



# Discovery of Electronic Evidence

[Seamus E. Byrne](#)

Australian Lawyer and Computer Forensics Expert

**Please Read – Disclaimer**

This presentation is made available by [Seamus E. Byrne](#), an Australian legal practitioner, for educational purposes only. Content is not to be used as legal opinion or as a substitute to qualified matter-specific legal advice within your jurisdiction. All endeavours have been made to ensure content accuracy as at March 2009.

For the [Law Institute of Victoria](#) Practice Management CPD – 11 March 2009 – Australian English (Duration: 50 minutes, Public Draft)

# Today

---

- **Introduction**

- Your Presentation
- Your Presenter

- **Electronic Evidence**

- Electronically Stored Information (ESI)
- Technical Introduction (Storage, Deletion, Metadata)
- Legal Considerations

- **Computer Forensics**

- Definition and relevance
- Key Applications

- **Search Orders**

- Key Considerations
- Practice Guidelines
- Recent Case Law

- **Regulatory Investigations**

# Today

---

## ■ **Electronic Discovery**

- Definition
- Practice Guidelines (Notes and Directions)
- Costs
- Electronic Discovery Reference Model (EDRM) Workflow
  - Information Management
  - Identification
  - Preservation
  - Collection
  - Processing
  - Analysis
  - Review
  - Production
  - Presentation

# Your Presentation

---

- **Coverage**

- Civil Litigation
- Supreme Court of Victoria and Federal Court of Australia
- Guiding Principles and Best Practice

- **Primary Audience**

- Victorian Litigators

# Your Presenter

---

## ■ Seamus E. Byrne

- Lawyer and Computer Forensics Expert (CISSP, CCE, EnCE)
- E-Discovery advisor to a number of [S&P/ASX 200](#) companies
- Co-Author, LexisNexis [Federal Civil Litigation Precedents](#)
- Contributor, Federal Court of Australia's [revised Practice Note 17](#)
- [HP](#) 'Information Hero' for E-Discovery in the Asia-Pacific region

# Electronic Evidence

---

## Historical Perspective

- Almost all of civilisation has relied upon physical information storage
- **Document** (*documentum* = proof)
- Basic unit of **information storage**
- **Information** may form a **document**
- **Select documents** may form a **record**
- **Late 19<sup>th</sup> Century**
  - Second industrial revolution
  - Typewriters, carbon paper and filing cabinets
- **Today**
  - 98% of corporate documents are stored electronically
  - Most are never printed!

# Electronic Evidence

---

## Electronically Stored Information (ESI)

### ■ Ever-Increasing in Volume

- What size was the hard drive in your first computer? (e.g. 10MB or 10GB)
- Today, you can purchase a 1TB (1000GB) hard drive for under AUD\$150
- Printing 1TB of electronic documents requires 50,000 trees of paper!

### ■ Dynamic

- The content of an electronic document can change over time

### ■ Deletion

- Routine system administration processes (e.g. [Disk Cleanup](#)) can delete or overwrite electronic documents without human intervention

### ■ Distributed Storage

- If I send you an e-mail, in how many geographic and electronic locations will the e-mail be synchronised and stored to?

# Electronic Evidence

---

## Technical Introduction – Metadata

- Metadata is the **primary difference** between an electronic document in its native, electronic form and the same document printed to paper

### Microsoft Word Document

- Formatting
- Text
- **Metadata**
  - Title
  - Author
  - Date Created
  - Date Last Saved and Last Saved By
  - Date Last Printed
  - Track Changes (Comments, Revisions)

### E-mail Message

- Formatting
- Text
- **Metadata**
  - Sender
  - Recipients (To, CC, BCC)
  - Subject
  - Sent Date and Time
  - Attachment Information

# Electronic Evidence

## Technical Introduction – Electronic Formats

- The **same electronic document** can be produced in **multiple formats**

### Native, Electronic Format

- **Native Format**
  - Microsoft Excel spreadsheet as “XLS”
- **Searchable Text**
  - Typically searchable by default
- **Metadata**
  - Available, unless removed

### Electronic Image

- **Image Representation**
  - Paper
  - Electronic
- **Common Formats**
  - Portable Document Format (**PDF**)
  - Tagged Image File Format (**TIFF**)
- **Searchable Text**
  - Can be made searchable
- **Metadata**
  - Complete metadata may not be available

- Formats vary for electronic databases, complex and proprietary file types

# Electronic Evidence

---

## Technical Introduction – Storage and Deletion

- A **file system** is used to store, organise and retrieve data (i.e. ESI) on a **storage media** (e.g. hard drive)
- A file system commonly references data using an **index table**
- The **index table** contains a **directory listing** for **each active data file** (i.e.accessible, not deleted), to reference the location of the data file on the storage media
- **When a data file is deleted**, only the directory listing for the data file is generally deleted, and not the actual data file itself
- Dependent on a number of variables, the ‘deleted’ data file **may be recovered**
- In contrast, **secure deletion** or **overwriting** endeavours to permanently delete both the directory listing and the actual data file, making any data recovery process difficult, if not impossible

# Electronic Evidence

---

## Legal Interpretation – Commonwealth

- [Evidence Act 1995](#) (Cth) (*Dictionary, Pt 1; Pt 2, Cl 8*)
  - “**Document** means any record of information, and includes:  
*Anything on which there is writing, or  
Anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them, or  
**Anything from which sounds, images or writings can be reproduced with or without the aid of anything else, or  
A map, plan drawing or photograph.***”
  - Includes any **part, copy**, reproduction or duplicate of a document
- [Acts Interpretation Act 1901](#) (Cth) s 25
- [Federal Court Rules](#) (O 1, r 4)
  - Commonwealth Evidence Act definition, and expressly includes:
    - **Any ...data or information stored or recorded by ...electronic means**

# Electronic Evidence

---

## Legal Interpretation – Victoria

- *Evidence Act 2008* (Vic)
  - Uniform Evidence Law definition of a ‘document’ applies
  - cf *Evidence Act 1958* (Vic) s 3
- *Interpretation of Legislation Act 1984* (Vic) s 38

# Electronic Evidence

---

## Legal Interpretation – Relevant Case Law

- **Discovery of electronic documents**
  - *NT Power Generation v Power and Water Authority* [\[1999\] FCA 1669](#) (Mansfield J)
- **The electronic storage medium as a ‘document’**
  - *"Electronic records, such as computer files and CD-ROMs have been the subject of discovery orders in this Court"*: ***Sony Music Entertainment v University of Tasmania*** [\[2003\] FCA 532](#) (Tamberlin J)
- **Metadata is ‘part’ of a ‘document’**
  - *"It is clear that embedded electronic information in relation to relevant documents, including the information embodied in electronic metadata, is discoverable"*: ***Jarra Creek Central Packing Shed v Amcor*** [\[2006\] FCA 1802](#) (Tamberlin J)

# Electronic Evidence

---

## Legal Considerations

- **Relevance**
  - Regardless of the form, evidence must go to a fact in issue
- **Chain of Custody and Evidence Copies**
  - Manage in a documented manner without (or with minimal) alteration
  - Take appropriate evidence management procedures, including physical security
- **Expert Opinion and Testimony**
  - May require specialist expertise not readily possessed by everyday IT personnel
  - **DO NOT** turn on “potentially relevant” computers without the assistance of an expert – may result in alteration or loss of data: *Egglishaw v ACC* [\[2006\] FCA 819](#)
- **Best Practice**
  - [Guidelines for the management of IT Evidence](#) (HB171-2003), Standards Australia
- **Privilege Management**
  - **REMEMBER** privilege attaches to confidential communications as information, and not documents as such

# Computer Forensics

---

## Introduction

Identify

Preserve

Analyse

Present

- *“The process of identifying, preserving, analysing and presenting **electronic evidence** in a manner that is legally acceptable in any judicial or administrative hearing”* ([Australian Institute of Criminology, 1999](#))
- Also commonly referred to as digital forensics, forensic computing or forensic technology
- **Not limited to ‘mere computers’**
  - Computer networks and the Internet
  - Communication devices (Mobile Phone, PDA, Satellite Navigation Systems)
  - Consumer devices (iPod/MP3 Players, Digital Cameras, Digital Voice/Video Recorders)

# Computer Forensics

---

## Key Applications

- **Interim Orders (e.g. Search Orders)**

- Identifying artifacts to confirm activities (e.g. connected USB devices, deleted data, etc.)

- **Electronic Discovery**

- Identification, Preservation and Collection

- **Authenticity of Electronic Documents**

- Forensic analysis of document metadata revealed that a number of invoices purportedly raised on specific dates, were backdated: *ASIC v Loiterton & Ors* [\[2004\] NSWSC 172](#)

- **Source or Authenticity of E-mail**

- Tracing the source of 'anonymous' defamatory e-mail messages: *Boniface v SMEC & Ors* [\[2005\] NSWSC 1099](#); [\[2006\] NSWCA 351](#)

- **Breach of Confidence and Intellectual Property (IP) Infringement**

- Sending confidential information to a **personal e-mail address**: *Austress Freyssinet v Joseph* [\[2006\] NSWSC 77](#)
- Copying confidential information to a **portable hard drive**: *AAS v Korchinski* [\[2007\] FCA 12](#)

- **Computer Usage and Activity**

- Breach of employer's **computer use policy**: *Lewis v Toyota Motor Corporation* [\[2001\] AIRC 213](#)

# Search Orders

---

## Key Considerations and Practice Guidelines

- Traditionally known as Anton Piller Orders
- Part of '*harmonisation of court rules*' project undertaken by the Council of Chief Justices of Australia and New Zealand
  - Revised [Federal Court of Australia Practice Note 24](#) (5 May 2006)
  - [Supreme Court of Victoria Practice Note 2 of 2006](#) (1 September 2006)
  - Formally introduced **the Independent Computer Expert (ICE)**
  - **Increased obligations** for all parties involved in a Search Order
- **Further Information**
  - '[Search Orders - Okay Computer?](#)', The Australian Corporate Lawyer, March 2008

# Search Orders

---

## Recent Case Law – Highlights Common Issues

- ***Metso Minerals (Australia) Ltd v Kalra*** [\[2007\] FCA 2093](#)
  - *“The circumstances in which confidential information has been accessed, presumably downloaded or transferred, and thereafter deleted from computers is sufficient to found a conclusion that there is a real possibility that evidence will be destroyed if the orders now sought are not made”*
- ***Metso Minerals (Australia) Ltd v Kalra (No 2)*** [\[2007\] FCA 2108](#)
  - Requested extension of time for Independent Computer Expert (ICE) to facilitate Search Order due to volume of ESI for preservation
- ***Jemella Australia Pty Ltd v Young (No 3)*** [\[2008\] FCA 579](#)
  - *“Unfortunately, in this particular case, the independent computer experts seem to have misdirected themselves about their duties and responsibilities under the orders...”*
- ***Aristocrat Technologies v Global Gaming Supplies*** [\[2006\] FCA 1707](#)
  - Highlighted importance of proactively devising a method for the review of ESI, particularly for privilege (280,000 electronic documents, 60,000+ e-mail messages)

# Regulatory Investigations

---

## Key Considerations and Recent Case Law

### ■ Search Warrants

- [Crimes Act](#) (Cth) s 3E warrants:
  - Three (3) conditions, seizure and removal (72 hour rule)
- *Oke v Cmr, AFP* [\[2007\] FCA 27](#)
  - Highlighted practical issues
- *Different Solutions Pty Ltd v Cmr, AFP (No 2)* [\[2008\] FCA 1686](#)
  - Liberal judicial interpretation of powers to seize or copy ESI

### ■ Other Coercive Information Gathering Powers (s263 [ITAA](#), s155 [TPA](#))

- *JMA Accounting v Cmr, Taxation* [\[2004\] ATC 4916](#)
- *Prescience Comms Ltd v Cmr, Taxation* [\[2006\] FCA 1561](#)
- *A. B. Pty Ltd v ACC* [\[2009\] FCA 119](#)

### ■ Further Information

- Australian Law Reform Commission, [Privilege in Perspective](#), Report 107 (2008)

# Electronic Discovery

---

## Definition

### ■ Discovery

- *“the disclosure, and subject to privilege, the inspection of an opponent’s documents;*
- *written interrogatories seeking admissions from an opposite party;*
- *procedures that resemble discovery, namely the inspection of the subject matter of the proceedings...and the preservation of evidence”*  
(Cairns, [Australian Civil Procedure](#) (7<sup>th</sup> ed, 2007) p 271)

### ■ Traditional Electronic Discovery

- **Conversion** of paper documents into an electronic format for production

### ■ Modern Electronic Discovery

- **Management** of electronic documents in an electronic format for production

### ■ Today = Transitional Phase

# Electronic Discovery

---

## Practice Guidelines (Notes and Directions)

---

Jurisdiction	Practice Guideline
<b>Federal Court of Australia</b>	<a href="#">PN 17 (2009)</a>
Supreme Court of New South Wales General	<a href="#">PN SC Gen 7 (2008)</a>
Equity Division (Select Lists)	<a href="#">PN SC Eq 3 (2008)</a>
<b>Supreme Court of Victoria</b>	<a href="#">PN 1 (2007)</a>
Supreme Court of South Australia	<a href="#">PD 2.1 (2006)</a>
Supreme Court of Queensland	<a href="#">PD 8 (2004)</a>
Supreme Court of the Northern Territory	<a href="#">PD 2 (2002)</a>

---

- The Supreme Courts of Western Australia, Tasmania and the Australian Capital Territory are yet to formally release similar practice guidelines

# Electronic Discovery

---

## Revised Federal Court of Australia PN 17, Visual Guide

- **Subject to Court's discretion**, the Practice Note applies at discovery and trial where there is likely to be over 200 electronic documents
- **DOES** provide a framework for parties to agree upon and manage discovery
- **DOES NOT** impose any new discovery obligations, **but re-emphasises**:
  - Need for parties to preserve discoverable electronic documents
  - Performance of a reasonable search per existing [Court Rules](#) and [PN 14](#)
- Court **may order** Pre-Discovery Conference (**PDC**)
  - Parties “meet and confer”
  - Parties may appoint an expert to assist
  - Reference the [Pre-Discovery Conference Checklist \(PDCC\)](#)
  - Parties endeavour to provide Court with mutually acceptable Discovery Plan
- Court **may order** parties to give discovery
- Please refer to [Visual Guide to Practice Note 17](#)

# Electronic Discovery

---

## Revised Federal Court of Australia PN 17

- **Pre-Discovery Conference Checklist (PDCC)**
  - Scope of Discovery
  - Reasonable Search (and Reasonably Inaccessible)
  - Preservation
  - Time Schedule and Cost Awareness
  - Privilege Management
  - Document Management Protocol (Default or Advanced)
  - Areas of Dispute

# Electronic Discovery

---

## Supreme Court of Victoria PN 1 of 2007, Costs

### ■ Practice Note 1 of 2007

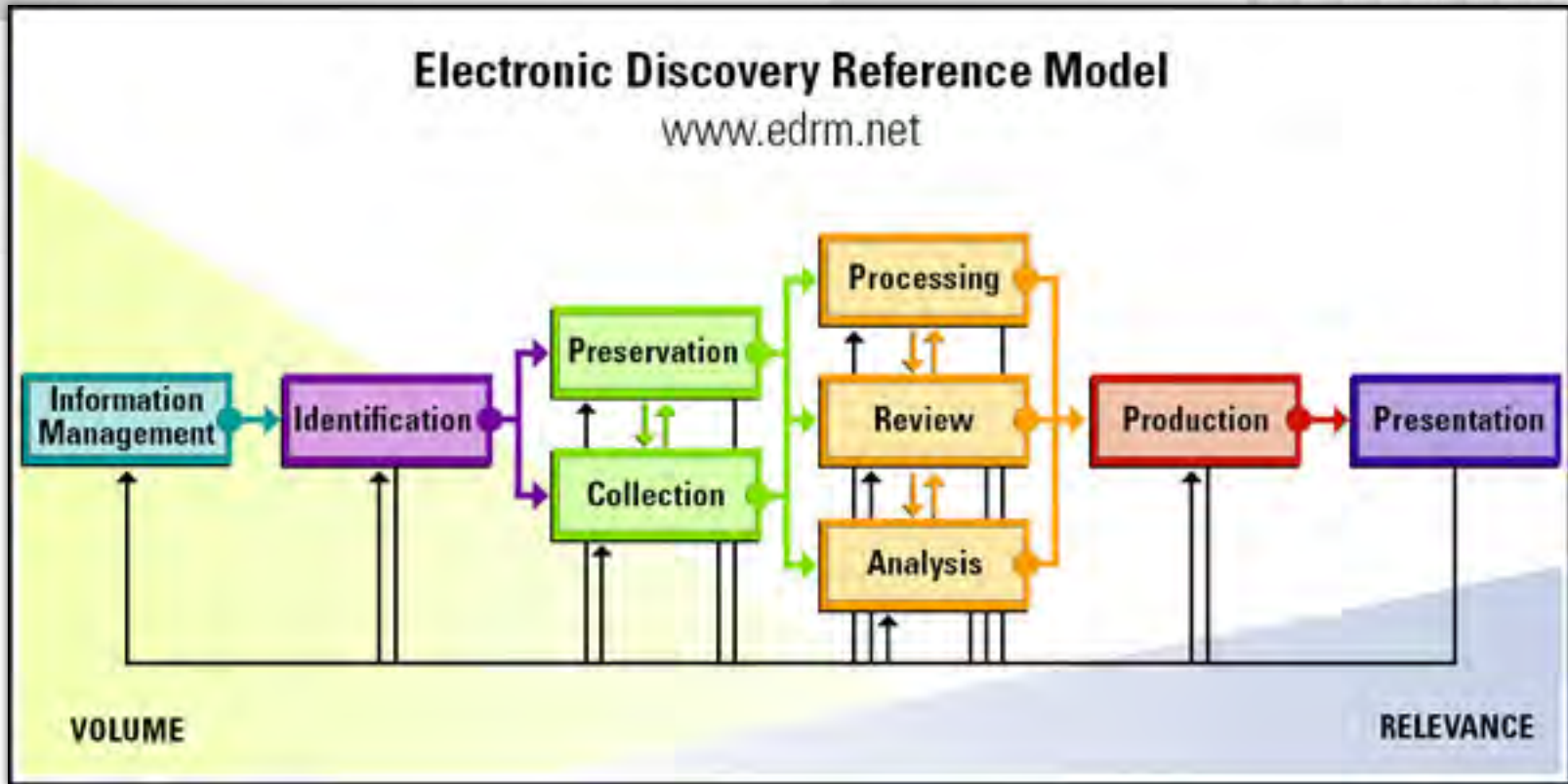
- An **optional framework to encourage** electronic exchange of paper and electronic documents for discovery and trial

### ■ **Costs**

- Emphasis to [Supreme Court \(General Civil Procedure\) Rules 2005](#) (Vic)
  - *“The power and discretion of the Court as to costs under [section 24 of the Act](#) shall be exercised subject to and in accordance with this Order”* (O 63 r 02)
- Cost orders for an electronic trial
  - *Kennedy Taylor (Vic) Pty Ltd v Grocon Pty Ltd* [\[2002\] VSC 32](#)
- Rejection of claim to provide a copy of discoverable documents on CD for Counsel
  - *Ipex ITG Pty Ltd v Melbourne Water Corporation (No 4)* [\[2008\] VSC 497](#)
- Refer to VSCL 2008 Conference Paper by Liz Harris and Annette Hughes, *'Taxation of Costs for e-matters'*

# Electronic Discovery

## EDRM Workflow



© 2005-2007 Socha Consulting LLC and Gelbmann & Associates. All Rights Reserved.

See also: [EDRM Evergreen Project \(2008-2009\)](#)

# Electronic Discovery

---

## First Steps

- Unfortunately, the discovery process is not yet as easy, fast, or cost effective as it should or could be!
- Increasingly, if your client **does not** have their “**electronic house**” in order, the potential to appropriately manage litigation is **significantly reduced**
- Any efficiency (and conversely, delay) to be derived from fulfilling your client’s (and your) **discovery obligations** is largely dependent upon your client’s **information management practices**, both paper and electronic

# Electronic Discovery

---

## Information Management

- **Proactive** (as opposed to reactive) **information management practices** can be seen as a measure of good corporate governance and risk mitigation, particularly for the 'litigation prone'
- Ideally, requires
  - Concise and Relevant **Document Retention Policy (DRP)**
  - Employee **Training**
  - Appropriate **Technology Infrastructure** (Implementation or Upgrade)
  - Regular **Reviews**
  - **Litigation Checklist**
- **Over 80+ pieces of legislation currently impose retention (and destruction) obligations on corporate Australia**

# Electronic Discovery

---

## Information Management – Document Retention and Destruction

- **Retention** obligations may rise from **contract** or **legislation**
  - **Corporate records** (7 years)
    - *Corporations Act 2001* (Cth) ss 286, 1306
    - *Financial Transactions Report Act* (Cth) s 23
  - **Tax records** (5 years)
    - *Income Tax Assessment Act 1936* (Cth) s 262A, [Tax Ruling TR 2005/9](#)
  - **Government commerce**
    - *Electronic Transactions Act 1999* (Cth) and State-level equivalents
  - **Personal information**
    - *Privacy Act 1988* (Cth), including 2001 private sector amendments
- **Destruction**
  - Current Australian common law test
    - *McCabe* [\[2002\] VSC 73](#); [\[2002\] VSCA 197](#)
  - Victorian legislative response
    - *Crimes (Document Destruction) Act 2006* (Vic)
    - *Evidence (Document Unavailability) Act 2006* (Vic)\*

# Electronic Discovery

---

*BT v State of New South Wales & Anor* [1998] FCA 363

- Your client must diligently manage their electronic documents – or else!
- Failure to adequately disclose your client's information management practices in a timely manner may lead to more onerous discovery obligations

# Electronic Discovery

---

## C7 'Mega-Litigation'

### ■ Evidence of News Limited General Counsel

- Outlined personal 'print or delete' retention policy
- Backups of deleted e-mails were retained for three (3) days only
- Only produced 50 relevant internal e-mails for the five (5) year period
- Admitted to destroying relevant handwritten faxes

# Electronic Discovery

---

## C7 'Mega-Litigation'

### ■ In Court

- News Limited (Hutley SC): *“What policy should a commercial organisation in the early 21<sup>st</sup> century, with the ubiquity of e-mails, adopt?”*
- Sackville J: *“Keep them, or don’t engage in a systematic process of removal of them so that in a case like this the end result is that ... as far as the trier of fact is concerned, I simply don’t know what the contemporaneous communications were within News [Limited]”*

### ■ Judgment

- *“[General Counsel’s] actions show that he was perfectly prepared to destroy documents he considered to be detrimental to his interests or to those of News”*
- *“Deliberately dishonest conduct”*
- Sackville J ordered a copy of the judgment to be given to the [Law Society of NSW](#)
  - *Legal Profession Regulation 2005 (NSW)* [Reg 177](#)
  - No public findings released by [Office of Legal Services Commissioner](#) as at January 2009

# Electronic Discovery

---

## Identification – Federal Court Guidance

**Order 15, rule 2(5) provides the matter-specific variables a party may consider in 'making a reasonable search':**

- (a) the nature and complexity of the proceedings; and*
- (b) the number of documents involved; and*
- (c) the ease and cost of retrieving a document; and*
- (d) the significance of any document likely to be found; and*
- (e) any other relevant matter.*

## **Order 15, rule 2(6)**

***If the party does not search for a category or class of document, the party must include in the list of documents a statement of the category or class of document not searched for and the reason why.***

# Electronic Discovery

---

## *Galati v Potato Marketing Corporation* [2007] FCA 919

- The CEO of the Potato Marketing Corporation advised that the party had **not undertaken a search** due to the burden arguably imposed by searching approximately 100,000 documents
- The CEO advised that he believed a search for those documents would be "*very onerous, time consuming and expensive*"
- Due to the apparent admission that no reasonable search had been performed, and that the categories of documents likely to be discovered were of significance, **the Court ordered further discovery by the Potato Marketing Corporation**
- A "**reasonable search**" varies upon circumstances and an organisation is best positioned to proactively seek external expertise if they consider discovery to be burdensome

# Electronic Discovery

---

## *Slick v Westpac (No 2)* [2006] FCA 1712

- Parties gave discovery
- During the relevant time, Quadrant only discovered a very small number of e-mails and no electronic calendar entries
- Quadrant had upgraded their technology infrastructure, including e-mail server, during the relevant time
- Unfortunately, Quadrant's CFO, as representative, was **unable to explain their searches and clarify the impact of the migration on their electronic documents**, specifically whether any documents could have been potentially deleted or no longer reasonably accessible as part of the process

# Electronic Discovery

---

## *Leighton Contractors v Public Transport Authority* [2007] WASC 65

- Reaffirmed the *NT Power* principle that the burden of discovery must be **proportionate** to the potential value of the electronic documents sought
- Time, cost and inconvenience are to be considered **in the context** of the litigation and financial resources available to the party
- The burden and obligation of discovery is **greater for a large organisation** due to the volume of electronic documents they manage
- Whilst discovery for a large corporation **may be onerous**, proportionality should ensure that it is **not oppressive**

# Electronic Discovery

---

## Identification - Types

- Consult with the client's technology personnel, in-house legal and/or an external advisor (**as translator**) to assist in identifying sources of 'potentially relevant' ESI
- Includes, but is not limited to:
  - E-mails
  - Documents
  - Spreadsheets
  - Databases
  - Presentations
  - Images
  - Logs (e.g. Activity, Transaction, Instant Messaging)
  - Audio (e.g. Voicemail)
  - Video

# Electronic Discovery

---

## Identification - Sources

---

### Common ESI Sources

#### Personal Computers

- Desktop
- Notebook

#### Computer Servers

- File Servers
- E-mail Servers
- Fax Servers
- Remote Access Servers

#### Archival Storage

- Network Attached Storage (NAS)

#### Backup Storage

- Tape Backups

### Potential ESI Sources

#### Communication Devices

- Mobile Phones and BlackBerry
- Personal Digital Assistants (PDAs)

#### Consumer Devices

- iPod/MP3 Players
- Digital Cameras
- Digital Voice Recorders

#### Portable and Removal Storage

- Optical Media (CD/DVD)
- USB Storage

#### Internet-Based Repositories

- Hosted Applications ([Salesforce CRM](#))
  - Hosted Storage ([MobileMe](#))
  - Social Networking ([Facebook](#), [MySpace](#))
-

# Electronic Discovery

---

## Identification - Locations

- **Location is both electronic and physical (geographical)**
- Understand **common environmental synchronisations** of ESI sources (i.e. multiple locations where the same ESI exists) in anticipation of having to advise upon and/or prioritise locations for preservation and collection
- **Examples**
  - Microsoft Outlook (Client) and Microsoft Exchange (Server)
  - Apple iPhone (Mobile Phone) and
    - Microsoft Exchange (Server)
    - MobileMe (Internet-Based Repository, Cloud Computing)

# Electronic Discovery

---

## Preservation and Collection

- Determine the most efficient method of preserving and collecting the 'potentially relevant' ESI sources
- Understand the options available and their strategic merits
- **Copy Type**
  - Physical Forensic Imaging
  - Logical Forensic Imaging
  - File Copy
- **Copy Method**
  - Dead (Traditional)
  - Live (Emerging)

# Electronic Discovery

---

## Processing

- Processing documents to a **readable and usable** form for analysis and review
- May be undertaken in-house using e-discovery processing software or by an external service provider
- Scan **paper documents** to electronic image format (e.g. TIFF, PDF)
  - Manual extraction of document metadata (e.g. Title, Author, Date)
  - Optical Character Recognition (**OCR**) enables searchable text
- Process **ESI**
  - Automated extraction of document and e-mail metadata
  - Extract compressed data (e.g. documents stored within ZIP archives)
  - Extract password-protected or encrypted data

# Electronic Discovery

---

## Analysis

- Analyse processed documents and take steps to filter prior to detailed legal review
- May be undertaken in-house using e-discovery processing software or in collaboration with an external service provider
- Also consider:
  - "Sampling" to validate filtering methods
  - Agreement on filtering methods with other parties
  - Filtering methods for non-text content (e.g. voicemail)

# Electronic Discovery

---

## Analysis – Filtering Methods

- **Search Queries**
  - Keywords
  - Concept Searching
- **De-Duplication**
  - Exact De-duplication
  - Near De-duplication
- **Key Custodians or Repositories**
- **File Types**
- **Date Ranges**

# Electronic Discovery

---

## Review

- Legal review of a filtered set of documents
- Documents may be ‘hosted’ in-house using an e-discovery **document review platform** or via an external service provider
- Select an document review platform which supports simplified document search, review and classification for lawyers
  - Cost
  - Scalability
  - Relevant Features
  - What are the other parties using?
- At this time, you may also **redact** (i.e. mask) part-privileged and/or part-confidential documents

# Electronic Discovery

---

## *GT Corp v Amare Safety* [2007] VSC 123

- Inadvertent disclosure of privileged electronic documents
- Privilege not waived under circumstances
- Exchanged electronically and inspected by opposing Counsel
- Opposing Counsel restrained from taking any further part in proceedings
- *“I have no doubt that the manner in which [the applicant’s] electronic discovery was provided, together with the complete lack of any index, has contributed significantly to the problems which have subsequently arisen”* (per Hollingworth J)

# Electronic Discovery

---

## Production

- **Produce a set of discoverable documents based on legal review which will require**
  - Assigning Document ID to (each page) of a document
  - Undertake final validation and quality assurance
  - Provide affidavit and document list in appropriate form
  - Produce documents in accordance with Document Management Protocol (**DMP**)
- Technical elements of production (i.e. electronic document stamping and 'load file' creation) may be undertaken in-house using e-discovery processing software or by an external service provider

# Electronic Discovery

---

## *Jarra Creek Central Packing Shed v Amcor* [\[2006\] FCA 1802](#)

- Unfortunately for Jarra Creek, their application to use a new DMP was dismissed in the interests of avoiding “*unnecessary discovery*”
- Reiterates the need to proactively agree upon a DMP, with all other parties, at the earliest opportunity
- Ensure that you **fully understand the DMP, and its implications**
- Be prepared to offer to pay the costs to other parties if you require anything above or beyond the agreed DMP to ensure that your lawyers can efficiently review discoverable documents

# Electronic Discovery

---

## *Westraint Resources v BHP Iron Ore (No 4) [2009] WASC 17*

- Highlights the critical relationship between the business process of information management, and the legal process of discovery
- Westraint requested order for further discovery of particular documents
- BHPIO successfully persuaded the Court **against such an order**
  - Filed multiple affidavits outlining extensive searches made for discoverable documents
  - Made extensive documented enquiries to current and former personnel, within multiple departments and jurisdictions
  - BHPIO's Records Manager and external legal counsel collaborated to undertake additional searches

# Electronic Discovery

---

## Presentation

- If the matter proceeds to trial, consider the use of an electronic courtbook to efficiently manage and display documents within the Court
- **Supreme Court of Victoria**
  - "eMaster"
- **Federal Court of Australia**
  - PN 17, [Pre-Trial Checklist](#)
  - "e-Registrars"

# Electronic Discovery

---

## Further Resources

- External Service Providers
- Internal Litigation Support Department
- “*In Pursuit of Relevance*” Blog (<http://www.elitigation.com.au>)

# Closing Remarks

---

- Discovery is the most time and cost intensive pre-trial exercise
- Practitioners are spending more of their time dealing with electronic documents
- Practitioners are increasingly required to satisfy their obligations relating to e-discovery
- Technology **should** assist and provide efficiency – not hinder!
- Consult specialist advisors to assist where required
- **Be informed - Use practice and procedure to your advantage!**

# Thank You

---

If you have any questions or feedback regarding this presentation please contact:

**Seamus E. Byrne**

+61 (0)416 214 388

[seamus@seamusbyrne.com](mailto:seamus@seamusbyrne.com)

<http://www.seamusbyrne.com>