COMMISSION ON ARBITRATION AND ADR | LEADING DISPUTE RESOLUTION WORLDWIDE

ICC COMMISSION REPORT

MANAGING E-DOCUMENT PRODUCTION

INTERNATIONAL CHAMBER OF COMMERCE

International Chamber of Commerce (ICC)
33-43 avenue du Président Wilson
75116 Paris, France
www.iccwbo.org

The views and recommendations contained in this publication originate from a Task Force created within ICC's Commission on Arbitration and ADR. They should not be thought to represent views and recommendations of the ICC International Court of Arbitration, nor are they in any way binding on the International Court of Arbitration.

Designed by Further™
furthercreative.co.uk

Contents

Techniques for Managing Electronic Document Production When it is Permitted or Required in International Arbitration

Techniques for Managing Electronic Document Production When it is Permitted or Required in International Arbitration

Report of the ICC Commission on Arbitration and ADR Task Force on the Production of Electronic Documents in International Arbitration

There is no automatic duty to disclose documents, or right to request or obtain document production, in international arbitration, and the advent of electronic documents should not lead to any expansion of the traditional and prevailing approach to document production. Thus, requests for the production of electronic documents, like requests for the production of paper documents—to the extent they are deemed necessary and appropriate in any given arbitration—should remain limited, tailored to the specific circumstances of the case and subject to the general document production principles of specificity, relevance, materiality and proportionality. Without endorsing any particular practice or scope of document production, this Report and the accompanying Appendices identify several techniques that arbitrators and parties may wish to consider using in order to manage, in a fair and efficient manner, any issues that may arise when production of electronic documents is permitted or required and, importantly, to ensure that international arbitration does not fall prey to the inefficiencies of electronic document production that have plagued litigation in certain national court jurisdictions like the United States.

1. INTRODUCTION

1.1 Mindful of the need constantly to monitor the effectiveness of international arbitration in delivering fair and efficient dispute resolution, the ICC Commission on Arbitration (as it was then known) constituted a Task Force on the Production of Electronic Documents in International Arbitration. The Task Force was co-chaired by Loretta Malintoppi and Robert Smit and comprised international arbitration users, practitioners, academics and technical experts from around the world. The Task Force analysed the issues raised by the production of electronic documents in international arbitration and prepared this Report with the aim of providing information of practical utility to parties and arbitrators who may be confronted with those issues.

1.2 A characteristic of international business disputes is the importance of documentary evidence. With the advent of the electronic age, communications and other information that used to be recorded in paper documen ts are now often created and stored in electronic form ("electronic documents"). Accordingly, much of the documentary evidence now produced in business disputes consists of electronic documents. The move from paper to electronic documentation has been accompanied by an exponential increase in the volume of material that is recorded in a permanent fashion.

1.3 Documentary evidence may be introduced into dispute resolution proceedings in broadly two ways. First, a party will typically submit documentary evidence in support of its own case. Secondly, depending on the procedural framework under which the dispute is being resolved, a party may also be able to obtain the production of such evidence in the possession or control of its opponent. The scope and efficiency of any document production process can affect the efficiency of the entire proceedings.

1.4 The extent to which a party to court litigation may obtain documents in the possession or control of its opponent differs considerably between jurisdictions. In some jurisdictions in which there is a general right to disclosure or discovery of documentary evidence in the hands of an opponent, the advent of electronic documents, and the increase in the volume of material, have given rise to challenges to the efficiency of the litigation process. This has been well documented in the United States, where document discovery is particularly wide-ranging. Other common law jurisdictions which provide for the disclosure of documents as a standard feature of litigation have also had to consider how to adapt those processes to the advent of electronic documents, and have sought to avoid the problems experienced in the United States. Conversely, most civil law jurisdictions do not consider extensive production of documents by the opponent to be a necessary or even appropriate tool to further procedural

fairness. Indeed, for cultural, historic and constitutional reasons, there is a deeply-seated resistance in many such jurisdictions to requiring a party to legal proceedings to assist the other side in gathering information that might be used against the producing party in court.

1.5 As noted above, in international arbitration, each party is responsible for submitting the documentary evidence on which it intends to rely to support its case and there is no automatic right to the production of documentary evidence in the possession or control of another party. Moreover, when a party is ordered to produce documents, the prevailing practice is that the scope of such production should be limited to specifically identified documents or to narrow and specific categories of relevant and material documents. Accordingly, the move from paper to electronic documentation in international arbitration has not generally occasioned the same difficulties as have been experienced in court litigation in those jurisdictions in which broad document discovery or disclosure is a standard feature.

2. EXECUTIVE SUMMARY

2.1 Under the ICC Rules of Arbitration (the "ICC Rules") arbitral tribunals have the power to decide whether or not to order the production of documentary evidence, including electronic documents, and to manage any such process in a fair and efficient way. In addition, the framework for the production of documents set out in the IBA Rules on the Taking of Evidence in International Arbitration (the "IBA Rules of Evidence") is a valuable resource to help parties and arbitrators deal with the issue of document production, and expressly encompasses the production of electronic documents. As reflected in the IBA Rules of Evidence, the same principles of specificity, relevance, materiality and proportionality apply to the production of both paper and electronic documents.

2.2 It does not seem necessary to prescribe specific "rules" or "guidelines" applicable specifically to the production of electronic documents. Furthermore, it may be undesirable to do so to the extent that such rules or guidelines may compromise the parties' and arbitrators' flexibility to address issues in light of the particular circumstances of each case. In particular, the production of electronic documents, if any, should not jeopardize the efficient and cost-effective use of arbitration and thus its attractiveness as a method of dispute resolution.

2.3 Typical practice in international arbitration, and a widely-shared concern of users, is that requests for the production of documents by an opponent, when available at all, should be limited to specifically identified documents or to narrow and specific categories of relevant and material documents. Moreover, an arbitral tribunal should also consider the proportionality of ordering any requested production: it should weigh the relevance and materiality of a document or category of documents against the likely burden of searching for, retrieving, reviewing and producing it.

2.4 In deciding whether to allow, and in managing, the production of electronic documents, parties and arbitrators should take account of particular features of such documents that give rise to additional or different practical considerations from those that arise in connection with paper documents. In so doing, it is essential not to discourage businesses from having recourse to arbitration by proposing approaches that are likely to increase the expense of the proceedings and the disruption to their business activities.

2.5 This Report describes the key features of electronic documents and how they may be managed, which is facilitated by a co-operative approach by the parties, by a focus on avoiding steps that will occasion unnecessary cost or delay, and by active case management by the arbitral tribunal. However, the advent of electronic documents should not lead to any expansion of the traditional and prevailing approach to document production, if any, in arbitration. Requests for the production of electronic documents, like requests for the production of paper documents, to the extent that they are necessary at all, should be limited and tailored to the specific circumstances of the case. The key to maintaining the efficiency of international arbitration, and avoiding the problems occasioned in some jurisdictions by the advent of electronic documents, is for parties and arbitral tribunals to continue to adhere to these general principles of specificity, relevance, materiality and proportionality.

2.6 Two Appendices accompany this Report. Appendix I provides a Primer—for the benefit of parties and arbitrators less knowledgeable about information technology—which contains a description of some of the differences between paper documents and electronic documents and explains how the latter are created, stored, searched, transmitted and deleted. This basic information about electronic documents is intended to assist parties and arbitrators in dealing with some of the practical considerations that may arise when addressing questions relating to electronic documents and to help them manage any production of such documents in a fair and efficient manner. Appendix II contains a Glossary of relevant terms relating to electronic documents.

3. EXISTING INTERNATIONAL ARBITRATION RULES

A. ICC Rules

3.1 As noted in the preface to the ICC Commission on Arbitration and ADR's Report on "Techniques for Controlling Time and Costs in Arbitration" ("Controlling Time and Costs"), a salient characteristic of arbitration is that "rules of arbitration themselves present a framework for arbitration proceedings but rarely set out detailed procedures for the conduct of the arbitration". This facilitates the flexibility of arbitration as a method of dispute resolution, and allows the parties and (where they cannot agree) the tribunal to decide the specific procedures for a particular dispute.

3.2 This general characteristic of arbitration applies equally to the production of documents (whether paper or electronic). The ICC Rules contain no specific provision governing the production of documents, and ICC tribunals enjoy wide discretion in managing the proceedings under the Rules. The most pertinent provisions are Articles 19, 22 and 25 of the ICC Rules in force as of 1 January 2012.

(a) Under Article 19, arbitral proceedings are governed by the ICC Rules and, where the Rules are silent, by any rules which the parties or, failing party agreement, the arbitral tribunal shall deem appropriate. Article 19 also explicitly states that parties and arbitrators need not apply the rules of procedure of any national law, subject to the need to take account of any applicable mandatory arbitral procedures prescribed by the national arbitration law in force at the place of arbitration.

(b) Article 22(4) of the Rules requires that the arbitral tribunal "shall act fairly and impartially and ensure that each party has a reasonable opportunity to present its case".

(c) Article 25(1) further provides that the arbitral tribunal "shall proceed within as short a time as possible to establish the facts of the case by all appropriate means".

(d) Article 25(5) provides that "[a]t any time during the proceedings, the arbitral tribunal may summon any party to provide additional evidence".

3.3 Accordingly, under the ICC Rules, issues such as whether and how much production of either paper or electronic documents will occur—i.e. whether document production is an appropriate means to establish the facts of the case—are left up to the parties and the arbitrators, provided that the parties are treated fairly and impartially and that each party has a reasonable opportunity to present its case.

3.4 Importantly, and unlike the practice before courts in some jurisdictions, under the ICC Rules there is no general duty on a party to disclose paper or electronic documents to its opponent; nor is there any automatic right for a party to request such documents from an opponent. Furthermore, and again unlike the case in litigation before some courts, a party is not placed under a duty to preserve paper or electronic documents, or other evidence, for the purposes of the arbitration. These features of the ICC Rules reflect the general practice in international arbitration.

B. IBA Rules of Evidence

3.5 The IBA Rules of Evidence, originally adopted in 1999 and revised by a resolution of the IBA Council of 29 May 2010, are intended to provide a resource to parties and to arbitrators for the efficient, economical and fair taking of evidence in international arbitration, particularly when the parties come from different legal backgrounds and cultures. They provide a detailed framework for addressing the production of documents in arbitration, including the production of electronic documents. While the IBA Rules of Evidence are not themselves binding, parties and/or arbitral tribunals may agree to adopt them, or use them as guidelines, in their entirety or in part, for the conduct of arbitral proceedings.

3.6 The IBA Rules of Evidence have always applied to both paper and electronic documents: "document", as defined in the 1999 version of these rules, meant "a writing of any kind" and expressly included writing recorded by "electronic means". The 2010 version of the IBA Rules of Evidence contains a new definition of a document which also encompasses electronic documents: "a writing, communication, picture, drawing, program or data of any kind, whether recorded or maintained on paper or by electronic, audio, visual or any other means". Accordingly, the principles governing the production of paper documents under the IBA Rules of Evidence apply equally to the production of electronic documents in order to ensure an efficient and economical document production process.

3.7 The IBA Rules of Evidence provide for:

(a) The production by each party, within the time ordered by the arbitral tribunal, of all documents on which it intends to rely to support its case (Article 3(1)); and

(b) A party's right to request, and the arbitral tribunal's authority to order, the production of either a specifically identified document, or "a narrow and specific requested category of Documents that are reasonably believed to exist", provided that they are not in the possession, custody and control of the requesting party, the "Documents requested are relevant to the case and material to its outcome", and production is not objectionable under Article 9(2) (Articles 3(3) and 3(7)). Article 9(2) instructs the arbitral tribunal to "exclude from evidence or production any Document" on relevance, materiality, burden, privilege, fairness and other listed grounds, such as compelling grounds of commercial confidentiality.

3.8 The IBA Rules of Evidence leave it to parties and arbitrators to determine what documents are "relevant and material" in an individual case, and, assuming that document production takes place at all, when it takes place—i.e. before, concurrent with or after the parties submit written memorials.

3.9 The IBA Rules of Evidence also leave it to the parties and arbitrators in individual cases to determine what constitutes a "narrow and specific" category of documents for the purpose of those document requests that are not limited to specific documents. With respect to electronic documents, Article 3(3) of the IBA Rules of Evidence adds only that: "in the case of Documents maintained in electronic form, the requesting Party may, or the Arbitral Tribunal may order that it shall be required to, identify specific files, search terms, individuals or other means of searching for such Documents in an efficient and economical manner". This provision was inserted as part of the 2010 revision of the rules.

3.10 Article 9(5) of the IBA Rules of Evidence provides that an arbitral tribunal may infer that a document would have been adverse to the interests of a party that, without satisfactory explanation, fails to produce it after being ordered to so. However, no provision is made for a duty to preserve documents (including electronic documents) or other evidence. Amongst the grounds for refusing production of a document, Article 9(2)(d) lists the "loss or destruction of the Document that has been shown with reasonable likelihood to have occurred".

C. General principles

3.11 As noted above, the IBA Rules of Evidence apply to both paper and electronic documents, and subject requests for the production of documents in both categories to the same principles. This reflects prevailing practice in international arbitration. There is and there should be no difference in principle between the production of paper documents and the production of electronic documents in arbitration. The mere fact that relevant and material information is or may be stored electronically rather than on paper (or may be stored in both formats) is not, in itself, a reason to grant or deny production of that information. The move from predominantly paper-based to predominantly electronic storage of information within businesses therefore requires no general reconsideration of the principles of document production in international arbitration. Application, however, of the principle of proportionality—i.e. that the burdens of production be proportionate to, and not outweigh, the likely benefits of production—may dictate different conclusions in particular cases with respect to the production of paper documents and electronic documents in light of practical challenges and opportunities presented by the way electronic documents are created, stored, searched, retrieved and produced. Arbitrators have sufficient powers under the ICC Rules and/or IBA Rules of Evidence to address those practical considerations and manage the production of either kind of document in a fair and efficient manner.

3.12 In determining the scope and means of document production (whether it concerns paper or electronic documents), parties and arbitrators should be guided by the basic principles of specificity, relevance, materiality and proportionality. First, only adequately identified, relevant and material documents (whether electronic or paper documents) should be subject to production. If the arbitrators are satisfied that the document or category of documents sought is sufficiently identified, relevant and material and all other applicable criteria for the production of documents are met (in particular, pursuant to the IBA Rules of Evidence or generally accepted "best practices"), they should then consider whether the requested production would be likely to impose an unreasonable burden on the producing party.

3.13 This process requires arbitrators to consider the balance between the likely benefits of production to parties and arbitrators and the potential costs, delay and other burdens that the production exercise may entail. It requires consideration of the specific circumstances of the case at hand. Parties and arbitral tribunals therefore require a degree of flexibility in this respect. The ICC Rules (as supplemented from time to time in the practice of arbitral tribunals by the IBA Rules of Evidence or generally accepted best practices) recognize as much and provide for an appropriate degree of flexibility. This might be lost if detailed new rules or guidelines were introduced.

4. CHARACTERISTICS OF ELECTRONIC DOCUMENTS

4.1 In applying the general principles discussed above, parties and arbitral tribunals need to take account of a number of features of electronic documents which can give rise to practical considerations different from or additional to those that arise in relation to paper documents. This section sets out the key features of electronic documents and the practical considerations.

A. Increased volume of material

4.2 Computers have made it possible for individuals and businesses to generate, accumulate and disseminate vastly greater quantities of information in electronic form than was the case when the principal means of written communication and record-keeping was in a physical, paper format. The simplicity and ubiquity of email invites voluminous, written records of information that previously would not have been recorded or communicated in written form.

4.3 The following practical considerations arise:

(a) Emails, and electronic documents generally, may provide additional contemporaneous written evidence which may assist a tribunal in identifying the facts of a dispute and reduce the extent to which it must rely on the recollection of witnesses.

(b) However, if a party is placed under an obligation to produce documents framed in broad terms, the retrieval, review and production of electronic documents in accordance with that obligation may give rise to considerable expense and delay. This has, indeed, been the experience in litigation in the United States, where parties are placed under particularly wide-ranging document discovery obligations.

(c) The volume of electronic documents may also mean that searching for a particular document held electronically in response to a document request—to the extent such document requests are allowed—is a more extensive process than it might have been when documents were predominantly paper-based.

(d) While parties of course review their own documents to some extent to prepare for or during the course of an arbitration, given the vast scope of and numerous sources for potential electronic documents, they often do not review the entire universe of documents that may have some relevance to the arbitration. Thus, such internal review typically does not suffice in case of extensive disclosure requests by the opposing party. As a consequence, the often costly and disruptive consequences of broad document requests cannot necessarily be avoided merely because a party has already undertaken some internal review of its own documents.

B. Dispersal

4.4 Electronic documents relating to a transaction or event may be dispersed more widely than the relevant paper documents. Whereas paper documents relating to a transaction or event may typically be stored in a limited number of physical locations (e.g. a number of files, boxes, drawers, a warehouse), electronic documents may reside simultaneously in several different locations (mainframe computers, network servers, personal desktop or laptop computers, BlackBerries or other hand-held devices, electronic back-up or disaster recovery systems).

4.5 The following practical considerations arise:

(a) The dispersal of electronic documents may lead to the retention of evidence that is relevant and material to a dispute when physical paper documents are no longer available.

(b) However, there may be a greater number of potential places to search for electronic documents in response to a document request than is the case for paper documents. This may increase the burden of any search ordered by an arbitral tribunal. It also requires the requesting party to show that the documents requested are not in its own possession or under its own control or at least not reasonably accessible.

(c) Electronic documents are often more accessible in some locations than in others. Electronic documents that are in everyday use will typically be readily accessible, although potentially voluminous. Electronic documents held for back-up or disaster recovery purposes will often be relatively inaccessible, and retrieving data from such a source may require the restoration of a large volume of material which may then have to be processed and searched. Each party's system is different; for example, the accessibility of archived electronic documents may vary depending on how well organized a party's archive is. The time and cost of retrieving electronic documents may vary considerably depending on how accessible they are.

(d) There may be significant duplication of electronic documents across a party's computer system. Several electronic copies of the same document may exist in various repositories within a party's system or network.

C. Durability and fragility

4.6 Electronic documents are both more durable and more fragile than paper documents.

(a) Even after they are "deleted" and even if no copies exist, emails and other electronic documents may nevertheless continue to exist and remain potentially recoverable. (A "deleted" electronic document is often simply moved to another location in a computer system, the space which it occupied is designated as available for storage of new data, and the document may only be lost as and when the system overwrites it with new data.) Such "deleted" material may not, however, be easily accessible and may be incomplete (i.e. an electronic document may only be recoverable in part). Recovery of such electronic documents may only be possible with the assistance of forensic specialists and attendant costs.

(b) Unlike paper documents, electronic documents are easily edited, modified or over-written, sometimes automatically without any human intervention (e.g. as with "auto-delete" functions). Everyday use of a system (e.g. accessing, copying or printing an electronic document) may result in changes to electronic documents (particularly metadata, as to which, see below). As a result, electronic documents are more vulnerable to being changed inadvertently or for improper purposes. Preserving an electronic document in the precise state it is in on a given date will typically require active steps, such as taking copies or forensically "imaging" it. Forensically preserving any large volume of electronic documents will typically involve significant costs and cause disruption to a party's ongoing business.

D. Use of hardware and software

4.7 Computer hardware and software is used to create, read and render an electronic document in a form that is viewable and printable.

(a) Most of the electronic documents created by a business are likely to be created and stored using well-known commercially available and reasonably standard hardware and software, to which other parties, counsel and arbitrators also have access.

(b) However, many electronic documents may not be readily accessible by others. They may be created and/or stored on specialized or even bespoke or obsolete hardware or software. Another party to a dispute, counsel and/or arbitrators may not have access to the hardware or software needed to view or print such electronic documents. A similar situation may arise with respect to documents created with standard commercial software that is not or not yet in use by that party or person (such as a different email system or a new version of a standard software product). It may be possible to convert such documents into another, more accessible format. For example, many of the major software providers enable new software releases to be "backward compatible" (i.e. able to access documents produced on earlier versions of the software) to a point. However, the time and costs involved to undertake such a conversion can vary depending on the nature of the electronic documents in question.

E. Metadata

4.8 "Metadata" is, literally, data about (electronically stored) data. Documents or files created on a computer will typically contain embedded information that is not readily apparent on the screen view of a file or in a printed version of the document or file. This secondary "metadata" is information about the electronic document or file that describes its characteristics, origins, or usage. There are three basic categories of metadata:

(i) "Substantive" (or "application") metadata is created by the software used to create the document, and reflects (among other things) editing changes or comments made to the document over time. Substantive metadata is embedded in the document it describes—and therefore remains with, and arguably part of, the document when it is copied, moved or produced—and may be useful in showing the genesis of a document and the history of proposed and/or accepted revisions to the document.

(ii) "Systems" metadata reflects automatically generated information about the creation or revision of a document, such as the document's author or the date and time of its creation, modification or delivery. Systems metadata is not necessarily embedded in the document but can be generated by the computer system on which the document was created, and can be relevant if a document's authenticity is at issue or there are issues as to who received a document (including blind copy recipients that do not appear on the face of a document) or when it was received.

(iii) "Embedded" metadata is inputted into a document by its creator or users but cannot be seen in the document's display, and commonly includes the formulas used to create spreadsheets, hidden columns, references, fields or linked files. Embedded metadata can be critical to understanding complex spreadsheets (such as those often used, for example, in construction projects) which on their face do not explain the mathematical formulas underlying or relating to the various rows or columns of information that are displayed on a computer screen or printed version of the spreadsheet.

4.9 "Visible" metadata should be distinguished from "hidden" metadata. Visible metadata is commonly displayed on screen and/or in print-outs and hidden metadata is not. In the case of an email, strictly speaking, all its constituent fields are metadata. Examples of visible metadata include the to/from/cc/date/title fields. Examples of hidden metadata would include the route the email took over the internet and the IP address from which it was sent. Most of the metadata mentioned in sub-paragraphs (i) to (iii) above is hidden metadata.

4.10 The following practical considerations arise:

(a) Visible metadata (e.g. the visible fields of an email mentioned above) and embedded metadata (e.g. the formulas used in a spreadsheet) will often be necessary to understand the data in an electronic document.

(b) Where there is a suspicion of fraud, forgery or deliberate tampering with evidence, hidden metadata may be valuable evidence. However, in most cases hidden metadata will not be relevant or material to the issues in dispute.

(c) Metadata is particularly vulnerable to inadvertent modification. Metadata may also be lost if an electronic document is converted from one format to another. It may be possible to preserve metadata forensically, but at a cost.

(d) If an electronic document is produced in "native" format (i.e. the format in which it was originally created), or something close to native format (e.g. a format created by review software which approximates the native format but allows it to be searched and handled more easily), the substantive and embedded metadata will normally be included in it. Typically, a document produced in such a format will be searchable by the receiving party to the same extent as it was by the producing party (provided the receiving party has similar software available to it). It may be possible to remove substantive or embedded metadata from an electronic "document", either by using software which strips out (some of)

the metadata, or by converting the document into another format. Doing so is likely to incur a cost for the producing party, and (depending on the alternative format into which the document is converted) may reduce the searchability of the document in the hands of the receiving party, thus increasing the costs of review for the receiving party.

(e) In connection with US-style e-discovery, the review of hidden metadata involves significant attendant costs. Although millions of pages of documents are frequently produced in a US commercial lawsuit, the number of documents containing hidden metadata material to the case is typically very small. To avoid the costs of review, parties in US litigation frequently agree not to produce most of their documents in their native format, but instead to produce them in a format that allows the documents to be searched but which does not include hidden metadata, and which therefore avoids the review of a significant volume of irrelevant hidden metadata by lawyers. Other jurisdictions that require disclosure of documents in litigation have taken a different approach to this. For example, in England and Wales, the presumption is that documents should be produced in native or near-native format, but that the hidden metadata (other than the date of creation of the document) is likely to be irrelevant and therefore need not be preserved or reviewed.

F. Electronic search and review tools and techniques

4.11 Computer technology offers a number of tools that may assist the process of searching for, organizing and producing electronic documents. Electronic tools may allow for the automatic searching and ordering of volumes of material for documents which satisfy certain parameters, based for example on key words, date ranges, file types, custodian or location on a computer system. Electronic tools may also allow the automatic de-duplication of documents.

4.12 The following practical considerations arise:

(a) A party may have access to some electronic tools as part of its computer system which it uses as part of its everyday business, and which it and counsel may use in identifying evidence in support of its case or to respond to a document request. However, the sophistication of such tools may vary widely. Specialist tools are available, but at a cost. Some counsel in international arbitration may have access to such specialist tools. In other cases, external experts would need to be engaged at additional cost. The most sophisticated specialist tools may be expected to be needed only to respond to broad document requests, of the kind that is generally inappropriate in international arbitration.

(b) All electronic search tools have their limitations. For example, date restrictions may be easier to implement in relation to emails than for other types of electronic documents. The effectiveness of key word searching depends upon the ability to identify search terms that are likely to feature in relevant material and unlikely to feature in irrelevant material. Where electronic documents are stored in multiple languages, care should be taken to identify appropriate key words in each language.

(c) Electronic tools may assist in identifying electronic documents that are potentially responsive to a document request. However, they can rarely, if ever, replace a manual review by counsel of at least some documents. The related costs have to be considered when such a document production request is submitted.

(d) The technique of data sampling entails the retrieval, review and production of only a portion of the repositories potentially containing relevant and material documents in order to assess whether the benefits of further review and production justify the costs and burdens of such review and production.

5. TECHNIQUES FOR MANAGING PRODUCTION OF ELECTRONIC DOCUMENTS, IF ANY

5.1 If international arbitration is to remain an attractive method of dispute resolution, it must avoid the problems to which electronic documents have given rise in court litigation in some jurisdictions. The production of electronic documents does not usually give use to particular difficulties in international arbitration, due (among other reasons) to the disciplined scope of document production in most international arbitrations and the arbitrators' management of the arbitral process. If and to the extent electronic document production issues arise, however, this section discusses techniques and approaches that parties and tribunals may adopt to address those issues in a fair and efficient manner. Nothing in this Report, however, should be interpreted as an endorsement of any particular technique, approach or practice, which remain the exclusive province of parties and arbitrators to decide in light of the particular circumstances of each case.

5.2 Parties are generally free to produce whatever evidence they wish to rely upon. Although some issues concerning the production of electronic documents (such as the format in which a document is produced) apply equally to documents on which a party relies and to requests for documents, most of the issues considered in this section relate only to the latter.

A. Electronic document production in context

5.3 The production of electronic documents is simply an aspect of document production. Since most documents today are created electronically, and many are stored electronically, almost every time a tribunal may be called upon to consider the production of documentary evidence, it will be considering the production of electronic documents.

5.4 Document production is but one of many procedural matters to be addressed by arbitrators as part of their task of managing the arbitral proceedings. As a general rule, parties and arbitrators should heed the two fundamental principles set forth in the introduction to Controlling Time and Costs, namely (i) that they should, wherever possible, make a conscious and deliberate choice early in the proceedings about the specific procedures suitable for the case, and (ii) that the arbitral tribunal should work proactively with the parties to manage the procedure from the start.

In addition, further guidance may be found in Appendix IV to the 2012 ICC Rules, which include case management techniques available to arbitral tribunals and parties to manage document production, paper and electronic alike.

5.5 In light of these principles, parties and arbitral tribunals may consider taking the following steps:

(a) Parties or tribunals may consider expressly adopting the IBA Rules of Evidence, either in whole or in part and either directly or by way of general guidance, to govern the production of documents, including electronic documents, in the arbitration. Logical junctures at which to consider this include at the time the arbitration agreement is drafted, at the time of adoption of the Terms of Reference, and/or in an early procedural order.

(b) Tribunals should encourage the parties to consider document production issues (including the production of electronic documents) as early as possible in the proceedings. Controlling Time and Costs and the ICC Rules recommend that an early case-management conference be convened, either at the time the Terms of Reference are finalized or (if later) once the parties have set out their cases in sufficient detail. The production of documents (including electronic documents) may be included on the agenda for such a conference.

(c) The parties and tribunal should consider whether any questions relating to document production can be resolved at the case-management conference. For example, it may be possible to devise a system for the organization of documents, agree on the format in which electronic documents are to be produced (either by a party in support of its own case or in response to document requests, if there are to be any), and/or agree on the time at which each party is to produce the documents on which it relies. Depending upon the extent to which the issues in dispute are sufficiently clear, it may also be possible at the case-management conference to consider issues of principle relating to document requests, such as whether there are to be any document requests at all and, if so, what procedure is to be followed (see Controlling Time and Costs and Appendix IV to the ICC Rules).

(d) Tribunals should be wary of imposing on parties detailed technical requirements relating to the production of electronic documents, and should only do so after obtaining a clear understanding of the time and costs involved in complying with those requirements. Tribunals should encourage parties to reach agreement regarding such requirements wherever possible, but should be willing to engage with the technical detail in order to resolve disputes. Parties should ensure that they have a clear understanding of the implications of technical requirements (and obtain advice if necessary) before agreeing to them. Parties and tribunals should demonstrate flexibility and be willing to reconsider technical requirements if necessary as an arbitration progresses.

B. Scope of production

5.6 The advent of electronic documents should not lead to any expansion of the traditional and prevailing approach to document production in arbitration. Under the IBA Rules of Evidence, for example, requests for the production of electronic documents, like requests for the production of paper documents, should remain limited to specific documents or narrow categories of documents relevant and material to the issues in dispute in the arbitration. The primary solution to the question of how to avoid the problems caused by the advent of electronic documents in some jurisdictions lies in parties and tribunals adhering to the existing prevailing practice in international arbitration as to the appropriate scope of document production. Parties and arbitrators should bear in mind the following general considerations:

(a) There is no automatic right in international arbitration to obtain documents from an opponent. Parties and tribunals should consider whether document requests are necessary or desirable in the context of the case at hand.

(b) Where document requests are allowed, parties and arbitrators should ensure that they are narrowly drawn in the manner envisaged in the IBA Rules of Evidence, that only documents relevant and material to the outcome of the case are requested and ordered to be produced, and that the benefits and burdens of production are properly assessed before production is ordered. "Fishing expeditions" should be avoided.

(c) Most of the burden, in terms of time and cost, of responding to a document request is often associated with searching for the responsive document or documents (including retrieving electronic documents from a party's computer system and reviewing them for responsiveness and privilege). Parties and tribunals should therefore consider not only the volume of documents that a responding party is being asked to produce, but also, and more importantly, the process it may be expected to undertake to locate and identify those documents if they are not readily available.

(d) Tribunals should avoid broad, US-style discovery, which is inappropriate in international arbitration, unless the parties have specifically agreed that they wish to adopt such an approach.

(e) Finally, parties may view and address electronic documents—their production, dissemination and storage—in very different ways, depending on various factors, including their legal culture, the frequency with which they take part in litigation or arbitration, regulatory requirements to which they are subject, and their size, resources and relative IT sophistication. For example, a party which regularly conducts litigation under rules which impose broad obligations to produce documents may have standard procedures in place designed to facilitate this, whereas a party that does not have such experience is unlikely to have such resources. In some cases, this may mean that a document production requirement which, on its face, applies equally to all parties to an arbitration is in practice more difficult for one party to comply with than for another party. At the same time, however, differences between the parties' relative sophistication in such matters should not be used to justify unfairly disproportionate obligations. Arbitrators should consider whether such factors affect the reasonableness of the proposed scope of production in a particular case and ensure that document production requirements are fair to all parties.

5.7 In implementing these general considerations, parties and tribunals should consider the following practical steps and issues to maintain the fairness and efficiency of the proceedings:

(i) Timing, number and focus of requests

5.8 The scope of document (including electronic document) production may be restricted by limiting the number of document requests a party may make and by permitting requests only in respect of documents relevant and material to particular issues in dispute. Delaying the submission of document requests until after the parties have submitted their memorials and the documents on which they wish to rely may facilitate more focused document requests. Requests can be confined to specific factual issues that are raised in the memorials and on which there are gaps in the documentary evidence already submitted. In general, in view of the requirements of relevance, materiality and proportionality, a tribunal will usually be in a better position to make an informed decision on requests for document production after at least a first round of submissions on the merits.

(ii) Specificity of requests

5.9 Generally speaking, the broader the scope of document requests allowed, the greater will be the cost and burden of production. Document requests should therefore identify, with the greatest specificity practicable, the specific document or specific and narrow category of documents sought. As envisaged in Article 3(3) of the IBA Rules of Evidence, the specificity of a request relating to electronic documents may be enhanced by identifying and/or limiting the scope of what is sought or ordered by reference to various characteristics of the electronic documents requested.

(a) The starting point should be to limit a document request by reference to what is sought (e.g. an email, a report, minutes of a meeting). Requests for specifically identified documents, whether paper or electronic, will ordinarily entail the least burden on the producing party.

(b) Where a specific and narrow category of documents is requested, limits may also be imposed by reference to a limited number of specific custodians who are expected to be in possession of the electronic documents in question, the sources of electronic documents to be reviewed, date restrictions and, if appropriate, the use of specific search terms to assist in locating relevant and material documents.

(c) As the party responding to a document request will typically be more familiar with its internal IT infrastructure and would therefore be in a better position to decide where and how to search for responsive electronic documents, it may be appropriate for the responding party to identify first the parameters of any search for responsive documents it intends to conduct, and then provide an opportunity for the requesting party to comment on the proposed parameters.

(iii) Accessibility of sources

5.10 The relevance and materiality of the electronic documents requested should be carefully weighed against the burden on the requested party of searching for, retrieving, reviewing and producing them. An important factor in this balance is the relative accessibility of the potential sources of the electronic documents requested. Electronic documents are most easily accessed from a party's office, personal computers, network servers and other computers on databases that are in active use during the ordinary course of a party's business operations. They are less readily accessible from removable storage media such as CDs, DVDs or USB drives, Blackberries or Palm Pilots, home office computers or off-site internet storage, which are not sources accessed in the ordinary course of a party's business or may simply be duplicative of other more readily accessible sources. Electronic documents are least accessible when they have been deleted and/or are located only on off-site or back-up storage data (such as back-up tapes) not used in a party's ordinary course of business.

(a) A tribunal should avoid ordering a party to search a less accessible source if a copy of a relevant and material electronic document is likely to be available from a more easily accessible source. A party should consider structuring any search for documents (whether for documents on which it wishes to rely, or in response to a document request) by searching the most accessible sources first, and only searching less accessible sources if it does not find the documents sought and the burden of extending the search is proportionate to the likely evidential value of the documents if they are found.

(b) In most cases, it should be sufficient to limit searches to sources of electronic documents used by a party in its ordinary business operations. If a document is likely only to be available from a less accessible source, a tribunal should consider carefully whether its likely relevance and materiality justify the inconvenience, cost and potential delay involved in retrieving it. Tribunals should ordinarily not order the production of electronic documents in back-up, deleted or archived files that are not readily accessible, unless the requesting party establishes a degree of relevance and materiality that outweighs the burden and costs involved.

(c) Article 3(12)(c) of the IBA Rules of Evidence provides that a party is not obligated to produce multiple copies of documents that are essentially identical unless the tribunal decides otherwise. This presumption against requiring production of multiple copies contributes to the efficiency of the process. A tribunal should generally avoid ordering a party to search for duplicate copies of a document in more than one location, even if they are all easily accessible. An exception to this might occur where identifying the location of copies of a document is itself of evidentiary value (for example, because it identifies which individuals had access to the document and this is of material importance in the arbitration).

(iv) Metadata

5.11 As explained above, whereas visible metadata will typically be required to understand an electronic document that is being produced, hidden metadata will usually be irrelevant to the dispute and it will therefore be unnecessary to produce them. Even where metadata is potentially relevant, the burdens of production may outweigh its potential evidentiary value. Tribunals should consider applying a presumption against requiring the production of hidden metadata associated with a document that is to be produced, unless the requesting party establishes a degree of relevance and materiality that outweighs the burden and costs involved.

5.12 Some of the relevant factors in addressing requests for production of hidden metadata, in addition to the general factors relevant to any document request, include: (a) the importance of the particular type of metadata requested to facilitating the parties' review, production and understanding of the documents to which the metadata relates; (b) the accessibility of the metadata sought; (c) the timing of the request for metadata; and (d) the ease and efficiency with which the metadata can be produced and used.

(v) Use of electronic tools and search methods

5.13 Parties should be encouraged to use technology where this can reduce the burden associated with document production, but parties and tribunals should be aware and take account of the limitations of and costs involved in using the available electronic tools. Computer technology enables parties to search large volumes of electronic documents for specific relevant words, names, subjects or phrases, which may pertain to the particular dispute concerned. This can be both more efficient and more accurate than human document review of paper documents. Although not all electronic documents are searchable in their native form, they may be convertible into a searchable format. However, the processes available to render electronic documents word-searchable may be expensive, and parties and tribunals will need to consider and weigh the extent to which such techniques are appropriate in the context of the circumstances of each individual case.

5.14 In addition to the use of simple key word searches—which risks either identifying too large a universe of responsive documents or missing relevant and material documents that do not include the key word—parties may consider using the ever-expanding array of more sophisticated search technologies (e.g. "Boolean"" searches, "fuzzy" searches, algebraic searches, probabilistic searches) designed to enhance the accuracy of electronic document searches. A manual review of at least some of the electronic documents identified by a key word or other automated search will invariably be required, but the volume of electronic documents that needs to be reviewed by the parties' lawyers should be much less than otherwise. This may, therefore, lead to a significant cost saving.

5.15 Key word searches can be used in different ways to enhance the efficiency of electronic document production. The requesting or responding party may choose, or be required to identify, with its request for production or response, search terms to be used to locate responsive relevant and material electronic documents. Absent objection, use of those search terms may be deemed to satisfy the responding party's obligation to search for and produce responsive electronic documents in good faith. It will often be desirable for the parties to agree on (or the tribunal to order) the relevant key words to be used before searches are undertaken, in order to avoid a search having to be repeated if there is a dispute about the adequacy of the search terms used. When electronic documents are stored in different languages, care should be taken to identify appropriate key words in each language.

5.16 Where relevant and material responsive information may potentially be located in several, or in voluminous, electronic document repositories, parties and arbitrators may wish to consider the technique of data sampling. Data sampling entails the retrieval, review and production of only a portion of the electronic document repositories potentially containing relevant and material information in order to assess whether the benefits of further review and production justify the cost and burden of such review and production. As with electronic document search terms, in appropriate

circumstances, a responding party may be deemed to have satisfied its good faith obligation to produce responsive electronic documents by conducting such data sampling.

5.17 The use of the foregoing electronic search tools should be limited to those particular cases involving a large volume of electronic documents, or different sources of electronic documents, in which the parties and arbitrators conclude that the benefits of such electronic searches outweigh their costs and burdens. In no event should the mere availability of those electronic search tools to search potentially large volumes of electronic documents justify inappropriately broad electronic document requests.

C. IT expertise

5.18 An understanding of a party's IT system will be important to the efficient management of any document production exercise. In most cases, a party's in-house IT staff is likely to be able to provide the necessary expertise to that party, in conjunction with counsel. In particularly complex or high-value disputes, a party may also seek advice from external experts.

5.19 In all but the most exceptional cases, parties, with the assistance of their advisers, should provide (and should be able to provide) the tribunal with sufficient information on their IT systems for the tribunal to manage the process. In the exceptional case, ICC tribunals have the authority to appoint their own IT expert under Article 25(4) of the ICC Rules. In deciding whether and how to appoint such an IT expert, tribunals should consider the guidelines for tribunal-appointed experts set forth in the report of the ICC Commission on Arbitration Task Force on Guidelines for ICC Expertise Proceedings entitled "Issues for Arbitrators to Consider Regarding Experts", published in the *ICC International Court of Arbitration Bulletin* Vol. 21 No. 1 (2010) 31. A tribunal-appointed IT expert, however, should be reserved for the rare case in light of the additional expense, delay and intrusion into the party's IT systems that a tribunal-appointed IT expert may entail.

D. Cost shifting

5.20 Normally, the production of both paper and e-documents, if ordered at all by a tribunal, should be contained and should not give rise to large volumes of documents produced and exchanged. In the rare and very exceptional cases where the volume of electronic documents to be searched and produced is large and/or review and production from less accessible sources of electronic documents is warranted, parties and arbitrators may wish to consider requests for electronic documents only on the condition that some or all of the costs of searching for, retrieving and/or producing those electronic documents is shifted from the responding party to the requesting party. The requesting party, for example, may be required either to (a) pay to the responding party the costs of extraordinary electronic document search and retrieval techniques, or of production in a particular electronic format, as such costs are incurred during or following the electronic document production process; (b) advance those costs to the responding party during the production process, subject to reallocation in the arbitration award in light of the results of the production process and/or the final outcome of the case; or (c) pay those costs once the arbitration award is rendered pursuant to the allocation of arbitration costs set forth in the award.

5.21 However, arbitrators should be mindful of a number of factors which may militate against cost shifting: (i) cost shifting does not reduce the overall cost of the arbitration; (ii) it may become a substitute for disciplined limitations on the scope of document production generally permitted in international arbitration; (iii) it does not give rise to the perceived ability of a party to "purchase" greater access to electronic document production than would otherwise be available; and (iv) it may become a tool for abuse between parties of unequal financial means.

5.22 More generally, arbitrators should be mindful that, like electronic discovery generally in the United States, the standards and practices of US courts with respect to the shifting of costs for the search and production of electronic documents are not generally relevant or appropriate in international arbitration due to the stark differences between US litigation and international arbitration practices with respect to document production and costs. In US litigation, the scope of document discovery is broad and parties ordinarily bear their own costs. In international arbitration, by contrast, the scope of document production is tailored and limited, and arbitrators (as under Article 37(4) of the ICC Rules) are empowered to allocate the costs of the arbitration (including the parties' reasonable attorney fees and other costs) between the parties and in the proportions the arbitrators deem appropriate. In allocating the arbitration costs of the parties, arbitrators may take account of the reasonableness with which a party has conducted the case as well as the outcome of the arbitration.

5.23 Cost shifting should therefore ordinarily be reserved for extraordinary circumstances and imposed only after a weighing of the relevant factors such as, for instance, the volume and accessibility of electronic documents to be reviewed, which party bears the burden of proof and persuasion in the case, the relative financial resources of the parties, and the amounts at stake in the arbitration.

E. Form of production

5.24 The form in which electronic documents are produced by a party in support of its case or in response to a document request may impact their utility to the other party and the arbitrators receiving the documents. Parties

and arbitrators should therefore address at an early stage of the proceedings the form in which electronic documents should be produced. As noted above, this may be done at the case-management conference.

5.25 Electronic documents generally should be produced in the most expeditious, cost-effective and efficient form appropriate in the circumstances.

(a) Parties and arbitral tribunals should note that requiring electronic documents to be converted into a particular format for production may increase costs (possibly significantly so), unless that format is carefully chosen. A producing party may incur conversion costs, only for the requesting party to incur further costs converting the documents into another format. For example, a producing party may incur costs upon converting electronic documents to paper form and filing such paper documents, only for the other party to then incur the additional and unnecessary cost of scanning the documents produced in paper form back into an electronic form with keyword-searchable or other electronic functionalities.

(b) Article 3(12)(b) of the IBA Rules of Evidence provide that, absent specific agreement by the parties or directions by the tribunal, documents in electronic form should be submitted or produced by the party that maintains them "in the form most convenient or economical to it that is reasonably usable by the recipients". This is helpful guidance. In order to avoid unnecessary discussions and potential disruption of the arbitration timetable, in case of doubt about accessibility, the producing party should discuss the format with the receiving party before production and endeavour to reach agreement about such format. In some cases, it may be sensible to convert the electronic documents to a searchable format which all parties and the tribunal are able to access. Conversion may result in the loss of metadata but, unless the lost metadata is likely to be relevant (e.g. visible metadata necessary to understand the document or, exceptionally, hidden metadata if there are doubts as to the authenticity of the document), this is likely to be acceptable, and may save time and costs if the parties otherwise would have reviewed that metadata. However, since the parties in any case should be discouraged from spending time and costs on reviewing irrelevant material, an alternative is for the parties to produce the documents in native format but not to review the hidden metadata, thus also avoiding conversion costs.

(c) Parties may also consider using a web-based repository to which both sides have access as a means of producing electronic documents.

5.26 If the receiving party objects to the producing party's proposed form of production, and the parties are unable to resolve the objection by agreement, arbitrators may consider requiring the receiving party to show that the need for an electronic document in the form it prefers outweighs the burden and cost of providing production in that form.

F. Privilege

5.27 As noted above, documents, including electronic documents, may be withheld from production in international arbitration on grounds of privilege.

5.28 Production of a document to which privilege attaches may amount, in certain jurisdictions, to an inadvertent waiver of that privilege. In cases in which a large volume of electronic documents must be searched and produced (perhaps using automated techniques) inadvertent waiver of privilege is a real concern for parties. The following techniques may be used in an effort to avoid this:

(a) *Privilege search term*. One technique is to apply appropriate search terms to the electronic documents identified in response to a document request, including for the surnames of known lawyers whose names may appear on emails or other documents associated with the gathered material, and for other key words that may appear on documents like "privileged" or "confidential". Documents containing these search terms may then be segregated from the larger set of responsive information and manually reviewed for any applicable privilege. Like all key-word searching, however, this has limitations: for example, many organizations have adopted the practice of incorporating "privileged" and "confidential" notations on all email communications, reducing the efficacy of such search terms.

(b) *"Claw-back"* agreements. Another technique is the use of "claw-back" agreements. A claw-back agreement provides ground rules in advance of production for each producing party to be able to retrieve inadvertently produced privileged documents without risk of waiver. A party may not feel the need to review all documents for privilege before it produces them if such a "claw back" agreement is made. However, the potential drawbacks of claw-back agreements include: (i) they may encourage swamping one's opponent with irrelevant documents, which is entirely inappropriate in international arbitration; (ii) they may not avoid the risk of waiver of privilege with respect to third parties in all jurisdictions; and (iii) they may not effectively protect the inadvertently produced privileged information since the receiving party will have seen the privileged material and may be able to take advantage of that information without actually using the document.

5.29 Use of these techniques should be reserved for extraordinary cases in light of the limited and tailored scope of document production generally available in international arbitration. Moreover, the availability of these techniques should not be used to justify an unduly broad scope of document production.

G. Preservation of and failure to produce electronic documents

5.30 As explained above, electronic documents (in particular, metadata) may easily be altered or destroyed inadvertently, for example by the operation of routine day-to-day computer network functions (including any "auto-delete" functions). Freezing, disabling or deactivating such functions may cause serious inconvenience to a party. In US litigation, procedures are often put in place to preserve and retrieve electronic documents forensically because the mere act of accessing or copying an electronic document will cause changes to be made to its metadata. This is an important factor which greatly contributes to the cost of discovery in US litigation.

5.31 As noted above, international arbitration operates under a very different regime. Tribunals should avoid importing from other systems notions with regard to the preservation of evidence that may give rise to unnecessary inconvenience or expense. While a party's intentional efforts to thwart disclosure of relevant and material evidence by destroying or altering an electronic document may warrant appropriate sanctions (such as an adverse inference contemplated by Article 9(5) of the IBA Rules of Evidence), inadvertent destruction or alteration of an electronic document as a result of routine operation of that party's computer network does not ordinarily reflect any culpable conduct or warrant any such sanctions. Moreover, whilst a party may wish, for its own benefit, to take steps to preserve relevant evidence, it is under no automatic duty to do so. Nor should a tribunal consider imposing such a duty absent a specific reason to do so, such as credible allegations of fraud, forgery or deliberate tampering with evidence.

5.32 If a party wishes to preserve evidence in its possession and control, it should focus its efforts on the most likely sources of relevant and material evidence and avoid taking steps that are likely to give rise to unnecessary inconvenience and expense.

(a) For example, attempting to freeze day-to-day functions across an entire computer network is likely to give rise to severe disruption and costs. Likewise, unless the circumstances of the particular case indicate that hidden metadata may be relevant and material to the dispute, a party should not be expected or required by the tribunal to incur the cost of obtaining a forensic snapshot of all or even a subset of its electronic documents.

(b) On the other hand, a party may consider taking a copy of a limited number of electronic documents from reasonably accessible sources and focused by reference to appropriate parameters (such as key custodians and/or particular electronic folders in which relevant transaction documents are held), and to put that copy to one side or entrust it to counsel for safekeeping. The electronic documents so preserved may provide a resource upon which the party may draw for evidence in support of its own case. It may also provide a convenient starting point for a search for documents in response to a document request.

5.33 Finally, in light of the fragility of electronic documents, if there is a dispute regarding their destruction or alteration, parties and arbitrators should consider placing the burden on the requesting party to show that the responding party has acted wrongfully, rather than on the responding party to show that its actions or inactions were reasonable and in good faith.

6. CONCLUSION

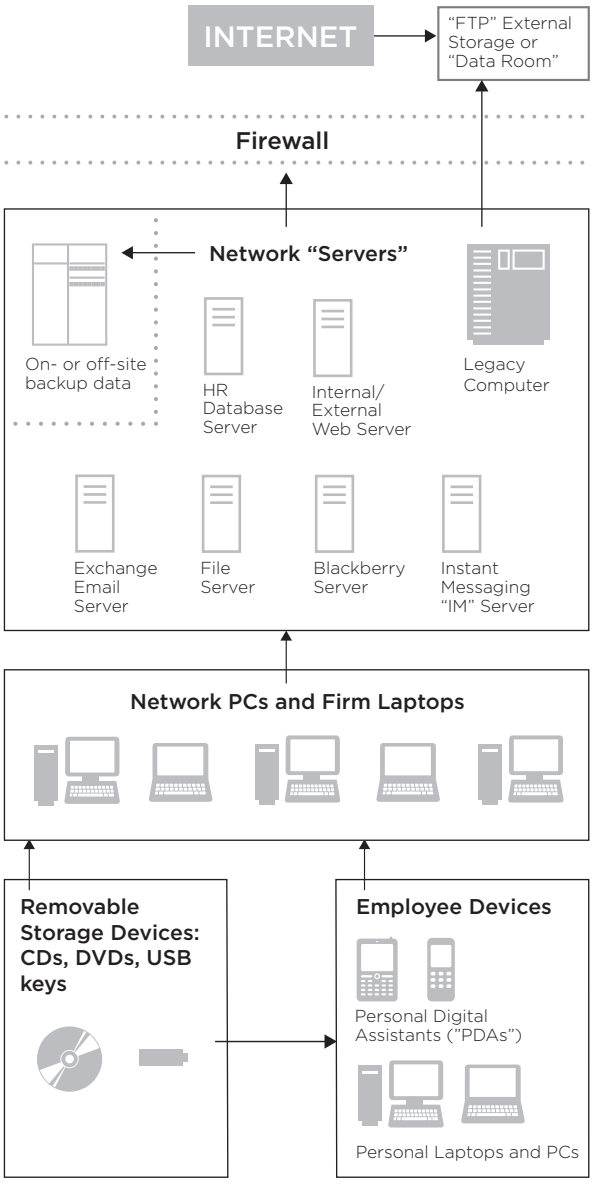
6.1 While each party is of course free to submit any documents in support of its claim or defence, absent a specific agreement between the parties to a case, or an order of the tribunal, there is no obligation to produce documents, including electronic documents, in international arbitration. In deciding whether to order electronic document production, tribunals should be guided by the principles of specificity, relevance, materiality and proportionality.

6.2 Keeping in mind this important framework, it is hoped that this Report will offer concrete assistance to tribunals and parties on how to address and manage as efficiently as possible any electronic document issues that arise, and control any costs and delays that may result when electronic document production is permitted or required in international arbitration.

Appendix I

A Primer on Electronic Documents

DIAGRAM OF A TYPICAL OFFICE COMPUTER NETWORK



1. This Appendix provides an overview of how electronic documents are created, managed and stored, and identifies some of the questions, challenges and opportunities that arise in the production of electronic documents as a result of its unique characteristics.

2. To address electronic document production issues that may arise, it is useful to have a basic understanding of how a typical office computer network works and where electronic documents responsive to a document request may potentially be located and retrieved. Electronic documents may potentially be located either in relatively accessible "active" sources or in less accessible "inactive" back-up, fragmented or deleted sources.

3. "Active" electronic documents—which ordinarily should be the sole source of production of any electronic documents in international arbitration—are generally stored in a readily usable format and are relatively easy to access. "Inactive" electronic documents are generally harder and more expensive to access and produce. The diagram opposite illustrates a simplified office computer network and the hardware components that may be used to create, manage and store electronic documents, and the sections that follow describe the "active" and "inactive" sources of electronic documents, as well as the data about electronic documents known as "metadata"

A. "Active" electronic documents

4. Personal computers: At a basic level, when a human being (a "user" or document "custodian") sits down at his or her "workstation" or desk and writes an email, drafts a word-processing document, populates an electronic spreadsheet (i.e. creates, stores or manipulates electronic documents), he/she does so on a "personal computer" (or "PC")—either a "desktop" or "laptop" computer. The PC will typically have a "local" hard drive where electronic documents created on that PC may be electronically located, stored and accessible only through that specific computer. The kinds of electronic

documents that may exist on the local hard drive of a personal computer include virtually any variety of document or file a person can create using today's vast array of computer software "applications". In a business context, these will most commonly include word-processing files, emails, spreadsheets, slide presentations—the familiar array of files that most office PCs are equipped to create.

5. Electronic documents created on any given user's PC may also be located wherever else those electronic documents may have been sent by the user, or otherwise automatically stored. For example, when a user sends an email, it will typically be recorded in the sender's "sent" box; it will also appear in the "in" box of one or many recipients. The email's recipients in turn may have forwarded the same email to other recipients. On a network, a copy of the email may reside on the PC hard drives of the sender and/or one or more recipients. As described below, it may also be recorded on a shared server, as well as a "personal digital assistant" ("PDA") device such as a Blackberry, which replicates each user's email remotely. The user's PC becomes an input and viewing device for electronic documents located on a server elsewhere.

6. Shared servers: To maximize computer efficiency and to promote office interconnectedness, each user/custodian's PC located at his or her desk will typically be part of a "network" of many such workstation PCs. A network of individual PCs will usually be constructed around a number of shared "server" computers, which constitute a second potential source of "active" electronic documents. A "server" computer is a separate computer from the PC computer located on each user's desk, located and operated centrally, that contains software to perform specific functions for all of the PCs (or "clients") in the network that are interconnected by the server. One example would be a shared email server. Office computer networks will typically have one or more servers that do nothing but "serve" the network's email needs for all of the users in the network. Thus, instead of users each having their own emails created, sent, received and stored on their individual PCs at their desks, all of the emails created, sent, received and stored by all users in the network will reside on one or more shared server computers that do nothing but process emails. The result is that a particular user's email, which they access from their PC, may not actually be located on their individual PC, but instead may be located entirely or in large part on a shared server computer, physically located somewhere else, to which their PC is connected, and which centrally provides email for all network users whose PCs are connected to that email server.

7. The shared functions within an office computer network that may be performed by servers rather than by each individual user's PC can be just about anything. Servers may be dedicated to providing network user access to the Internet, providing internal kinds of messaging applications separate from email, managing the printing of all documents in the office, managing and storing electronic documents created by Blackberry or other handheld devices, or maintaining other kinds of network electronic documents, like all word-processing files or all accounting or staff personnel files in a centrally accessible location. Having dedicated "servers" perform different aspects of a company's business on behalf of all PCs in a network enables centralization and administrative control over a company's electronic documents, whereby a company's "Information Technology" ("IT") officer or department can monitor use, or assign or withhold different user access rights, for instance by limiting the number of users/custodians who may access the server containing the company's staff personnel files or other sensitive need-to-know data.

8. When shared servers are used to create an office network, electronic documents generated by an individual network user at his or her PC may actually be stored in a shared server computer located somewhere else, which that individual user's PC accesses for the particular kind of electronic documents involved—email, word-processing, accounting data, and so on—rather than located on the hard drive of the individual user's desktop or laptop PC. Consequently, a file created by one user in the network may be equally accessible to all or several other users in the network, who can equally access, copy, modify, delete, overwrite or send a particular document or file that was created by another user on the shared server.

9. "Legacy computers": Sometimes a company's network of computers may include "legacy computers", i.e. outdated computer hardware containing antiquated software or data that is still necessary to perform certain aspects of the company's business. For example, a company may have an antiquated or custom-designed accounting system, which resides on a specific computer that can still support the accounting application the company has been using for many years. The speed at which new hardware and software is introduced on the market to replace, supplement or update a company's existing computer systems may often result in piecemeal changes and updates to an existing computer network, requiring phased integration of old and new hardware and software over an extended period of time. Electronic documents created and stored on legacy computers may only be located on one or more specific legacy computers in the network and may not be accessible or readable on any of the company's other computers since other forms of hardware do not support the data concerned. Such legacy electronic documents may be difficult to retrieve and produce in an accessible format if the outdated hardware or software used to create those documents is required to read and use them. Many of the

major software providers enable new software releases to be "backward-compatible" (i.e. able to access electronic documents produced on earlier versions of the software) to a point. However, this is not always the case, for example if a company is operating a bespoke system.

10. PDAs: In addition to serving individual PC and laptop workstations connected within the office network, specific servers may also serve other kinds of client computers, such as personal digital assistants—an ever-expanding array of portable handheld devices, including BlackBerries, smart phones and Palm Pilots—as well as remote PCs or laptops maintained by company employees at home or otherwise outside the office. All of these remote or wireless devices are capable of creating, managing and storing electronic documents in their own right, and remotely accessing, altering, deleting and exchanging electronic documents located on the office network servers via an Internet connection. PDAs will typically contain hard drives of their own where electronic documents may also be stored, in addition to accessing remotely electronic documents that are located on the office network. However, in many cases, any document received, created or sent by a PDA will be automatically synchronized back to a central server.

11. Third-party PCs, servers, and data rooms: Electronic documents may also be found on third-party servers or PCs, completely external to a company's network. For example, data and files may be sent to and then stored on a third-party's PC or network through a "file transfer protocol" ("FTP") client, which allows easy transfer of large amounts of data and files through the Internet. Electronic documents might also be found on an external server in a virtual "data room". Data rooms usually are password-protected, but are often accessible to multiple parties through the Internet. Data rooms may be maintained by the company or a third-party vendor that provides off-site data storage and management, and can contain data and files of both the company and third parties.

12. Removable media: Finally, "active" electronic documents can also be stored on removable media, such as CDs, DVDs, disks, tapes, and USB portable drives. These compact storage devices for electronic information can be used on any computer. They effectively provide a removable and portable hard drive, capable of storing any of the same kinds of electronic documents that a PC can generate, and may be located virtually anywhere—in the office, at home, in a car, in a briefcase, a pocket, with a third party, etc.

B. "Inactive" electronic documents

13. In addition to the foregoing components of a typical "active" computer network, business computer networks typically will also include "archived" or "inactive" electronic documents. Such inactive electronic documents can be located on the same clients and servers that are part of a company's active network, or on dedicated back-up servers or removable disks or tapes, which are maintained separately from the active network so as to protect and preserve electronic documents that can be vital to a business's survival in the event that a catastrophe compromises the company's active computer system and the electronic documents it contains. Depending on a company's business practices, archived electronic documents may be stored within an organized structure. In contrast, back-up servers or tapes will typically maintain a "snapshot" of all or specific portions of a company's active electronic documents, taken on a periodic basis to preserve the company's data in the event of catastrophic system failure, loss or damage such as may be caused by a fire, earthquake, virus contamination, or other core threats to a company's business. Back-up servers or tapes should not, therefore, be expected to provide a comprehensive set of all of a business's electronic documents. Furthermore, back-up electronic documents are typically not maintained in a format that is readily accessible or searchable, as they are intended only for disaster-recovery purposes. Typically, back-up tapes are not well structured. Therefore, it is usually necessary to restore the entire tape or collection of tapes (at considerable expense) in order to investigate only a small part that may be relevant to a particular dispute.

14. "Deleted" electronic documents: "Deleted" electronic documents are another form of inactive electronic documents. "Deleted" is a misnomer insofar as "deletion" of a document or file on a computer may serve only to move it from one location (e.g. an email inbox) to another (e.g. an email "trash" or "recycle" folder) where it remains and can readily be retrieved for some period of time. When an electronic document is then deleted from a trash or recycle file, that typically means only that the digital storage space required to maintain that particular electronic document has been designated as available for the storage of different information as and when the computer automatically determines that the same space is needed to store new or different information. But the deleted item continues to reside on the computer until it is overwritten with new and different information. This can result in "fragmented" files, as computers will move and divide data designated as deleted in order to efficiently make room for new data. However, computer forensic techniques exist even to retrieve a deleted electronic document long after it has been designated as such.

15. It is also worth noting that even when an electronic document is deleted from one location on one computer, PDA or storage device, an identical copy may continue to exist somewhere else on a company's computer system. For example, if the sender of an email deletes the email from his or her sent box at work, the email may continue to exist in a multitude of other email folders of other network users.

C. Metadata

16. "Metadata" is, literally, data about (electronically stored) data. Documents or files created on a computer will typically contain embedded information that is not readily apparent on the screen view of a file or in a printed version of the document or file. This secondary metadata is information about the electronic document or file that describes its characteristics, origins, or usage. There are three basic categories of metadata:

(i) "Substantive" (or "application") metadata is created by the software used to create the document, and reflects (among other things) editing changes or comments made to the document over time. Substantive metadata is embedded in the document it describes—and therefore remains with the document when it is copied, moved or produced—and may be useful in showing the genesis of a document and the history of proposed and/or accepted revisions to the document.

(ii) "Systems" metadata reflects automatically generated information about the creation or revision of a document, such as the document's author or the date and time of its creation, modification or delivery. Systems metadata is not necessarily embedded in the document but can be generated by the computer system on which the document was created, and can be relevant if a document's authenticity is at issue or there are issues as to who received a document (including blind copy recipients that do not appear on the face of a document) or when it was received.

(iii) "Embedded" metadata is inputted into a document by its creator or users but cannot be seen in the document's display, and commonly includes the formulas used to create spreadsheets, hidden columns, references, fields or linked files. Embedded metadata can be critical to understanding complex spreadsheets (such as those often used, for example, in construction projects) which on their face do not explain the mathematical formulas underlying or relating to the various rows or columns of information that are displayed on a computer screen or a printed version of the spreadsheet.

17. It should be noted that "visible" metadata should be distinguished from "hidden" metadata. Visible metadata is commonly displayed on screen and/or in print-outs and hidden metadata is not. In the case of an email, strictly speaking, all its constituent fields are metadata. Examples of visible metadata include the to/from/cc/date/title fields. Examples of hidden metadata would include the route the email took over the Internet and the IP address from which it was sent. Most of the metadata mentioned in sub-paragraphs (i) to (iii) above is hidden metadata.

18. Metadata is most commonly produced either in (a) a pdf or tagged image format (TIFF) with an accompanying "load file" which permits the recipient to search the document for the relevant metadata, or (b) in the "native" format in which the document being produced was created and which provides the recipient with all of the information available to the original user.

Appendix II

A Glossary of Electronic Document Terms

Note: Words in *Italics* refer to entries in this Glossary.

Archived Electronic Sources: means *Electronic Sources* that are stored for a shorter or longer term for the purpose of preservation. Storage for the purpose of archiving (preservation) means that a copy of the *Electronic Source* is made and stored on a *Data Carrier* to preserve it in the actual state without subsequent alterations of its substance. Normally, *Electronic Sources* are archived on dedicated *Data Carriers* which are logically and/or physically kept separate from electronic information that is in use. *Archived Electronic Sources* are a "snapshot" of the archived data in existence at the time the archive was created. Archived *Electronic Sources* may be a complete "snapshot" of this data or incremental. Incremental means that, if compared to the last *Back-up*, only new or changed data is archived.

Authenticity, of electronic document: Archiving or backing up electronic data is mostly done by using dedicated *Computer Programs* that allow the date and time of any modification to data included in the archive to be tracked. Some of these programs comply with national legal requirements for preserving the data integrity, i.e. *Authenticity.*

Authenticity of an Electronic Document is a non-technical attribute ascribed to it in a communication context, here a dispute. An *Electronic Document* is considered as being authentic if (i) the author or creator who figures as such in the context of the information displayed in the document or identified by somebody as being the author/creator really is or is determined by the arbitrators to be the "real" author/creator; (ii) that this author/creator did produce exactly this *Electronic Document* at the moment ascribed to it by him or a third party; and (iii) that the *Electronic Document* was not subsequently altered by anybody.

Back-up: means a copy of electronic data for the purposes of preservation. See also *Archived Electronic Sources.*

Client: refers to dedicated *Software* that is locally installed on a *Computer* linked to a *Network* within which a *Server* is accessed by the *Client*, to which it provides a service. For example, an *email Client* interacts with an *email Server*, such as MS Outlook with MS Exchange or a Lotus Domino *Server* with a Lotus Notes *Client*. Therefore, Network System architecture using *Servers* and *Clients* is referred to as *Server-Client*-architecture.

For the purpose of *eDocument* disclosure it is useful to know, that a *Client* may, but need not always locally and permanently store copies of *ESD*, and that certain *Server-Client*-Systems may store *ESD* permanently only in a *Directory* of the *File System* pertaining to a *Server* (this may be increasingly the case where web-based services are employed in the relevant sphere of control, especially if *Cloud Computing* is used). This may be relevant for identifying *Custodians*.

Cloud Computing: is a catch-all term essentially referring to *Network* based computing systems within which *Software* applications are being provided to local *Computers* by remote *Servers* as a service on demand. Furthermore, *Cloud Computing* is generally characterized by exclusive permanent storage of *ESI* in *Directories* of the *File Systems* pertaining to *Servers* in the so called cloud. A further common feature of *Cloud Computing* is virtualization of *Servers.* Virtualization means that the *Server Software* is dissociated from the *Server*-computer (also called *Server*) hardware and may move from one computer location to another.

The same applies to *Directories* of the *File Systems* pertaining to the *Server Software*. Application service *Software* is often provided by third parties on the basis of complex service providing or outsourcing agreements. This may be relevant for identifying *Custodians* and/or the identification of the physical location of hardware means for *ESI* storage.

Typically, the *User* may access *Cloud Computing* services from any computer in the *Network* using a *User*-ID and password, if such computer is equipped with a web-front-end and *Software* pertaining thereto (e.g. a web-browser such as Mozilla Firefox, Safari, MS Explorer, Java-Runtime). The front-end *Software* may also be referred to as *Client*, which is rather general-purpose and not dedicated (specialized) *Software*. However, *Cloud Computing* may also require dedicated *Software* for certain services.

An example of *Cloud Computing* most people may know are the so called "web-mailers" for managing personal *email* accounts.

Computer Forensics: refers to a branch of forensics dealing with (i) security threats to computing systems and intrusions, but also (ii) *Data Recovery* and verification of data integrity, which are relevant to *eDisclosure*. *Computer Forensics* is a service provided by experts and comprises *inter alia*:

- Extraction of relevant data from computer systems and *Data Carriers*.
- Recovery of deleted data.
- Data analysis for establishing the "history" of data and *Authenticity.*

Computer Hardware: refers to physically existing devices that generate, process, store and display any kind of data, such as *inter alia*: computers, displays, printers, *Network* devices, disk drives and tape drives.

Computer Programs: refers to a recorded machine readable and executable code that is used to operate data processing devices and/or process data. *Computer Programs* usually consist of many *Files* that may also have different formats. *Computer Programs* are normally dedicated for a specific purpose, such as word-processing, spreadsheet calculation, visual presentations, data conversion, data *Back-up*, voice- or video communication.

Computer Programs must be compatible with their environment, i.e. other programs such as the operating system (e.g. Windows, Linux, MacOS, Unix) and possibly other dedicated programs, since they use functions of these programs during operation, by exchanging data through *Software* interfaces.

Computer Programs are normally protected by intellectual property rights, e.g. usually copyright and sometimes patents. Therefore, they may only be used in accordance with the terms and conditions of the licence of the holder of the rights.

Copy: is the reproduction of the original data. In relation to electronically recorded data, the problem is to distinguish copy from original. For example, if you send an *email*, a copy of which is stored in the (virtual) out-box of the sender's *email Client,* the question may arise whether the copy of the message in the (virtual) in-box of the recipient's *email Client* or the copy in the out-box of the sender's *email Client* is the original,. When processing data, computer programs may create several virtually identical *Files* in the background that are stored in different places. Therefore, unlike a sheet of paper with text and signatures, it may be a futile to try to distinguish the original *eDocument* from a copy. The question then is whether the copy is authentic (see *Authenticity*). In our example one could compare the copy in the out-box with the one in the in-box.

Custodian, of electronic data: refers to a natural or legal person that has had or has control over electronic data, such as a specific word-processor file. Such control comprises physical access to a medium on which the electronic data is stored and the rights of access to the electronic data. Physical access means access to a computer or terminal that is technically enabled to access the storage medium on which the data is stored. This access may take place over a *Network*. Technically, access rights are controlled by computer *Software* that is configured by the system operator (SysOp) according to the applicable policies. Access rights range from "read" to "read/write", "delete", "create" to "change name". Access rights are also defined by company policy or legal regulations to which natural persons who are *Custodians* may be subjected. Legal and natural persons who are *Custodians* may be subjected to contractual restrictions and/or legal rules that govern their rights of access to or authority over disclosed electronic data.

Data Mining: originally relates to the extraction of knowledge (information) from databases in a meaningful (intelligible) format for analysis for a specific purpose. Also useful is the context of the production of relevant *ESD*, since parties are required to produce not only *ESD* they know to exist but also which they happen to find by chance. Rather, they must extract and provide the existing *ESD* that falls under an agreed or ordered definition. The dispersion of *ESD* on *Data Carriers*, the variety of possible *File Formats,* and the sheer quantity of *ESD* that must be searched during the process, prevents this process from being carried out manually. Therefore, the use of *Search Tools* is required to extract potentially disclosable *ESD* at a first stage, which is followed by an analysis carried out by somebody at a second stage. This is followed by the extraction and organization of the *ESD* meeting the definition(s). Such *ESD* is mostly organized using *Software* that relies on relational databases. Finally, "mined" *ESD* meeting the definition is disclosed in specified formats, unless *ESD* is privileged.

Data Carrier: means any tangible object on which electronic data is stored (see *Electronic Means of Storing or Recording Information*).

Data Deletion: refers to data, usually a *File* or *Directory* with regard to which somebody has completed the command "delete", Deletion will cause the relevant *Computer Program*, usually the operating system, to treat the data as non-existent, i.e. the *File* or *Directory* is no longer displayed (the logical pointers to the data in the *File System* and data disk sectors are removed). However, this does not mean that the relevant data has disappeared from the *Data Carrier* on which it was stored, unless the sections where bits and bytes of which it is composed are overwritten. Often, all or some deleted data can be recovered even after deletion. This requires dedicated recovery *Software* and, possibly, special technical expertise (see *Computer Forensics*).

Data Erasure: refers to more than *Data Deletion*, since erased data is overwritten and thereby completely destroyed on the storage medium on which the erasure is carried out.

Data Recovery: refers to the complete or partial reconstruction of deleted or erased data using dedicated recovery tools, i.e. programs that analyze and reassemble residual deleted or erased data on a *Data Carrier* (see *Computer Forensics*).

Data Room: This term refers to a dedicated *File Repository* on a *Server* that uses advanced web technology.

Deleted eDocument: refers to a copy of an *eDocument* with regard to which somebody has performed the command "delete". Deletion will cause the relevant *Computer Program*, usually the operating system,

to treat the *eDocument* as non-existent, i.e. the copy of the *eDocument* is no longer displayed. However, this does not mean that the relevant data has disappeared from the *Data Carrier* on which it was stored, unless the sections where bits and bytes of which it is composed are overwritten (see *Data Deletion, Computer Forensics*).

Disaster Recovery System: refers to a *system* consisting of hard- and *Software* with procedures that allow the technological infrastructure, including data, to be recovered or resumed should that infrastructure be hit by a disaster. For this purpose, such system will include periodical *Back-up* of critical *ESI* contained in the primary system.

Directory: refers to a hierarchical system (the *File System*) for organizing and retrieving electronic data used by *Computer Programs*, including the operating system, which is or may also be made visible as a 'folder' or 'drawer' (icons) via the graphical *User* interface, i.e. the display. With the exception of the so-called 'desk top', *Directories* are always logically placed and visualized below one or more physical or logical *Data Carriers*. A *Directory* may contain *Files* or sub-*Directories*. Sub-*Directories* are *Directories* located in another *Directory*, i.e. at a lower point in the logical hierarchy. Each *Directory* has an identifier, i.e. name. *Directories* on the same level in the hierarchy may not have identical names.

eDisclosure: is a non-standardized term used herein. It refers to the process by which a party to an arbitration or any third entity extracts data in electronic format from the *Data Carriers* in its custody and provides one or more other parties to the arbitration with such data in a certain format under the control of the arbitral tribunal and/or in accordance with the terms these parties have agreed. *eDisclosure* also comprises disclosure of copies of physically existing material (e.g. documents, photographs) that have been reduced into digital format.

Electronic Document (eDocument, e-document): may, but need not necessarily be, a "photographic" copy of a physical document that was digitized (scanned). Herein *eDocument* is understood as falling within the definition of "Document" in the IBA Rules on the Taking of Evidence in International Arbitration [2010]. The term *eDocument* is a sub-category of *ESI*, which is the broader term.

Black's Law Dictionary defines the term "Document" as meaning something tangible on which words, symbols or marks are recorded. In short, a document is something tangible on which information that is intelligible by humans is recorded. An *Electronic Document* is a document that is not tangible but may be displayed or printed with the aid of a computer and its peripherals.

In most instances *Electronic Documents* are recorded as *Files*. However, it is also possible that a document is assembled automatically from several *Files* or some information contained in a *File* by a *Computer Program* for the purpose of displaying or printing the *Electronic Document.*

*Electronic Document*s may also contain or consist of video or audio recordings.

Electronic Mail (email): is a means of communicating via computer *Networks* including the *World Wide Web* by using POP or SMTP protocols. *Email* is the primary source of material for *eDisclosure*, since it is intensively used for intra-company communications. *Emails* can be sent and received by any person or logical entity that has an *email* account, i.e. an *email* address and a system with the *Software* required for sending and receiving messages pertaining to this address. To access or send *emails*, *Users* either use a locally installed dedicated program that is called *email Client*, or they access a *Server* with the required *Software* via their web browser over a *Network*.

Email is mainly a means for text-based communication. However, *Files* can and often are "attached" to *emails*.

A sent *email* is normally locally stored by the *Client* or the *Server* behind the web-front-end and then forwarded by *email* computer *Server* systems in blocks (data segments) via *Network(s)* to the *email Server* of the domain to which the recipient's *email* address belongs. This *Server* stores the *email* and forwards it to the *email Client* that is configured for receiving *emails* sent to the *email* account to which the recipient's *email* address belongs, if this *Client* (automatically) sends a signal to the *Server* indicating that it "wants" to or can receive messages.

Each copy of an *email* that was created during the process can be deleted by a person with the required access rights, or automatically (normally after a certain period of time) where the system is configured to allow automatic deletion. However, the existence of large numbers of copies, as happens when there are multiple recipients, increases the probability that one or more copies remain available somewhere.

Proving actual receipt of an *email* by an intended recipient, in the event the recipient denies receipt, may be difficult for technical reasons. However, the content of other available information (documents) may indirectly prove receipt. *Computer Forensics* may also be used to clarify the issue.

Issues relating to *Authenticity* or subsequent alterations of messages (technically easy) may be resolved by comparing copies of *emails*. Otherwise, *Computer Forensics* may also be used to clarify the issue.

Electronic Means of Storing or Recording Information: refers to dedicated computer hardware for storing data, such as hard disks, memory cards, diskettes, back-up tape machines, USB-sticks, CD/DVD/Blu-ray drives and the discs they use, as well as the *Software* for carrying out read/write operations. Storing implies a certain duration; the random access memory (RAM) used by computers to store transient bits and bytes during processing is not included.

Electronic Sources: mean information of any kind stored in machine-readable electronic format that may be relevant for the outcome of the dispute in relation to disclosure.

ESD: is an acronym for *eDocument* (see *ESI, Electronic Sources, File*).

ESI: is an acronym for electronically stored information or information stored in digital format (see *eDocument, Electronic Sources, File).*

ESI, active: refers to *ESI* that is accessible to *Custodians* within a computer or a *Network* without any need to access *Back-up ESI*.

ESI, inactive: refers to *ESI* that is not accessible to *Custodians* within a computer or a *Network* and requires access to *Back up ESI.*

Extranet: see *Intranet*.

File: refers to a finite sequence of bytes representing information that are flagged as pertaining to this *File* when used in relation to computing. *Files* are normally stored for a certain duration on a storage medium. *Files* are part of the *File System*. Each *File* has an identifier (e.g. *File Name*) that must be unique within the *Directory* where it is located. The name is followed by a suffix describing the *File Type*.

Unless a *File* is "flagged" to restrict certain operations such as deletion, the operating system is enabled to carry out read/write, renaming and deletion or erase actions. Apart from *Files* incorporating executable program codes, the arrangement of the information in a *File* is defined for the *File* to be used by a program such as a word-processor or media player. The type of program to which the *File* pertains may in such case be seen from the suffix. Without the correct program, the information may not be extracted correctly from the *File* and information cannot be correctly written into the *File* without expert knowledge and special tools.

Although a *File* is treated within a computer system as single logical entity, this does not mean that it is stored as one single sequence on the storage medium. Depending on the way storage is organized on such a medium, a *File* may be stored in blocks of bytes at different logical locations on the storage medium. Logical flags and indices used by the operation *Software* manage these blocks (see *File Fragment*).

File, active: is not a technical term and refers to a *File* that is not archived and may be accessed by a *User* with the required rights during normal operations.

File, accessible: is not a technical term and refers to a *File* that is accessible to a *Custodian*. Unless there are legal impediments, *active Files* are accessible. *Deleted Files* are normally no longer accessible to programs, including *Search Tools*, or may only be accessible with unreasonable effort using dedicated recovery tools, since they have disappeared from the *File System*. *Erased Files* are inaccessible unless dedicated tools used by *Computer Forensics* can recover all or some fragments from a *Data Carrier.* The required effort may be unreasonable, especially if the purpose of the search is not defined. Finally, a *File* may be inaccessible to a certain person or entity because that person or entity no longer has physical access to or the legal right of access to the computer/system to which the *Data Carrier* on which the *File* is stored is related.

File, deleted / erased: see *Data Deletion, Data Erasure*.

File Name: refers to a unique and arbitrary identifier for a *File* within a *Directory* of a *File System*. Depending on the operating system a *File Name* must comply with certain requirements. Certain applications, such as word-processors, allow *Users* to determine the prefix of the *File Name*. It is good practice to use a meaningful and systematic approach to naming *Files*. Automatically created *Files* are assigned prefixes consisting of strings in accordance with a programmed naming system. Today, the prefix is followed by a dot and a suffix (file extension/type) that is normally assigned automatically. This suffix indicates the *File Format*.

Active Files can easily be searched in a *File System* on the basis of their (truncated) *File Name* using available *Search Tools*.

File Format: refers to the *File* type represented by the suffix. The suffix indicates to *Users* the programs and what kind of programs should be enabled to properly extract, use/manipulate, visualize or make audible the information in the *File*, since the structure and arrangement of the bytes in the *File* have been defined by the programmer to be used by that specific program or kind of programs. Certain *File* types have been subject to considerable standardization efforts but others are proprietary. If a *User* knows the file extension he or she can search the corresponding program(s) on the Internet (see e.g. <http://www.file-extension.com>, <http://www.filext.com/>, <http://www.file-extensions.org>).

File Fragment: refers to a block of data pertaining to a *File*. When *Data Recovery* is carried out, *File* fragments are retrieved, identified and reassembled to the extent that this is technically possible (see *Computer Forensics*),

File Repository: refers to a logical place, normally accessible via a *Network*, where *Files* are stored for retrieval. In most instances, the *User* accesses the *File Repository* through the interface of dedicated document management *Software* (DMS) that is either locally installed (in part) or via the web browser and allows *Files* to be uploaded, downloaded, visualized and processed, depending on *User* rights, which can often be defined down to the level of a particular *File*. The DMS normally comprises relational data *Software* allowing additional information to be associated with any *File* and versions and *User* access to be tracked. In most cases the *Files* in the *File Repository* are presented to the *User* in a hierarchical structure of folders that resembles the structure of the *File System*, even if the actual visual representation may be more sophisticated. The DMS usually allows complex search operations and can include functions such as optical character recognition (OCR).

File Repositories may be particularly useful for disclosure of *eDocuments* and/or electronic filing.

File System: refers to a defined system by which electronic data in *File Format* is organized for access, processing and storage. On a *PC* the *File System* may be visualized by icons that are mostly arranged in a hierarchical structure comprising *Directories*, sub-*Directories* and *Files*, which reside in physical *Data Carriers*.

However, there are also virtual *File Systems* that overlay more specific *File Systems*, each of which may have a different specification according to the interface provided by the virtual *File System*. Global *File Systems* are cluster-*File Systems* that comprise *Directories* and *Files* on a multitude of physical *Data Carriers* within a storage data area *Network*. *Network File Systems* support *File* sharing over a *Network*, mostly by using a *Server*.

Format, of submission for eDocument: refers to the *File Format* in which *eDocuments* are filed with the arbitral tribunal. *eDocuments* are often submitted to the arbitral tribunal as a print-out or, if provided in digital format, as a PDF copy, since it is reasonable to submit *eDocuments* in a format that any addressee (other parties, arbitrators) can open and read without needing to subscribe to special *Software*, which may not otherwise be easily available on acceptable conditions. However, this approach may sometimes not be useful due to the particular nature of the *eDocument* or because the original version of the *eDocument* includes relevant *Metadata* that would not be preserved if the *eDocument* is produced in a different easily accessible *Format*.

Format, of disclosure of eDocument: refers to the *File Format* in which *eDocuments* are disclosed to the other side. The *File Format* for disclosure may, but need not necessarily be the same format which is used for submissions to the arbitral tribunal. Sometimes it is suggested that *eDocuments* be disclosed in their original format, so that all *Metadata* included in the "original" *eDocument* is preserved. However, unless the recipients of disclosed *eDocuments* already have a licence to the *Software* to which the original format pertains, such party may have difficulty accessing the information in the *File* with reasonable effort.

Handheld Devices (Blackberry): refers to small data-processing units that are small enough to fit into a person's hand and are from time to time, or most of the time, connected to a *Network* (mobile telephone *Networks*, WLAN, Bluetooth, USB, etc.) for communication purposes. *Handheld Devices* are extensively used for text messaging, *email* or instant messaging (SMS). In- and outgoing messages are stored on the mobile device for a variable duration, depending on the *Data Carrier* that may be built into the device, or may be exchangeable (see *Archived Electronic Source, Custodian*).

Internet: refers to the global *Network* of computers consisting of a decentralized structure of *Networks*, comprising hard- and *Software* within which connected computers can exchange data, using the standard Internet protocol suite (TCP/IP). The *Internet* comprises various services/application types, such as the *World Wide Web*, *email*, *File* transfer (e.g. using FTP).

Intranet: refers to a *Network* that is used to communicate and share information in electronic format among a defined group of *Users* related to an organization, normally a company or a group of companies. However, persons or entities that do not belong to the organization but interact with it, such as suppliers and customers, may have certain rights to access information within the *Intranet*. An *Intranet* usually interfaces with the *Internet*. Sometimes a distinction is made between an *Intranet*, whose *Users* are attached to the organization, and an extranet, which includes the aforementioned external *Users*.

In any event, virtualization removes the need to distinguish between *Inter- Intra-,* and extranets, since what matters is the access to the *Networks* defined by the *User* ID, password, and rights of access to a secure environment (data encryption) that has been defined as a *Network*.

Laptop: refers to a kind of portable *Personal Computer.*

Legacy Hard- and Software: refers to older hard- and *Software* that has become obsolete due to technical progress and is not fully compatible with the system now used by the organization in question. Such outdated hard- or *Software* may be kept available within organizations for the purpose of accessing *Back-ups* or other *ESI*.

Local Means of Storage: local refers to system devices or computers that are located at the workplace of the *Custodian*, e.g. a *Laptop* or *Personal Computer*. Means of storage refers to *Electronic Means of Storing or Recording Information.*

Mainframe Computer: refers traditionally to high-performance central computers run by big organizations that were accessed via terminals. Today, *Mainframe Computers* operate in *Networks* using *Internet* protocols and may host *Network Servers*.

Metadata: refers to data that is related to other data, such as *Files*, and describes attributes thereof. Certain *Metadata* provides book-keeping information within *File Systems*, such as *File* creation, modification, storage dates, *File Format*, access permission settings, and can often be easily visualized. Other *Metadata* depends on the *File Format* and/or the application *Software* environment. *File Repositories*, case management *Software* and other applications use database *Software* for creating, managing and storing arbitrarily defined categories of *Metadata*.

Network: (also referred to as "Computer Network") may refer to the cables and devices by which computers and peripherals are connected and can exchange data. *Networks* can be classified as Local Area *Network* (LAN), Wide Area *Network* (WAN), Virtual Private *Network* (VPN), etc. However, the relevant hardware and *Network Software* constitute only the *Network* infrastructure, since the devices relate to a specific *Network* only because they were arbitrarily made to do so. For this purpose each device has a unique identifier and defined access rights within the *Network* to which the *User*'s rights correspond. A device that is not "flagged" as being part of the *Network* does not belong to it.

Network Server: refers to a *Server* that is linked to a specific *Network*.

Original, of Electronic Document: see *Authenticity, Copy, File.*

Personal Computer (PC): refers to "stand-alone" computers, such as desktop computers, *Laptops*, etc. These computers are characterized by consisting of hard- and *Software* that allows them to be used independently of a *Network* connection. Prior to the advent of *PCs*, *Mainframe Computers*, to which *Users* connected via terminals without local storage capacity, were used. Today, *PCs* are nearly all permanently or temporarily connected to *Networks*, and the *Software* they use is not always or not completely installed locally. More importantly, data processed on a *PC* may not be stored, or not permanently stored, on a local *Data Carrier,* but also be held on *Network* storage devices.

PDA: is the abbreviation for personal digital assistant and means a mobile *Handheld Device*. Technologically, PDA's merge into mobile communication devices such as smart phones like Blackberry's, iPhones and the like.

Search Tool: refers to *Software* for *Data Mining*. The technical sophistication of such tools for predictably reliable results is crucial, since the tool must allow complex (multi-criteria) search operations and be capable of using these on a maximum of *File Formats* or at least those formats in which the *ESD* that are searched will in all likelihood exist. It is important to know that while many *File Formats* contain information that is directly machine readable (i.e. using search words), bit map *File Formats* (digital photocopies) may not be searchable unless converted using optical character recognition (OCR).

However, the best *Search Tool* will provide only results of a quality that is determined by the quality of the search instructions. Thus, search methodology is crucial, and transparency in this regard is commendable.

Server: sometimes refers to a dedicated computer that is connected to a *Network* on which *Server* applications are running. However, the term essentially refers to *Computer Programs* providing services to other *Computer Programs*, usually in a *Network* by using *Network* protocols. *Server* programs may run on *Mainframe Computers*.

In the context of *eDisclosure* it is important to know that much data exchanged inside or outside an organization is managed by a *Server*. The storage media where such data is held may be directly connected to the computer on which the *Server* runs. However, the trend is to have *Servers* run in virtual operating system environments, i.e. in an environment where devices are logical and to a certain extent disconnected from the actual hardware, allowing processed and/or stored data to move around or to be stored in several physical locations. The metaphor for this delocalized existence is "cloud".

Shared Server: is a *Server*, normally a *Network Server,* hosting *ESI* for defined groups of *Users* having defined rights with regard to the hosted data.

Software: see *Computer Programs*.

User: is a logical entity possessing the access rights for using a computer or *Software* or accessing a *Network*. A *User* may have the right to carry out any operation (e.g. system administrator) or be assigned restricted rights (e.g. normal *User*) with regard to operations and/or access to *ESI* for which usage restrictions have been implemented. For managing *User*-rights, systems use *User*-names (*User*-ID) and access codes (e.g. passwords or biometrical data). A physical person possessing such access information will be treated by the system as the logical *User* with whom this set of data is associated and is also called *User*. Depending on the assigned rights, a person who is a *User* may be a *Custodian*.

Version History: refers to the different stages of "existence" of data, especially *Files*, such as creation or modification dates. Certain basic historic information is nearly always stored as *Metadata*. Depending on the *Format*, or the *Software* used, historic information may be more complete. *File Repositories* and other dedicated *Software* systems (e.g. case-management systems) may store data including the complete *Version History* of a *File* and, possibly, any different versions of such *File*.

WAN: is an acronym meaning Wide Area *Network* (see *Network, World Wide Web*).

World Wide Web: refers to the global *Network* of hypertext pages served through *Servers* via the *Internet* according to agreed standards and includes small *Software* programs and services that enable a vast array of operations via the *Internet*.

ICC COMMISSION ON ARBITRATION AND ADR

The ICC Commission on Arbitration and ADR is ICC's rule-making and research body for dispute resolution services and constitutes a unique think tank on international dispute resolution. The Commission drafts and revises the various ICC rules for dispute resolution, including the ICC Rules of Arbitration, the ICC ADR Rules, the ICC Rules for Expertise and the ICC Dispute Board Rules. It also produces reports and guidelines on legal, procedural and practical aspects of dispute resolution. In its research capacity, it proposes new policies aimed at ensuring efficient and cost-effective dispute resolution, and provides useful resources for the conduct of dispute resolution. The Commission's products are published regularly online, in the *ICC International Court of Arbitration Bulletin* and as individual booklets.

The Commission brings together experts in the field of international dispute resolution from all over the globe and from numerous jurisdictions. It currently has over 600 members from more than ninety countries. The Commission holds two plenary sessions each year, at which proposed rules and other products are discussed, debated and voted upon. Between these sessions, the Commission's work is often carried out in smaller task forces.

The Commission aims to:

- Promote on a worldwide scale the settlement of international disputes by means of arbitration, mediation, expertise, dispute boards and other forms of dispute resolution.
- Provide guidance on a range of topics of current relevance to the world of international dispute resolution, with a view to improving dispute resolution services.
- Create a link among arbitrators, counsel and users to enable ICC dispute resolution to respond effectively to users' needs.

ICC Commission on Arbitration and ADR
www.iccwbo.org/policy/arbitration
arbitration.commission@iccwbo.org
T +33 (0)1 49 53 30 43
F +33 (0)1 49 53 57 19

Chair of the Commission: Christopher Newmark
Secretary to the Commission: Hélène van Lith
Assistant to the Secretary: Claudia Pansa

Managing E-Document Production is a Report produced within the Commission Task Force on the Production of Electronic Documents in International Arbitration, whose participants are listed below.

Loretta Malintoppi and **Robert H. Smit**, Co-Chairs of the Task Force
Peter Wolrich, former Chair of the Commission
Francesca Mazza, former Secretary to the Commission

Task Force members by country represented:

Australia: Jonathan Barnett, Stuart Dutson, Douglas Jones
Austria: Florian Haugeneder, Christian Konrad, Barbara Helene Steindl, Maria Theresa Trofaier
Belgium: Herman W. Verbist
Bulgaria: Assen Alexiev
Brazil: Paulo Cezar Aragão, Lauro Gama
Chile: Juan Eduardo Figueroa Valdés
Colombia: Eduardo Silva Romero
France: Geneviève Augendre, Olivier Buisson, Emmanuelle Cabrol, Benoît de Roquefeuil, Jalal El Ahdab, Jean-Claude Goldsmith, Laurent Gouiffès, Benoît Le Bars, Daniel Noel, Tim Portwood, Daniel Schimmel
Germany: Richard H. Kreindler, Paul Salazar, Erik Schäfer, Rolf A. Trittmann, Fabian von Schlabrendorff
Greece: Antonias Dimolitsa
Hungary: Milàn Kohlrusz
Italy: Fabio Bortolotti, Andrew Colvin
Lebanon: Roland Ziadé
Lithuania: Renata Berzanskiene
Malaysia: Vinayak P. Pradhan
Mexico: Laura Altamirano López, Cecilia Flores-Rueda, Carlos Jeffrey McCadden Martínez, Claus von Wobeser, Rodrigo Zamora Etcharren
Netherlands: Pieter Sanders
New Zealand: Stephen Jagusch
Sweden: Lars Perhard
Switzerland: Jacques Beglinger, Roberto Dallafior, Felix Dasser, Christopher P. Koch, Bernhard F. Meyer, Philippe Preti, Michael E. Schneider, Marc Veit,
Tunisia: Fathi Kemicha
United Kingdom: Sanjay Bhandari, Peter Cresswell, Michael Davison, Dorothee Heinze, Christopher Newmark, Matthew Saunders
United States of America: C. Mark Baker, Stephen R. Bond, Jeffrey Dasteel, Donald G. Gavin, David M. Greenwald, Hugh E. Hackney, Bryan E. Hopkins, Philip Lacovara, Sarah Loscher, Thomas M. Mueller, Eridania Perez, David W. Rivkin, Tyler Robinson, John D. Roesser, John L. Sander, Victoria Shannon, Josefa Sicard-Mirabal, Jonathan D. Siegfried, Stephen E. Smith, Suzanne Ulicny, Sharon Zealey

ICC Publication 860-0 ENG
ISBN 978-92-842-0158-7