given that many of the documents will not be read out, or referred to, during the course of the trial. The exercise proposed by the claimant would be very time consuming, given the number of documents, and the defendant are likely to insert additional confidential documents into the draft bundle. It is suggested by the defendants that the claimant should identify the documents to which it is likely to refer at trial and that those documents should be the focus of the review exercise.

42. The court acknowledges that the document review exercise will be time consuming. In order to be effective, the review must be carried out by experienced lawyers with an in-depth understanding of the issues in the case and the issues surrounding the appropriate designation of confidential information. It is not an exercise that should be left to inexperienced, junior members of the team; they should not be burdened with the responsibility of protecting the parties' confidential information; further, to be effective, the review requires an approach that is not over cautious.

43. The exercise can be made more manageable if the parties agree a core bundle and prioritise for review those categories of document that are perceived as significant. It is highly unlikely that all documents in the trial bundle will be referred to at trial. On the contrary, experience of trials suggests that the key documents that will be relied on by the parties in the hearing are likely to be few in number. Obvious candidates for the core bundle are the pleadings, factual witness statements and experts' reports, together with documents referred to in the same. The exercise of compiling the core bundle can start immediately. Other documents can be added to the core bundle from the main bundle as the trial progresses.

44. It would not be reasonable to require the claimant to give advance notice of the documents on which it wishes to rely at trial. In any event, it is unlikely to be in a position to give any such indication until much closer to the hearing. However, both parties should be given the opportunity to identify specific documents, or categories of documents, that should be reviewed following the initial exercise in respect of the core bundle. Thereafter, further documents or categories of document can be reviewed, as and when they are identified by any party as being documents that are likely to feature in the hearing.

Principles or presumptions

45. The legal authorities provide a useful starting point for the test that defines what amounts to confidential information. Confidential information comprises private information that is not in the public domain or accessible readily by persons other than those to whom it has been shown. It may be communicated to selected persons but in circumstances importing an obligation of confidentiality. Confidentiality is a relative and not an absolute concept; in each case, the issue must be considered in context and is fact-sensitive: *Bamford v Manitou* (above) at [37]-[42].

46. Further guidance can be found in Article 2 of the Trade Secrets Directive (effectively replicated in regulation 2 of the Trade Secrets (Enforcement etc.) Regulations 2018):

> "… 'trade secret' means information which meets all of the following requirements:
>
> (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) it has commercial value because it is secret;
>
> (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

47. The difficulty with the above definitions is that they are at a very high level of generality. Given that the documents must be considered in context on the facts of each case, although the authorities provide general guidance against which specific information can be considered, they do not provide a comprehensive set of rules for the parties to follow in this case.

48. The parties agree that source code should remain designated as Source Code Information (category A). This is already defined in the Confidentiality Order and includes computer source code (whether written in a high-level language, low level-language, Assembler or other instructions) and related instructions and associated metadata. It is also agreed that the IP addresses should be redacted from documents. There appears to be a dispute as to whether surrounding text should be treated as confidential. The answer is that it depends on the context and the content of the surrounding text.

49. There have been discussions between the parties regarding the designation of Discovery Request ("DR") documents as confidential. In the Confidentiality Order, requests and responses through the DR system are included in the definition of Source Code Information but subject to any contrary agreement by the parties or decision of the court. The defendants have reviewed some of the DRs and removed the redactions to parts of those specific examples but maintain their claim to restrict access to the information that is annexed to those DRs. The parties should arrange a meeting to discuss this as soon as possible. If they are unable to resolve the issue, it should be referred to the court for determination at the next hearing.

50. The parties agree that the identity of customers should remain designated as Inner Confidentiality Ring (category B). Customer Confidential Information is defined in the Confidentiality Order and extends beyond the customer identity. It includes information that relates or refers to source code information of a customer, proprietary or confidential information, or information which is covered by confidentiality arrangements in place. The court has already ruled

on a limited number of disputed documents in respect of this category. It is unlikely to assist for the court to proffer any additional guidance on this in the absence of specific disputed documents. As above, whether it is sufficient to redact the IP address in any particular case, depends on the context and the content of the surrounding text.

51. The delineation of category C by reference to "trade secrets" and the "short cut" issue is likely to be helpful in identifying obvious candidates for redaction but not sufficient to determine the issue in all cases. Material documents in this case are not limited to software "design" documents as such; they extend to documents that expose the process of development of the SDM, aspects of which process that the defendants seek to keep confidential. As above, whether each document falls within the definition of confidential information that is highly commercially sensitive, so as to justify redaction, depends on the context and the content of the document.

52. The default position proposed by the claimant, that all other documents are not confidential (category D), is not one that the court is prepared to order without full written and oral submissions from the parties by reference to specific documents. The court has been invited to rule upon the status of eight documents in the application bundle which the claimant contends should not be designated as confidential. However, without explanation as to the context in which the exchanges took place, the court is not in a position to determine whether the references to program or module names, or customer names should be designated as confidential.

53. The five year rule of thumb that is referred to in some of the authorities is unlikely to assist in this case. The nature of the dispute requires investigation of the SDM development process and use of IBM mainframe software over a period of more than ten years. IBM mainframe computers have been developed over decades on an iterative basis through the introduction of innovations and improved features by releases at various intervals. The claimant seeks to protect IBM mainframe software without reference to the date on which it was introduced because it is still part of its valuable confidential information. Development of the SDM started in 2011/2012 and was marketed from 2016. The defendants seek to protect LzLabs software without reference to the date on which it was introduced because it is still part of its valuable confidential information. This serves to emphasise the fact-specific nature of technical and commercially sensitive information.

Further steps

54. The exercise of review has already started and should continue as quickly as reasonably practicable, having regard to the proximity of the trial.

55. The parties should endeavour to agree a core bundle as soon as possible, at least in draft, identifying lists or categories of documents that should be subject to priority review.

56. In each case, the parties should consider whether it is essential for the document to remain confidential to protect highly sensitive confidential information; if so,

consideration must be given to whether the confidentiality can be maintained by redaction of parts of the document rather than the whole. If the document, or part of it, is to remain confidential, the parties should consider the level of confidentiality which should apply.

57. It is incumbent on the parties to give a clear and coherent explanation of any claim to retain the confidentiality designation of each document or class of documents.

58. If a party disagrees with the proposed designation of a document, that party should respond with a brief explanation of the basis on which confidentiality is disputed, so as to enable identification of any issues that arise for the court's determination.

59. Any further dispute will be considered at the PTR in March 2024.

Conclusion

60. Following hand down of this judgment, the hearing will be adjourned to a date to be fixed for the purpose of any consequential matters.