Part IVA: DISCOVERY AND INSPECTION OF ELECTRONICALLY STORED DOCUMENTS

43A. Introduction

(1) This Part provides a ~~an opt-in~~ framework for proportionate and economical ~~requests and applications for the giving of~~ discovery, ~~and~~ inspection and supply of electronic copies of electronically stored documents~~, and the supply of electronic copies of such documents~~. This Part or any portion thereof applies (a) by mutual agreement of all the parties in the cause or matter or (b) when the Court so orders, either on its own motion or on application by a party. A party that seeks to rely on this Part must cite the relevant paragraph(s) in any request or application made hereunder.

(1A) Parties should consider the application of this Part or any portion thereof in the following cases:

(a) where the claim or the counterclaim exceeds $ 1 million;

(b) where documents discoverable by a party exceeds 2,000 pages in aggregate; or

(c) where documents discoverable in the case or matter comprise substantially of electronic mail and/or electronic documents.

(1B) For the avoidance of doubt, this Part applies to pre-action discovery, discovery between parties in a pending cause or matter, and third-party discovery.

Location of electronically stored documents

(2) Electronically stored documents may reside in storage management systems, folders or directories in storage locations, electronic media or recording devices, including folders or directories where temporarily deleted files are located (for example, the Recycle Bin folder or Trash folder). Electronically stored documents or parts thereof may also reside in the unallocated file space or file slack on an electronic medium or recording device as deleted files or file fragments which may be recovered through the use of computer forensic tools or techniques.

~~*Definition*~~ *Meaning of "metadata information"*

(3) Metadata information refers to the non-visible and not readily apparent information embedded in or associated with electronically stored documents and may include both application metadata, which is created by the application software used to create the electronic documents, and system metadata, which is created by the operating or storage system. Examples of application metadata include hidden columns or text, formatting and display codes, formulae, prior edits and editorial comments; examples of system metadata include data relating to creation, modification and access of the electronic document, its size, file format and storage location, and other document profile information like title, author, subject and keywords or tags. Metadata information may be stored internally within the electronically stored document or externally in a separate file or database. Externally stored metadata information shall be discoverable as separate documents.

Meaning of "not reasonably accessible documents"

(4) Electronically stored documents which are not reasonably accessible include:

(a) deleted files or file fragments containing information which may be recovered only through the use of computer forensic tools or techniques; and

(b) ~~archived~~ documents archived using backup software and stored off-line on backup tapes or other storage media.

Meaning of "forensic inspection"

(5) A forensic inspection of an electronic medium or recording device means a reasonable search of the electronic medium or recording device for the purpose of recovering deleted electronic documents, which may extend to a forensic examination of the unallocated file space or file slack of the electronic medium or recording device using computer forensic tools and/or techniques.

43B. ~~Time to consider e~~Electronic discovery ~~issues~~ plans during general discovery

(1) Within two weeks after the close of pleadings, p~~P~~arties are encouraged to collaborate in good faith and agree on issues relating to the discovery and inspection of electronically stored documents ~~within the framework for discovery set forth in Order 24 of the Rules of Court~~. Such issues may include the scope and/or any limits on documents to be given in discovery, whether parties are prepared to make voluntary disclosures, whether specific documents or class of documents ought to be specifically preserved, search terms to be used in reasonable searches, whether preliminary searches and/or data sampling are to be conducted and the giving of discovery in stages according to an agreed schedule, as well as the format and manner in which copies of discoverable documents shall be supplied. Parties are encouraged to have regard to the list of issues at Appendix E Part 1 (Check list of issues for good faith collaboration) in their discussions. Parties should exchange their checklists prior to commencing good faith discussions.

(2) ~~Parties may, immediately after the close of pleadings, but within the time prescribed in Order 25, Rule 8(1)(a) of the Rules of Court, agree on a~~ An electronic discovery ~~protocol which~~ plan may take the form set forth in Appendix E Part 1. Parties may include the agreed electronic discovery ~~protocol~~ plan in the summons for directions. The Court shall consider the adequacy of the agreed electronic discovery ~~protocol~~ plan and may make such order or give such direction as it thinks fit, for the just, expeditious and economical disposal of the cause or matter. The agreed electronic discovery ~~protocol~~ plan, as amended by such order or direction of the Court as the case may be, shall form part of the order under the summons for directions to be extracted for the action.

(3) If parties are unable to agree on an electronic discovery ~~protocol~~ plan, the party seeking discovery of electronically stored documents ~~pursuant~~ under ~~to~~ this Part may make an application to court~~apply for an order~~. The application must include a draft electronic discovery ~~protocol~~ plan and must be supported by affidavit providing an account of the attempts made by parties~~' attempts~~ to collaborate in good faith to ~~reach agreement~~ agree on an electronic discovery ~~protocol~~ plan.

43C. ~~Requests and applications for the giving of discovery~~Discovery of metadata information

~~*Requests for discovery*~~

(1) ~~A request for discovery of any electronically stored document or class of electronically stored documents may be made before the commencement of proceedings, or at any time to any party to a cause or matter, or any person who is not a party to the proceedings.~~ Internally stored metadata information shall be discoverable as part of the electronically stored document in which it is embedded. Externally stored metadata information shall be discoverable separately from the electronically stored documents or class of electronically stored documents that it is associated with. Unless ~~the~~ a request for discovery specifies that discovery of externally stored metadata information of the requested electronically stored documents is required, the party providing discovery shall not be required to discover externally stored metadata information.

(~~4~~2) An application for discovery of externally stored metadata information of any electronically stored document or class of electronically stored documents ~~which includes externally stored metadata information~~ must be supported by an affidavit showing that a request for such externally stored metadata information ~~of the requested electronically stored document or class of electronically stored documents~~ had been made previously.

43D. Reasonable searches for electronically stored documents

(~~2~~1) A class of electronically stored documents may be described by specifying or describing a search term or phrase to be used in a ~~reasonable~~ search for electronically stored documents which shall be reasonable in scope ("reasonable search"). A request for the giving of discovery by describing a class of electronically stored documents with reference to ~~reasonable~~ search terms or phrases must specify or describe limits on the scope of the search; such limits shall include at least the following:

(a) specifying or describing custodians and repositories, eg physical or logical storage locations, media or devices; and

(b) specifying the period during which the requested electronically stored documents were created, received or modified.

(2) Subject to paragraph 43E (Proportionality and economy), requests for reasonable searches shall not extend to electronically stored documents which are not reasonably accessible unless the conditions in this paragraph are met. A party requesting a reasonable search for electronically stored documents which are not reasonably accessible must demonstrate that the relevance and materiality of the electronically stored documents justify the cost and burden of retrieving and producing them.

(3) The obligations of a party responding to a request for reasonable search for electronically stored documents is fulfilled upon that party carrying out the search to the extent stated in the request and

disclosing any electronically stored documents located as a result of that search. The party giving discovery shall not be required to review the search results for relevance.

~~(3) A request shall not be made for the discovery of deleted files or file fragments containing information which may be recovered through the use of computer forensic tools or techniques unless:~~

> ~~(a) a request is made for the discovery of the electronic medium or recording device on which a forensic inspection is to be conducted; and~~
>
> ~~(b) a request is made for inspection of the said electronic medium or recording device in compliance with paragraph 43F.~~

Applications to Court ~~for discovery~~

~~(4) An application for discovery of any electronically stored document or class of electronically stored documents which includes externally stored metadata information must be supported by an affidavit showing that a request for externally stored metadata information of the requested electronically stored document or class of electronically stored documents had been made previously.~~

(~~5~~4) An application for discovery of any electronically stored document or class of electronically stored documents which specifies or describes a search term or phrase to be used in a reasonable search for electronically stored documents must specify or describe limits on the scope of the search to be conducted.

(5) An application for discovery of any electronically stored document or class of electronically stored documents which specifies or describes a search term or phrase to be used in a reasonable search for electronically stored documents which are *not reasonably accessible* must:

> (a) specify or describe limits on the scope of the search to be conducted; and
>
> (b) be supported by an affidavit demonstrating that the relevance and materiality of the electronically stored documents sought to be discovered justify the cost and burden of retrieving and producing them.

~~(6) An application for the discovery of a computer database, electronic medium or recording device may be made together with an application for inspection of the said computer database, electronic medium or recording device in accordance with paragraph 43F.~~

~~(7) Upon the hearing of an application for an order for discovery of electronically stored documents, the Court shall have regard to the matters set forth in paragraph 43D.~~

Review for the purpose of asserting privilege

(~~6~~7) Nothing in this paragraph shall prevent the party giving discovery from reviewing the discoverable electronically stored documents or the results of any reasonable search for the purpose of identifying privileged documents. However, such review for the purpose of identifying privileged documents shall not extend to the intentional deletion, removal or alteration of metadata

information. Review for the purpose of asserting privilege must, unless otherwise agreed by parties or ordered by the Court, be concluded within fourteen (14) days after the search results are made available to the party giving discovery.

43ED. Proportionality and economy ~~Matters to which regard shall be had in determining whether discovery or inspection is necessary~~

(1) Order 24, Rules 7 and 13 of the Rules of Court state~~s~~ that an order for discovery and production of documents for inspection shall not be made unless such order is necessary either for disposing fairly of the cause or matter or for saving costs. The matters to which regard shall be had, in determining whether an application ~~for discovery or inspection (including the supply of copies) of electronically stored documents is necessary either for disposing fairly of the cause or matter or for saving costs~~under this Part is proportionate and economical, shall include:

(a) the number of electronic documents involved;

(b) the nature of the case and complexity of the issues;

(c) the value of the claim and the financial position of each party;

(d) the ease and expense of retrieval of any particular electronically stored document or class of electronically stored documents, including—

(i) the accessibility, location and likelihood of locating any relevant documents,

(ii) the costs of recovering and giving discovery and inspection, including the supply of copies, of any relevant documents,

(iii) the likelihood that any relevant documents will be materially altered in the course of recovery, or the giving of discovery or inspection; and

(e) the availability of electronically stored documents or class of electronically stored documents sought from other sources; and

(f) the ~~significance~~ relevance and materiality of any particular electronically stored document or class of electronically stored documents which are likely to be located to the issues in dispute.

43FE. Form of list

(1) The following matters shall be included in any list of documents made pursuant to the giving of discovery in accordance with this Part in which electronic documents are enumerated:

(a) the name of the electronic file constituting or containing the electronic document; and

(b) the file format ~~(and its version)~~ of the electronic document.

(2) An electronic copy of an electronically stored document which reflects that document accurately, or which has been manifestly or consistently acted on, relied upon or used as an accurate copy of that electronic document may be identified in the list of documents as an original.

(32) Where the party giving discovery objects to the production of certain discoverable electronically stored documents solely on the ground that the internally stored metadata information is protected by privilege, he must state in the list of documents whether he objects to the production of the electronic documents without the internally stored metadata information. If he does not object to the production of the electronic documents without the internally stored metadata information, he must enumerate the electronic documents in Part 1 of Schedule 1 to the list of documents. In any event, he must enumerate such documents in a separate section in Part 2 of Schedule 1 to the list of documents and shall state that he objects to the production of the whole or part of the internally stored metadata information of these documents.

(43) Reasonable efforts shall be made to remove duplicated documents from the list of documents. A document shall be considered a duplicate of another if the contents of both (including metadata information) are identical. The use of a hashing function to identify duplicates shall be deemed to be reasonable effort.

(54) If copies of electronic documents are supplied in one or more read-only optical disc(s) or other storage medium, the party giving discovery shall provide a further list, at the time when such copies are supplied, stating the following:

(a) the storage format ~~(and its version)~~ of the optical disc or storage medium; and

(b) if there are multiple optical discs or storage media, a list of electronic documents stored on each optical disc or storage medium.

(65) An index of documents enumerated in a list of documents referred to in sub-paragraph (1) or (4) above shall be provided in an electronic, text searchable and structured format. In the absence of parties' agreement, this index or load file shall be provided in a delimited text file in the Comma Separated Value (or 'CSV') file format.

43GF. Inspection of electronically stored documents

(1) A party required to produce electronically stored documents for inspection under Order 24 of the Rules of Court shall provide reasonable means and assistance for the party entitled to inspection to inspect the electronically stored documents in their native format.

(2) Where ~~an inspection is carried out under Order 24, Rule 9, 10 or 11(1) of the Rules of Court and~~ the inspecting party wishes to take copies of electronically stored documents produced for inspection, his request to take copies shall comply with the ~~protocol~~ procedures set forth in paragraph 43I(3) – (6) (Supply of copies of electronically stored documents)~~G~~.

Inspection of computer databases

(3) An inspection protocol shall be adopted by parties for inspections of computer databases, in order to ensure that the party entitled to inspection has access only to records therein that are necessary, and is not allowed to trawl through the entire computer database.

(4) An application for inspection of a computer database shall include an inspection protocol. On the hearing of an application for an order for the inspection of a computer database, the Court shall have the power to review the adequacy of the inspection protocol and may make such order or give such direction as it thinks fit for the just, expeditious and economical disposal of the cause or matter.

(5) Nothing in this paragraph shall prevent the party producing computer databases for inspection from reviewing the discoverable records or the results of any reasonable search for the purpose of identifying privileged records before such records are produced for inspection. However, such review for the purpose of identifying privileged documents shall not extend to the intentional deletion, removal or alteration of metadata information. Review for the purpose of asserting privilege must, unless otherwise ordered by the Court, be concluded within fourteen (14) days after the search results are made available to the party producing the electronic media or recording device.

43H~~FA~~. Forensic i~~I~~nspection of ~~computer databases and~~ electronic media or recording devices

(~~3~~1) No request or application for the forensic inspection of any ~~computer database,~~ electronic medium or recording device shall be made unless discovery of ~~the computer database, electronic medium or recording device~~that electronic medium or recording device has been given. A request or application for the discovery of an electronic medium or recording device may be made together with a request or application for forensic inspection of that electronic medium or recording device.

~~(4) A request may be made for the inspection of an electronic medium or recording device (for which discovery has been given) for the purpose of recovering deleted electronic documents through the conduct of a forensic examination of the unallocated file space or file slack of the electronic medium or recording device using computer forensic tools or techniques.~~

(2~~5~~) ~~Where an~~ A request or application ~~under Order 24, Rule 11(2) is made~~ for the forensic inspection of ~~computer databases,~~ electronic media or recording devices ~~for which discovery has been given, the party seeking inspection~~ shall include ~~in his application~~ an inspection protocol, which may take the form found in Appendix E Part 3 (Protocol for forensic inspection of electronic media or recording devices)~~2~~, in order to ensure that the party entitled to inspection has access only to electronic documents that are necessary, and is not allowed to trawl through ~~die entire database,~~the entire electronic media or recording device.

(3~~6~~) ~~Upon~~ On the hearing of an application for an order for the forensic inspection of ~~computer databases,~~ electronic media or recording devices, the Court shall have ~~regard to the matters set forth in paragraph 43D. The Court shall have~~ the power to review the adequacy of an inspection protocol and may make such order or give such direction as it thinks fit, for the just, expeditious and economical disposal of the cause or matter.

(47) Nothing in this paragraph shall prevent the party producing ~~computer databases,~~ electronic media or recording devices for forensic inspection from reviewing the discoverable electronically stored documents or the results of any reasonable search for the purpose of identifying privileged documents. However, such review for the purpose of identifying privileged documents shall not extend to the intentional deletion, removal or alteration of metadata information. Review for the purpose of asserting privilege must, unless otherwise ordered by the Court, be concluded within fourteen (14) days after the search results are made available to the party producing the electronic media or recording device.

43IG. Supply of copies of electronically stored documents

(1) Copies of discoverable electronically stored documents shall generally be supplied in the native format in which the requested electronic documents are ordinarily maintained and in one or more read-only optical disc(s).

(2) Metadata information internally stored in the native format of discoverable electronically stored documents shall not be intentionally deleted, removed or altered without the agreement of the parties or an order of Court. Where the party giving discovery objects to the production for inspection of certain discoverable electronically stored documents solely on the ground that the internally stored metadata information is protected by privilege, but does not object to the production of the electronic documents without the internally stored metadata information, copies of such documents may be supplied in a reasonably usable format with all or such of the metadata information over which privilege is claimed removed.

Requests for the supply of copies

(3) A request for copies of discoverable electronically stored documents may specify the format and manner in which such copies are to be supplied, If the party giving discovery does not agree with the specified format or manner or both, he may either:

> (a) propose a reasonably usable format and/or storage medium and/or a reasonable manner in which he intends to supply copies of the requested electronic documents; or
>
> (b) in default of agreement, supply copies of the requested electronic documents in accordance with sub-paragraph (1).

(4) The party giving discovery shall not be required to supply copies of electronically stored documents in more than one format.

(5) The file formats ~~versions~~ set forth in Appendix E Part 4 (Reasonably usable formats)~~3~~ shall be deemed to be reasonably usable formats for the purpose of this paragraph.

Applications for the supply of copies

(6) Applications for the supply of copies of discoverable electronically stored documents shall specify the format and manner in which copies of such electronic documents are to be supplied.

43J. Discovery by the supply of copies *in lieu* of inspection

(1) Where the use of technology in the management of documents and conduct of the proceeding will facilitate the just, expeditious and economical disposal of the cause or matter, the Court may order, on its own motion or on application by a party, that discovery be given by the supply of electronic copies of discoverable electronically stored documents *in lieu* of inspection.

(2) An order for discovery made under this paragraph may take the following form:

(a) Discovery of electronic mail and electronically stored documents which are in the parties' possession, power or custody be given by providing electronic copies in native format or one of the reasonably usable formats set forth in the Supreme Court Practice Directions, Appendix E Part 4 (Reasonably usable formats);

(b) Electronic mail in Microsoft Outlook or Lotus Notes be provided in Personal Storage Table (PST) or Notes Storage Format (NSF), as the case may be, with all attachments intact, and that the electronic mail from each custodian be supplied in a single PST or NSF file;

(c) Electronic copies of discoverable electronically stored documents be supplied using one or more read-only optical disc(s), unless parties agree to an alternative storage medium (eg, removable flash storage or hard disks) or manner (eg, online folders or directories);

(d) Discoverable electronically stored documents are to be organised into meaningful categories and copies of all electronically stored documents in each category are to be stored in a separate folder or directory in the optical disc or storage medium, and further, for sub-categories to be organised as sub-folders or -directories;

(d) Enumeration of electronically stored documents in the list of documents is to be dispensed with, but a meaningful description is to be provided for each category or sub-category in the list of documents instead;

(e) All documents in the parties' possession, power or custody that are in printed or paper form are to be digitised and processed using Optical Character Recognition (OCR) software programs to render the digitised documents searchable, and further, electronic copies are to be supplied in Portable Document Format (PDF) or in any other reasonably usable format (as parties may agree) in accordance with the terms of this Order;

(f) Parties are to exchange electronic copies of discoverable documents together with a list of documents in accordance with paragraph 43F (Form of list)of Part IVA of the Supreme Court Practice Directions, as modified by this Order, within fourteen days of this Order;

(g) Inspection be deferred and that Order 24, Rule 10 applies to the list of documents ~~and~~ as though it was a pleading or an affidavit; and

(h) The time for objections under Order 27 be ordered to run from the date of exchange of electronic copies in paragraph (f) herein or the date of inspection, if any, whichever is the later.

(3) For the avoidance of doubt, nothing in this paragraph requires parties to agree to adopt an electronic discovery plan or conduct reasonable searches for electronically stored documents under this Part. An order may be made under this paragraph in proceedings where parties have identified discoverable documents pursuant to the procedure set out in Order 24 of the Rules of Court.

43K~~H~~. Restriction on use of privileged document, inspection of which has been inadvertently allowed

(1) Order 24, Rule 19 of the Rules of Court applies to the giving of discovery or inspection of electronically stored documents, including the supply of copies, as it would to the giving of discovery or inspection of any other document.

43L~~I~~. Costs

(1) ~~Except~~ Save for orders made in respect of third party or pre-action discovery, the costs of complying with an order for ~~the giving of~~ discovery or inspection of electronically stored documents shall generally be borne by the party giving discovery; and disbursements incurred in providing copies shall be reimbursed by the party requesting for copies.

(2) The Court may invoke its inherent powers under Order 92, Rules 4 and 5 of the Rules of Court ~~to make or give such further orders or directions incidental or consequential to any order as may be necessary,~~ to order the party entitled to discovery to bear the whole or ~~a portion~~ part of the costs of compliance with ~~such~~ an order for ~~the giving of~~ discovery or inspection of electronically stored documents~~, and the supply of copies~~, if such order is necessary to prevent injustice or to prevent an abuse of the process of the Court.

APPENDIX E PART 1

CHECK LIST OF ISSUES FOR GOOD FAITH COLLABORATION

Where electronic discovery and inspection is contemplated, parties should discuss and consider, with a view to agreeing to as much as possible, the aspects relating to electronic discovery and inspection, including the following:

1. Scope of reasonable search

(a) Who are the custodians of documents that have to be discovered?

Typically, the custodians will eventually be called as witnesses in the trial. The key witnesses are also likely to be the custodians of key documents.

(b) The physical locations where the documents and any reasonable searches will be conducted.

Identify the computing equipment, communication and storage devices, etc for each custodian. Examples include personal and notebook computers, tablets, mobile phones, removable storage devices like flash drives and external hard disks, external storage media like optical discs, cloud-based storage, etc. Parties should be aware that there may be centralised online or networked storage locations which may be accessible by the custodians.

Consider the amount of printed documents that will be disclosed during discovery. Discuss whether printed documents should be digitised, and if so, whether the digitised electronic copies should be subjected to text-conversion using Optical Character Recognition (OCR) software to facilitate searching. Documents with typewritten text will undergo OCR conversion with a higher degree of accuracy than documents containing handwritten text and drawings.

(c) The precise date range of requested documents, including the period during which the requested documents were created, modified, and/or sent ~~received~~, if necessary.

(d) The specific categories of documents sought to be disclosed.

For example, electronic mail, instant messages, Short Message Text messages, web-based electronic mail, etc.

(e) The use of agreed search terms and/or phrases.

Discuss the keywords to be used with reference to the issues in dispute and pleadings. Try to avoid common words which will result in many hits. It is useful to consider the following categories of search terms and/or phrases:

(i) names, nick names and e-mail addresses of key witnesses or custodians;

(ii) search terms and/or phrases derived from the names of projects or products;

(iii) search terms and/or phrases derived from significant events, eg date or location of a key meeting or discussion,

Be familiar with the search engine that will be used and explore the use of search operators (eg proximity searches).

2. Use of software tools to facilitate searches and to save costs

(a) The use of search engines and the preparation of the search engine.

If each party is using a different search engine, to agree on steps to minimise discrepancies in search results. For example, preparation of a fresh index of the search engine.

Documents which are image files (these include image-based PDF files) and which have not undergone text conversion using OCR software will not be searchable. Similarly, electronic documents which are password protected or encrypted may not be indexed by the search engine and hence may not be searchable.

Parties should also be aware of the foreign language capabilities of the search engine that will be used and be familiar with the amount of electronic documents which are in different languages.

(b) The use of de-duplicating software, and/or the methods used to identify duplicate documents.

(c) The format(s) of documents which parties accept for the purposes of the discovery.

Document review software platforms are able to produce a set of discoverable documents in PDF or TIFF documents or, increasingly, in native format. Production in native format is preferred. If production is in PDF or TIFF formats, the original electronic documents in native format should remain available for inspection, if necessary.

(c) Review of search results

Where search terms are used, the search results are deemed to be relevant and discoverable subject to review for the purpose of identifying privileged documents. Parties **should not** expend additional time, effort and resources to review search results for relevance.

3. Privilege review and redaction of privileged material

(a) The methods to be used to identify privileged documents and other non-discoverable documents.

Search terms may be considered to identify potentially privileged documents for the privilege review. For example, the email addresses of solicitors, the law firm's file reference number, "without prejudice", "legal privilege", "legal advice privilege", "litigation privilege", etc.

(b) The methods used to redact documents, where required.

Where legible parts of documents are to be redacted, the redacted document can be provided in PDF or TIFF format. Where internal metadata is to be redacted, the redacted documents can be provided as a new version (without the metadata) in native format or in PDF or TIFF format.

4. Preliminary searches, data sampling or discovery in stages

(a) Conducting preliminary searches on the agreed repositories using the agreed search terms and limits.

Preliminary searches are conducted after parties have agreed on the repositories and also the limits (eg time periods). The agreed search terms are used to run a search in order to identify whether there are some search terms that will lead to little or no hits and whether there are those search terms that will lead to too many hits. This does not entail either party viewing the contents of documents in the search results (at least not the full contents, perhaps highlights of documents if the search engine supports this function). This in intended to assist parties in discarding search terms with little or no hits and to refine the search parameters and/or operators for search terms that turn up too many hits.

(b) The use of data sampling methods to test the suggested search terms.

Data sampling requires that parties agree to a sample of documents, which is ideally representative of the documents which will eventually be given during discovery. A sample may be, for example, selected electronic mail and softcopy folders of a key custodian. A reasonable search is conducted and the documents in the search results reviewed. This is intended to assist parties arrive at a useful set of search terms for the actual reasonable search. Safeguards to preserve privilege will have to be agreed by parties. As this method is resource intensive, parties should agree to limit the number of times data sampling is used to test the efficacy of search terms.

(c) The use of a staged approach in the discovery of electronic documents, if appropriate.

In staged discovery, parties agree to discover documents from the repositories of key custodians or witnesses initially. After reviewing the documents, they may then agree to proceed to discovery of other custodians or witnesses, or they may agree that the initial stage is sufficient for general discovery and proceed with specific or further discovery. Staged discovery is useful if there are a few key custodians who have the majority of the relevant and material documents in the repositories under their possession, power or control.

5. Inspection and provision of copies

(a) The place of inspection of the documents.

For inspection of electronic document which require proprietary or obsolete computing equipment (including software programs), the place for inspection may be the client organisation's premises where the electronic documents are accessible.

(b) The manner of inspection of the documents.

Inspection may be carried out by an operator who will retrieve each document that is to be inspected, and display it on the display panel. He will then manipulate the document on the screen at the request of the party entitled to inspection. Parties may also need to consider a protocol that will allow the solicitors for the party giving discovery to prevent disclosure of privileged information (including metadata), where relevant.

(c) The supply of copies of documents, if any, and the format and manner in which the copies will be supplied.

Apart from optical discs, parties may discuss supply of copies on removable hard disks, flash drives, online storage folders, etc.

6. Production of non-reasonably accessible documents and metadata

(a) Whether production of deleted documents which are recoverable only with forensic techniques is necessary and proportionate.

(b) Whether production of ~~archival~~ data archived using backup software and stored off-line on backup tapes or other storage media ~~stored offline~~ is ~~necessary and~~ proportionate and economical.

(d) Whether metadata is stored externally, and if so, whether production of externally stored metadata is necessary.

7. Appointment of computer experts for inspection and/or forensic examination

(a) The appointment of a joint computer expert for the acquisition of the Original Acquired Image where there is to be forensic inspection of electronic medium or recording devices.

(b) Whether the joint computer expert will also be appointed to carry out the reasonable search on the electronic medium or recording device, or parties will appoint their own computer expert to carry out the reasonable search.

(c) The costs of and incidental to the conduct of the search, including the costs of appointment of any joint experts.

APPENDIX E PART ~~1~~2

AGREED ELECTRONIC DISCOVERY ~~PROTOCOL~~PLAN

1. Scope of electronic discovery

(a) General discovery of the following class or classes of electronically stored documents shall be given:

[eg for each custodian, the repositories to be identified as well as the classes of electronically stored documents – e~~E~~lectronic mail, correspondence, letters, etc.]

(b) The party giving discovery shall take reasonable steps to decrypt encrypted files or encrypted storage locations, media or devices in order to identify discoverable electronically stored documents. This may include taking reasonable steps to obtain the decryption code and/or using reasonable technical means to perform decryption of the encrypted files or encrypted storage locations, media or devices.

(c) For the avoidance of doubt, electronically stored documents residing in folders or directories in storage locations, media or devices, including folders or directories where temporarily deleted files are located (for example the Recycle Bin folder or Trash folder) are within the scope of general discovery~~;~~. Electronically stored documents that are (i) not reasonably accessible, for example deleted files or file fragments containing information which are recoverable through the use of computer forensic tools or techniques during a forensic inspection of the unallocated file space or file slack, (ii) files and folders which are not known to the party giving discovery to be hidden in the file system, and (iii) ~~archived~~ documents archived using backup software and stored off-line on backup tapes or other storage media are **not** within the scope of general discovery.

(d) **Reasonable search.** The search terms or phrases specified in the first column will be used in the conduct of a reasonable search for relevant electronically stored documents. The reasonable search will be limited by the scope described in the second column.

Search term or phrase	*Scope*
[Specify the keyword(s).]	[Describe the scope of the search by reference to custodian and repository, eg physical or logical storage locations, media or devices, the period during which the requested electronically stored document was created, modified or received, etc.]

(e) **Preliminary search.** A preliminary search of the repositories identified in sub-paragraph (d) above is to be conducted forthwith. Such preliminary search is limited to providing information relating to the number of hits and/or the number of documents containing the keywords. Parties shall review the search results within two (2) days of being provided with the same; and within a further five (5) days, parties shall meet to discuss whether the keywords and/or the repositories identified in sub-paragraph (d) above need to be revised. Parties agree to abandon any keywords with no hits and to review any keywords with hits exceeding [*insert a*

figure, eg *10,000*] for the purpose of constraining the keywords. Unless mutually agreed, no new keywords may be introduced following the performance of the preliminary search.

(f) **Data sampling.** Parties agree to perform a reasonable search of the following repositories in sub-paragraph (d) above: [*insert a sample of the custodians and repositories by referencing the table in sub-paragraph (d)*]. Parties shall review the search results within seven (7) days of being provided with the same; and within a further seven (7) days, parties shall meet to discuss whether the keywords and/or the repositories identified in sub-paragraph (d) above need to be revised. Data sampling in accordance with the terms of this sub-paragraph shall be performed no more than twice.

(g) **No review for relevance.** Subject to paragraph 3 (Review for privileged material) below, each party's obligation to conduct a reasonable search is fulfilled upon that party carrying out the search to the extent agreed in this plan; the party giving discovery shall not be required to review the search results for relevance.

2. Format of list

The list of documents shall categorise and list electronically stored documents separately from documents in printed or other form. The list of documents enumerating electronically stored documents shall include the following columns: [*contents of table for illustration*]

Description of electronically stored document	**File name & location**	**File format**
Contract for sale and purchase of 123 Blackacre Heights Singapore 234123	//Contract Documents/Contract_Sale_Purchase_123_Blackacre_Heights.doc	Adobe Acrobat
Excel spreadsheet showing rental income and outgoings on 123 Blackacre Heights Singapore 234123	//Income Documents/Rental_Outgoings_Tabulation.xls	Microsoft Office Excel 2007
E-mails from Christopher Tan's e-mail account "chris.tan@realter.com.sg" in relation to 123 Blackacre Heights Singapore 234123 for the period 1 January 2010 to 31 December 2010.	//Correspondence/Thomas Liew.pst	Microsoft Outlook PST

~~[eg description of the electronically stored document, the name of the corresponding soft copy file, the file format version of the electronic document, the hash value of the file, *etc*]~~

An index of documents enumerated in the list of documents shall be provided in an electronic spreadsheet in the [eg Excel 2007 Binary (.xls), Comma Separated Value (.csv), etc] file format.

3. Review for privileged material

Nothing in this ~~protocol~~plan shall prevent the party giving discovery from reviewing the documents in any list provided hereunder for the purpose of claiming privilege. If the party giving discovery claims privilege over any document or record, he shall list the electronic documents or class of electronic documents over which privilege is claimed in the list of documents.

4. Inspection and copies

(a) **Arrangements for inspection.** The place for inspection of discoverable electronic documents should be stated separately if it is different from the place for inspection of other discoverable documents. If the party entitled to inspect intends to inspect through or with the assistance of its appointed computer expert, such computer expert shall provide an undertaking of confidentiality to the party giving inspection before he commences his inspection.

(b) **Supply of copies.** During inspection, copies shall not be taken. If copies are required, a request should be made. Electronic copies of discoverable documents will be supplied in their native format and in read-only optical discs upon request. Electronic copies of discoverable documents where privilege is claimed only with respect to their internally stored metadata information will be supplied in the Tagged Image File Format (or TIFF) with privileged metadata information removed. For each of the read-only optical discs supplied, a further list stating the storage format version of the optical disc and enumerating the list of electronic documents stored therein shall be provided.

5. Forensic i~~I~~nspection of ~~computer databases and~~ electronic media or recording devices

Parties agree that the protocol for forensic inspection of ~~computer databases and~~ electronic media or recording devices (~~Annex~~ Appendix E Part 3 ~~2~~) shall apply for the inspection of the following:

[List the ~~computer databases,~~ electronic media or recording devices]

6. Inadvertent disclosure of privileged documents

Notwithstanding compliance with the procedures in this ~~protocol~~plan, nothing in this ~~protocol~~plan is intended to be or shall be taken to amount to a waiver of privilege.

7. Discovery and production only if necessary

For the avoidance of doubt, nothing in this ~~protocol~~plan shall compel any party to give discovery of any document or produce any document for inspection which is not otherwise discoverable under Order 24, Rules 7 or 13 of the Rules of Court (Cap 322, R5) [(*where the*

party giving discovery is a bank) or disclose customer information in a manner contrary to its banking secrecy obligations].

APPENDIX E PART ~~2~~3

PROTOCOL FOR FORENSIC INSPECTION OF ~~COMPUTER DATABASES AND~~ ELECTRONIC MEDIA OR RECORDING DEVICES

1. Appointment of computer experts

(a) **Joint appointment.** The party producing the ~~computer database,~~ electronic media or recording device for inspection ("**the Producing Party**") and the party entitled to inspection of the ~~computer database,~~ electronic media or recording device thus produced ("**the Inspecting Party**"), may jointly appoint a computer expert ("**the Joint Expert**") for the purpose of making a forensic copy of such ~~computer database,~~ electronic media or recording device ("**the Original Acquired Image**"). The Joint Expert's role shall be restricted to the acquisition of the Original Acquired Image and the performance of a reasonable search on a copy of the Original Acquired Image in accordance with the terms of this protocol. Before the Joint Expert commences his appointment, he shall provide, and shall procure that each of his employees, representatives, agents or sub-contractors involved in the engagement provides, an undertaking of confidentiality to the Court and to all parties concerned in the inspection.

(b) **Costs and expenses of Joint Expert.** All costs and expenses relating to the appointment of the Joint Expert under this protocol shall initially be borne equally between the Producing Party and the Inspecting Party. Nothing in this protocol is intended to or shall be taken to prevent any party to the cause or matter from seeking the recovery of such costs and expenses in accordance with the Rules of Court (Cap 322, R5).

(c) **Individual appointments.** Nothing in this protocol shall prevent the Producing Party, the Inspecting Party and any other party concerned in the inspection, from appointing his own computer expert.

2. Acquisition of the Original Acquired Image

(a) **Where Joint Expert appointed.** The Joint Expert shall acquire the Original Acquired Image under the supervision of all parties concerned in the inspection, their representatives or computer experts. Sufficient copies of the Original Acquired Image shall be made as necessary in order that the Producing Party and each of the Inspecting Party may be supplied with an electronic copy of the Original Acquired Image. The Joint Expert shall provide sufficient information with the copy of the Original Acquired Image to enable each ~~the~~ party's computer expert to access the copy supplied.

The Original Acquired Image shall be sealed and delivered to the custody of the Producing Party, who shall enumerate it in a list of documents to be filed under Order 24 of the Rules of Court (Cap 322, R5).

(b) **Where Joint Expert not appointed.** The Producing Party's computer expert shall be responsible for acquiring the Original Acquired Image under the supervision of all parties concerned in the inspection, their representatives or computer experts.

Sufficient copies of the Original Acquired Image shall be made as necessary for the purposes of inspection and reasonable search to be provided under this protocol.

The Original Acquired Image shall be sealed and delivered to the custody of the Producing Party, who shall enumerate it in a list of documents to be filed under Order 24 of the Rules of Court (Cap 322, R5).

(c) **Original Acquired Image to be produced when ordered by Court.** The party to whose custody the sealed Original Acquired Image has been delivered shall not tamper with or break the seal, and shall produce the Original Acquired Image to the Court or such other person(s) as the Court may direct.

3. Safeguards for reasonable search

This paragraph applies in situations where a reasonable search is conducted on the contents of a copy of the Original Acquired Image.

Where Joint Expert appointed

(a) **Conduct of reasonable search.** The Inspecting Party shall specify or describe the search terms or phrases to be used in a reasonable search to be conducted on the contents of a copy of the Original Acquired Image to the Producing Party and the Joint Expert.

If the Producing Party does not object to the search terms or phrases so specified or described, he shall communicate his consent to the Joint Expert and the Inspecting Party. The Joint Expert shall make arrangements for the conduct of the reasonable search on a copy of the Original Acquired Image under the supervision of all parties concerned in the inspection, their representatives or computer experts.

If the Producing Party objects to any or all of the search terms or phrases so specified or described, he shall forthwith inform the Joint Expert. The parties shall resolve such objections before any further steps are taken for the conduct of the reasonable search. The Joint Expert shall not take any further steps for the conduct of the reasonable search until:

(i) he is informed by the Producing Party of his consent to the original search terms or phrases; or

(ii) the Inspecting Party specifies or describes a new set of search terms or phrases and to which the Producing Party provides his consent in accordance with this sub-paragraph.

A copy of the documents or records that are the results of the reasonable search ("**the Search Results**") shall be made and released to the Producing Party.

(b) **Review for privileged material.** The Producing Party shall be at liberty to review the Search Results for the purpose of claiming privilege. If the Producing Party claims privilege over any document or record from the Search Results, he shall list the electronic documents or records over which privilege is claimed.

(c) **Release for inspection.** Thereafter, the Joint Expert shall remove copies of any documents or records over which privilege is claimed from the Search Results ("**the Redacted Search Results**"). The Joint Expert may maintain a separate privilege log which records the documents or records which are thus removed and the reasons given for doing so. For the avoidance of doubt, the privilege log shall not be included in the Joint Expert's report but the Joint Expert shall produce the privilege log to the Court if so directed by the Court.

The Redacted Search Results shall be released to the Inspecting Party for inspection together with the list of electronic documents or records over which privilege is claimed.

Where Joint Expert not appointed

(a) **Conduct of reasonable search.** The Inspecting Party shall specify or describe the search terms or phrases to be used in a reasonable search to be conducted on the contents of a copy of the Original Acquired Image to the Producing Party. If the Producing Party objects to any or all of the search terms or phrases so specified or described, parties shall resolve such objections before any further steps are taken for the conduct of the reasonable search.

Upon resolution of any objections or if the Producing Party consents to the specified or described search terms or phrases, he shall make arrangements for his computer expert to conduct the requested reasonable search on a copy of the Original Acquired Image under the supervision of all parties concerned in the inspection, their representatives or computer experts.

(b) **Review for privileged material.** The Producing Party shall be at liberty to review the Search Results for the purpose of claiming privilege. If the Producing Party claims privilege over any document or record from the Search Results, he shall list the electronic documents or records over which privilege is claimed.

(c) **Release for inspection.** Thereafter, the Producing Party shall remove copies of any documents or records over which privilege is claimed from the Search Results. The Redacted Search Results shall be released to the Inspecting Party for inspection together with the list of electronic documents or records over which privilege is claimed.

4. Safeguards for forensic examination

This paragraph applies to the forensic examination of a copy of the Original Acquired Image for the purpose of identifying electronically stored documents thereon or for the recovery of deleted files or file fragments from unallocated file space or file slack using computer forensic tools or techniques. A Joint Expert shall be appointed for the purpose of such forensic examination.

(a) **Conduct of forensic examination.** The Inspecting Party shall specify or describe the search terms or phrases to be used in the forensic examination to be conducted on the contents of a copy of the Original Acquired Image to the Joint Expert. The Joint Expert shall not at any time disclose to the Producing Party the search terms or

phrases specified or described by the Inspecting Party and shall not include the search terms or phrases in his report.

The Joint Expert shall make arrangements for the conduct of the forensic examination on a copy of the Original Acquired Image. Neither the Inspecting Party nor the Producing Party, or any of their solicitors, computer experts, employees, representatives or agents shall be present during the conduct of the forensic examination.

A copy of the documents or records that are the results of the reasonable search ("**the Search Results**") shall be made and released to the Producing Party. The Producing Party is not entitled to a copy, and shall not request the Joint Expert for a copy, of the search terms or phrases specified or described by the Inspecting Party.

(b) **Review for privileged material.** The Joint Expert and the Producing Party shall jointly review the Search Results for the purpose of permitting the Producing Party to identify electronically stored documents, deleted files or file fragments over which he claims privilege. If the Producing Party claims privilege over any electronically stored documents, deleted files or file fragments from the Search Results, he shall identify them to the Joint Expert. The Producing Party shall list the electronic documents, deleted files or file fragments over which privilege is claimed.

(c) **Release for inspection.** Thereafter, the Joint Expert shall remove copies of any electronic documents, deleted files or file fragments over which privilege is claimed from the Search Results ("**the Redacted Search Results**"). The Joint Expert may maintain a separate privilege log which records the electronic documents, deleted files or file fragments which are thus removed and the reasons provided for the request. For the avoidance of doubt, the privilege log shall not be included in the Joint Expert's report but the Joint Expert shall produce the privilege log to the Court if so directed by the Court.

The Redacted Search Results shall be released to the Inspecting Party for inspection together with the Producing Party's list of electronic documents, deleted files or file fragments over which privilege is claimed.

5. Inadvertent disclosure of privileged documents

Notwithstanding compliance with the procedures in this protocol, nothing in this protocol is intended to be or shall be taken to amount to a waiver of privilege.

6. Discovery and production only if necessary

For the avoidance of doubt, nothing in this protocol shall compel any party to give discovery of any document or produce any document for inspection which is not otherwise discoverable under Order 24, Rules 7 or 13 of the Rules of Court (Cap 322, R5) [(*where the party giving discovery is a bank*) or disclose customer information in a manner contrary to its banking secrecy obligations].

APPENDIX E PART ~~3~~4

REASONABLY USABLE FORMATS

File Format	Version
Office documents	
Hypertext Markup Language	HTML 4.01 or ISO/IEC 15445:2000
Extensible Hypertext Markup Language	XHTML 2.0
Rich Text Format (RTF)	RTF 1.9.1
Plaintext Format	ASCII or Unicode
Portable Document Format (PDF)	PDF 1.7 or ISO 32000-1:2008
Microsoft Office file formats	Word 97-2007 Binary File Format (.doc) Specification PowerPoint 97-2007 Binary File Format (.ppt) Specification Excel 97-2007 Binary File Format (.xls) Specification Excel 2007 Binary File Format (.xlsb) Specification Office Drawing 97-2007 Binary Format Specification
Electronic Mail	
Multipurpose Internet Mail Extension (MIME)	RFC 5322
.eml	Mozilla Thunderbird, Windows Mail and Microsoft Outlook Express e-mail messages
.msg	Microsoft Office Outlook e-mail messages
Personal Storage Table (PST)	Microsoft Outlook
Notes Storage Format (NSF)	Lotus Notes
Images	
Joint Photographic Experts Group (JPEG)	ISO/IEC 10918-1
JPEG 2000	ISO/IEC 15444-1:2000
Portable Network Graphics (PNG)	ISO/IEC 15948:2004
Tagged Image File Format	TIFF
Portable Document Format (PDF)	PDF 1.7 or ISO 32000-1:2008
Audio	

MPEG-1 Audio Layer 3 (MP3)	ISO/IEC 11172-3
Advanced Audio Coding (AAC)	ISO/IEC 14496-3:2005

Video

Moving Picture Experts Group (MPEG-1)	ISO/IEC-11172
H.264	ITU-T H.264
MPEG-4 Part 10 or MPEG-4 AVC (Advanced Video Coding)	ISO/IEC 14496-10

Multimedia container formats

Audio Video Interleave	AVI
QuickTime	MOV
MPEG-4 Part 14	ISO/IEC 14496-14:2003