

1	Key Points	2
2	Introduction	2
3	Electronic Discovery.....	2
4	Information Management	4
5	Identification.....	6
6	Preservation and Collection	7
7	Processing, Analysis and Review	9
8	Production and Presentation.....	12
9	Closing Remark	13

1 Key Points

- (a) Proactively approach e-discovery to avoid unnecessary risk, time and cost
- (b) Learn efficient strategies for managing discovery involving electronic documents
- (c) Understand the role of a computer forensics expert in relation to e-discovery

2 Introduction

“A cigarette packet carries the warning that smoking can kill you. Solicitors’ standard terms of business should carry a warning that litigation can cost you.”

Lord Justice Ward in *Hedrich & Anor v Standard Bank London Ltd & Anor*.¹

Discovery often attracts criticism as the most time and cost intensive process of litigation. The recent England and Wales Supreme Court of Appeal decision of *Hedrich* is one of the increasing case law examples where a lawyer and/or their client has mismanaged discoverable electronic documents. Such examples often result in significant litigation inefficiency, and at worst, an unfavourable judgment.

This article introduces electronic discovery (“**e-discovery**”) with a stage-based framework. Further, it outlines the supportive role performed by a computer forensics expert for a lawyer (or legal team) and their client to efficiently discharge their obligations where electronic documents are subject to an order for discovery.²

3 Electronic Discovery

Defining E-Discovery

E-Discovery can be defined within two meanings:

- (a) **Traditional E-Discovery** – The management of discoverable paper documents by conversion to electronic form; and
- (b) **Modern E-Discovery** – The management of discoverable electronic documents in electronic form.

E-Discovery is not exclusive to either definition. It is also important to note that courts increasingly understand the value of retaining electronic documents in electronic form, rather than parties undertaking an expensive printing and photocopying exercise. Consequently,

¹ *Hedrich & Anor v Standard Bank London Ltd & Anor* [2008] EWCA Civ 905.

² O 24, Rules of Court.

the production of electronic documents in paper form has the real potential to give rise to a failure to comply with discovery.

Defining Electronic Documents

The concept of a “document” is broadly defined in the *Evidence Act*.³ The definition is interpreted to include electronically stored information (“**ESI**”), not limited to documents, spreadsheets, databases, images and other electronic data files.⁴

Defining Electronic Form

An electronic document may be represented in its native format, or as an electronic image. The production of a Microsoft Excel spreadsheet in Microsoft Excel spreadsheet format is its native form and includes spreadsheet data, any formulas populating the spreadsheet and metadata. The production of that same Microsoft Excel spreadsheet as a Portable Document Format (“**PDF**”) or Tagged Image File Format (“**TIFF**”) is an electronic image representation of the spreadsheet data only, typically without any formulas or metadata.

Electronic documents can be produced in their native electronic form, as an electronic image, or printed to paper form. In contrast, paper documents can only be produced in paper form, or as an electronic image.

Defining Metadata

The typical electronic document consists of three layers: data, structure and metadata. Metadata is the primary difference between an electronic document in its native form, and the same electronic document converted to an electronic image or printed to paper. Metadata is generally described as any descriptive information related to an electronic document.

For example, Microsoft Word document has the actual text typed (data), any formatting applied (structure) and embedded information (metadata). Such metadata often provides particulars such as authorship, creation date, revision history and any tracked changes.

Defining Protocols

Protocols exist to establish guidelines and agreement in various aspects of the discovery process. A “Search Protocol” defines how searches for electronic documents are to be performed. In contrast, a “Document Management Protocol” defines the production format for discoverable documents. It is strongly recommended that any protocols be agreed upon between the parties, and accepted by the Court, at the earliest opportunity following the commencement of proceedings and prior to any order for discovery.

³ *Evidence Act* (Cap 97, 1997 Rev Ed) s 3(1).

⁴ *Megastar Entertainment Pte Ltd & Anor v Odex Pte Ltd* [2005] SGHC 84; *Alliance Management SA v Pendleton Lane P & Ors* [2007] SGHC 133.

Electronic Discovery Reference Model

The Electronic Discovery Reference Model (“EDRM”) provides a jurisdiction-neutral, nine-stage framework for e-discovery management.⁵

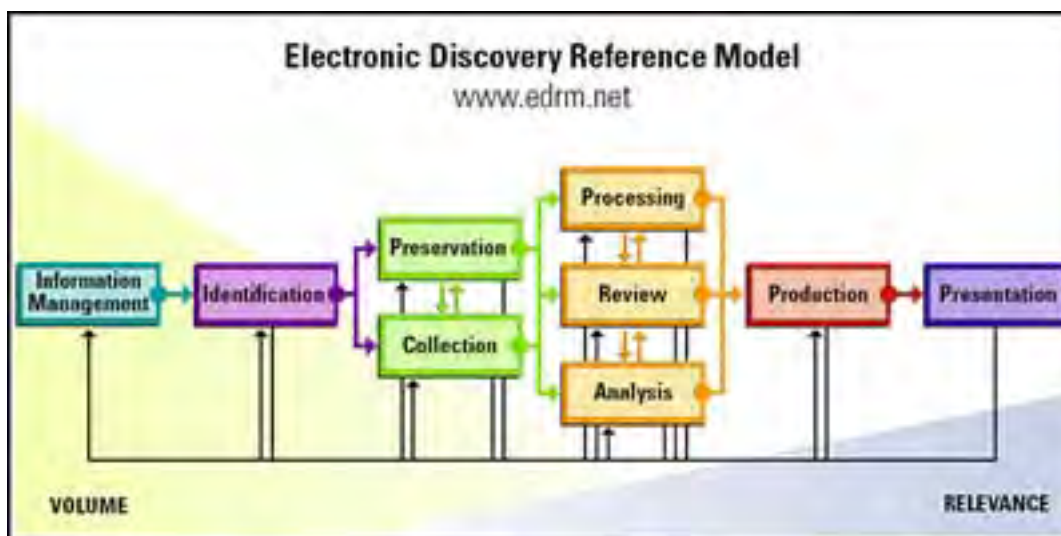


Figure 1 - Image Copyright 2005-2007. Socha Consulting LLC and Gelbmann & Associates.

4 Information Management

It is estimated that 98 percent of all business correspondence and documents are created and stored in electronic form. The vast majority of such electronic documents are never converted to paper. Due to the volatility of electronic form, even routine computer system administration processes, such as using the Microsoft® Windows Disk Cleanup software utility, can delete or overwrite electronic documents without direct human intervention.

In *Hong Leong Singapore Finance Ltd v United Overseas Bank Ltd*⁶, the need for solicitors to proactively educate their client as to the duty of discovery and the importance of preserving potentially discoverable documents was emphasised.

In *Tan Chor Chuan & Ors v Tan Yeow Hiant Kenneth & Ors*⁷, an application to impose an adverse inference sanction on a party was dismissed, where the organisation successfully asserted that the deletion of discoverable e-mails occurred as part of “ordinary practice” and in apparent good faith, prior to notice of litigation.

The efficiency with which you can manage your client’s discovery is largely subject to your knowledge and their information management practices. Information management entails all of the preparatory actions undertaken, prior to notice of litigation, by your client’s organisation

⁵ <http://www.edrm.net>

⁶ [2007] 1 SLR 292 (Menon JC).

⁷ [2004] SGHC 259 (Low AR).

to manage electronic documents within their control. A diligent approach to implementing an information management strategy typically includes the following:

- (a) Policy;
- (b) Technology Infrastructure;
- (c) Training;
- (d) Litigation Checklist; and
- (e) Regular Review.

Policy

A Document Retention Policy (“**DRP**”) details the time period that a particular type of document created or managed by an organisation will be retained for, prior to deletion or destruction.

Technology

The size, structure, industry, resources, budget and any existing technology infrastructure of your client’s organisation will dictate the requirements for the implementation of any electronic document management system (“**EDMS**”) or similar.⁸

Every organisation should maintain a current inventory of technology and information assets. Further, every organisation should also possess at least one individual who can clearly provide documentation and explain to a lawyer or computer forensics expert, how electronic documents (including e-mails) are created, managed and archived.

Training

It is considered best practice for all employees, including internal contractors, to receive basic training as to the organisation’s **DRP**, and how to use in-use technology, to manage electronic documents in a compliant manner.

Litigation Checklist

For organisations considered “active litigants” or “litigation prone”, it is also advised to implement a checklist of actions to be performed when notice of litigation is received. A litigation checklist should specify the:

- (a) Primary contact for internal litigation management;
- (b) Process for the primary contact to communicate with internal and external stakeholders, as required;
- (c) Process for the engagement of external legal counsel;

⁸ Large organisations may also consider the need for implementation of dedicated e-discovery management infrastructure.

- (d) Process for the engagement of litigation support resources (e.g. internal technology department, external computer forensics provider, photocopy or scanning bureau); and
- (e) Process for identifying and subsequently preserving potentially discoverable documents, pending an order for discovery (i.e. “litigation hold”).

Regular Review

Regular reviews demonstrate a commitment to good corporate governance. Further, a review serves the critical purpose of assessing compliance with an information management strategy.

5 Identification

The Identification stage is concerned with the ability to identify potentially discoverable documents prior to preservation and collection, and subject to the particulars of an order for discovery.⁹ The term “*potentially relevant*” is used, as a specific computer may need to be identified in the first instance, prior to review. This is akin to identifying a potentially relevant archive box or folder, where only a small number of documents may actually be reviewed as relevant.

With electronic documents, the process of identifying potentially discoverable documents within your client’s possession, custody or power, is often compounded by the complexity of understanding their information management strategy, during the relevant discovery time periods.

Where the relevant discovery time periods are over a number of years, the process of identification must be thorough and account for all potentially relevant custodians. This may include both current and former employees or contractors. The process may also involve retracing the lifecycle of multiple computer systems.

In *Raffles Town Club Pte Ltd v Lim Eng Hock Peter & Ors*¹⁰ (“**Raffles**”), Justice Kan considered an appeal in relation to an order for discovery due to purported excessive width and oppression. His Honour noted that such issues were to be viewed “*in the context of the circumstances*”.¹¹

In *Raffles*, the substance of the specific, significant claims, financial resources of the parties and the tenacity of the parties’ litigation conduct to date was considered.¹² The appeal was dismissed on the basis that discovery had been restricted to specific classes of documents, and that the tenacious conduct of the parties suggested that the “*facts and issues will be fully*

⁹ O 24, *Rules of Court*.

¹⁰ [2008] SGHC 141.

¹¹ *Ibid*, [18].

¹² *Ibid*, [20].

examined and contested at trial". Further, that the order for discovery satisfied the overriding principle as being "*necessary either for disposing fairly of the cause or matter or for saving costs*".¹³

Consultation with a computer forensics expert provides the ability to combine your legal acumen with their technical knowledge, to objectively assess the arguments for and against an order for discovery related to electronic documents.

For example, as a solicitor, you may be faced with an order for discovery of an entire database in circumstances where only specific records are potentially relevant. The discovery of an entire database may impose significant cost and contain a significant volume of confidential and irrelevant information, which is difficult to make available for inspection, or to produce for review by other parties without a specifically configured database server. In contrast, it may be mutually beneficial to search the database for records matching an agreed database search query criteria and for such records to be produced in a common electronic form.

Alternatively, the cost in recovering deleted e-mails or e-mails from backup tapes can impose significant time and cost burdens for a party. A computer forensics expert may be able to advise as to cost estimates or assess the technology infrastructure to determine the likelihood of the e-mails being accessible in a more time and cost effective location.

The UK Practice Direction 31 also provides persuasive criteria for considering an order for discovery involving electronic documents.¹⁴

6 Preservation and Collection

This stage involves the preservation and collection of "potentially relevant" electronic documents. The key proposition is a risk mitigation exercise to balance the significance of the litigation against the internal resources, time, financial budget and risk adversity of the client.

Unlike paper documents, the ease in which electronic documents, and their associated metadata, may be altered (inadvertently or otherwise) has increasingly led to challenges as to their authenticity and accuracy. Further, even printing electronic documents to paper for the purposes of discovery may also give rise to such a challenge under the *Evidence Act*.¹⁵

¹³ *Ibid*, [15]; O 24, r 7.

¹⁴ UK Civil Procedure Rules, Practice Direction 31 – 2A.4.

See also: *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch).

¹⁵ *Evidence Act* (Cap 97, 1997 Rev Ed) s 35(1)(a).

In the recent case of *Alliance Management SA v Pendleton Lane P & Ors*¹⁶, Justice Ang held that, *inter alia*, the defendant's mismanagement of electronic evidence constituted an abuse of process to the Court, and justified striking out their defence, whilst imposing an order for the plaintiff's application costs.

A diligent preservation and collection process involves:

- (a) Collection Methodology; and
- (b) Chain of Custody.

Collection Methodology

"Copying" and "imaging" are the primary methods of electronic document collection.

Copying is the common method of transferring one or more electronic documents from one electronic storage location to another. Typically, copying is performed without using any specialised tools or methodology.

In contrast, forensic imaging, also simply referred to as "imaging", the process of making an "exact or bit level copy" of selected electronic documents, or an entire hard drive, using specialised tools and methodologies.¹⁷ In contrast to copying, the forensic imaging process makes an exact and verifiable copy of the original electronic documents, including all metadata.

When making a forensic image of a hard drive or other electronic storage medium, deleted data and unallocated data can also be preserved for recovery and analysis, as required. Traditionally, the forensic imaging process is undertaken when a computer is shut down or powered off. However, emerging technologies now enable a computer forensics expert to make a forensic image whilst a computer is still operating. This reduces downtime and liability that may arise if a mission-critical computer is unavailable for an extended period of time.

Chain of Custody

To avoid arguments around tainted evidence or spoliation, it is also essential to maintain chain of custody documentation for each electronic document, including any hard drive copied or forensically imaged, from time of collection, to the time it may be relied upon in court, or is subsequently destroyed.

In practice, your balancing exercise during the preservation and collection stage may involve your client's internal technology resources, the engagement of a computer forensics expert,

¹⁶ [2008] SGHC 76.

¹⁷ See also: *Megastar Entertainment Pte Ltd & Anor v Odex Pte Ltd* [2005] SGHC 84.

or a hybrid approach of both resources. Regardless of the method used it must ultimately be documented, whilst encompassing a defensible and repeatable process.

7 Processing, Analysis and Review

As the volume of electronic documents typically collected as part of satisfying an order for discovery increases, the practicality of performing a full manual review of each and every potentially relevant electronic document is tested. Technology, when used appropriately, preferably with the mutual agreement of all parties, and with diligent computer forensics experts, provides the ability to efficiently manage and make available for review significant volumes of documents.

Processing

Processing is a purely technical stage where documents are processed to a readable and useable form for legal analysis and review. Typical tasks include:

- (a) Scanning paper documents to electronic images;
- (b) Using Optical Character Recognition (“**OCR**”) to enable searchable text in unsearchable electronic images;
- (c) Extracting compressed data (e.g. electronic documents stored within ZIP archives or stored on backup tape); and
- (d) Extracting password-protected or encrypted electronic documents.

Analysis

Analysis is the use of search technologies to filter and reduce (“cull”) the volume of potentially relevant documents to a more focused set for review. This process may be subject to a “Search Protocol”.

The Analysis process is typically undertaken under the direction of a lawyer with technical assistance. Whilst a computer forensics expert is recommended, a lawyer ultimately requires someone who can clearly explain, if required to the Court, which electronic documents were searched, how they were searched and whether the search technologies used were subject to any known limitations.

Analysis may involve the use of one or more of the following filtering techniques:

Key Custodians or Locations

Filtering based on specific key custodians (e.g. individuals, departments, project groups) or key locations (e.g. computers and other information repositories) based on their likely relevance.

Date Ranges

Filtering by specific dates or date ranges. For example, all e-mails sent by John Smith between 1 March 2007 and 31 December 2007.

File Types

Filtering by specific electronic file types. For example, all Microsoft Excel spreadsheets.

Search Queries

Filtering using search queries in the form of keywords or phrases. Such queries can range from simple keywords to more complex Boolean searches¹⁸ and/or regular expressions¹⁹

In *Alliance Management SA v Pendleton Lane P & Ors*²⁰, a party produced 36,740 electronic documents following a search using 62 keywords. Justice Ang reminded the parties that the results of keyword searches must still be appropriately reviewed prior to production, *“it is not proper to list a large amount of documents retrieved from keyword searches for such an approach alone is insufficient and requires the other party to sort through them”*.

It is very important to diligently consider which keywords to use in order to avoid reviewing a significant number of irrelevant documents. For example, the word “the” and any number between 1 and 100 are not considered “good” keywords. In contrast, keywords and terms specific to the litigation are “good”.

It is also important to consider “sampling”. That is, testing a list of potential keywords over a limited set of electronic documents to ascertain the potential for returning relevant electronic documents. Sampling provides the ability to demonstrate to the Court a robust and diligent approach to using technology.

It is also crucial to understand any limitations of your search tools. A limitation may be the inability of a search tool to automatically search text stored in a graphical image file or that it is unable to accurately index and search one or more languages.

Emerging search technologies are becoming increasingly available to perform “concept searching”. That is, often using a dictionary, thesaurus and complex search algorithms, to identify all relevant documents based on a particular concept. For example, the keyword “java” may relate to a number of things, for example, a type of coffee, the computer programming language or the Indonesian island. Concept searching endeavours to understand the difference, and subsequently, return similar results. For example, in relation to the first meaning of java, documents matching coffee, Arabica, etc may be grouped together.

¹⁸ Boolean search operators include AND, OR and NOT.

¹⁹ Regular expressions are a method of using wildcards or other “limiters” to broaden or narrow search results.

²⁰ [2007] SGHC 133.

Search technologies are becoming available to perform search queries across audio files. This may facilitate searching recorded conversations and voicemail messages for discovery.

De-Duplication

A vast majority of electronic documents are duplicated across multiple computers and information storage repositories. Duplication has become commonplace as e-mails are sent to multiple recipients, documents are stored in multiple storage repositories and regular backups are made. De-duplication is the process of identifying and removing duplicate electronic documents. This is performed by “exact de-duplication” or “near de-duplication”.

Exact de-duplication is the calculation of a cryptographic hash value for a particular electronic document, effectively acting as a *digital fingerprint*, and comparing it with the hash value for another electronic document. At present, the most prevalent cryptographic hash function is the Message-Digest algorithm 5 (“**MD5**”).

Near de-duplication is an emerging technology that typically uses complex algorithms to identify and group electronic documents that are “similar”. For example, you may have a contractual precedent that you have used on ten different matters. Dependent upon the variables provided to the search tool and amendments to the precedent, you may typically expect for the precedent and the ten electronic documents to be grouped as a “near duplicate”.

Review

By the Review stage, you should have a reduced and refined set of documents for manual relevance review and classification (e.g. privileged, confidential).

Many solutions are available to facilitate document review. Document review platforms allow multiple reviewers, often in disparate locations via the Internet, to concurrently and securely review and classify document sets. Popular document review platforms include LexisNexis Concordance, EPIQ DocuMatrix, Autonomy ZANTAZ Introspect, kCura Relativity, FTI Ringtail Legal and Attenex Patterns.

The volume of electronic documents to review may lead to the inadvertent disclosure of privileged or confidential documents. In *Ser Kim Kor & Anor v Fulton William Merrell & Ors*²¹, Justice Prakash dismissed an appeal from a party who attempted to amend their filed list of documents by deleting privileged and irrelevant documents. Regardless of the solution used, it is essential to implement appropriate quality control measures to mitigate the risk of inadvertent disclosure.

²¹ [2008] SGHC 23.

8 Production and Presentation

Production

Production involves the drafting of a List of Documents and the inspection or exchange of electronic documents in a particular format, e.g. paper form, an electronic image format or their native, electronic form.

The format of production is often dictated by a “Document Management Protocol”.

If inspection is ordered following exchange of the List of Documents, an independent computer expert is typically appointed, subject to a confidentiality undertaking, to manage the maintenance of privilege, subject to any claims of the producing party, prior to production to the receiving party.²²

Presentation

Presentation involves the actual tendering of electronic documents as evidence in-court. You may consider making use of court technology resources.²³

²² *Alliance Management SA v Pendleton Lane P & Ors* [2008] SGHC 133.

²³ For example, in the Supreme Court of Singapore: <http://app.supremecourt.gov.sg/default.aspx?pgID=8>.

9 Closing Remark

“The overriding principle in discovery is that it must be either for disposing fairly of the cause or matter or for saving costs.”

Justice Tay in *Ting Kang Chung John v Teo Hee Lai Building Construction Pte Ltd*²⁴

The prevalence of electronic documents has presented new challenges to the discovery process. This article has provided a stage-based framework for e-discovery. Such knowledge provides the ability to proactively approach discovery and reduce the likelihood of technology advance overtaking the real legal issues and need for efficient dispute resolution.

Seamus E. Byrne²⁵ and Roger Clay²⁶

February 2009

²⁴ [2008] SGHC 54.

²⁵ Seamus E. Byrne is a Lawyer and Computer Forensics Expert. See: <http://www.seamusbyrne.com>.

²⁶ Roger Clay is a Computer Forensics Expert and Associate Director within the Fraud Investigation & Dispute Services practice of Ernst & Young Singapore.

© 2009 Seamus E. Byrne and Roger Clay. All Rights Reserved.