



Discovery of Electronic Evidence

Seamus E. Byrne ([eDiscovery Tools](#)) and Geoffrey Lambert ([KordaMentha](#))

Please Read - Disclaimer

This presentation is made available by [Seamus E. Byrne](#) and Geoffrey Lambert, Australian legal practitioners, 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 July 2008.

For the [Law Institute of Victoria](#) (LIV) CPD - 14 August 2008 – Australian English (Duration: 55 minutes, Public Draft)

Today

- **Introduction**
 - Your Presentation
 - Your Presenters
- **Electronic Evidence**
 - Electronically Stored Information (ESI)
 - Technical Introduction (Metadata, Storage and Deletion)
 - Legal Considerations
- **Computer Forensics**
 - Definition
 - 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

The background of the slide features a grayscale image of classical architectural columns. The columns are fluted and have ornate capitals, with a strong sense of perspective as they recede into the distance.

- **Coverage**

- Victoria and Australia
- Civil Litigation
- Guiding Principles and Best Practice

- **Primary Audience**

- Victorian Litigators

Your Presenters

■ **Seamus E. Byrne**

- Chief Operating Officer, [eDiscovery Tools](#)
- Lawyer and Computer Forensic Expert (CISSP, CCE, EnCE)
- eDiscovery Advisor to a number of [S&P/ASX 200](#) companies
- Co-Drafted revised Federal Court of Australia Practice Note 17

■ **Geoffrey Lambert**

- Director, [KordaMentha](#)
- Lawyer, Computer Forensic Expert and eDiscovery Advisor
- Editorial Board and International Legal Panel, [Digital Investigation](#) (Elsevier)
- Regulatory electronic evidence management specialist (ACCC, ASIC, ATO)

Electronic Evidence

Historical Perspective

- Almost all of civilisation has relied upon **physical information storage**
- **Document** (*documentum* = proof)
 - Basic unit of information storage
 - **Late 19th Century**
 - Second industrial revolution
 - Typewriters, carbon paper and filing cabinets
 - **Today**
 - 98% of corporate communications and documents exist electronically
 - More than 30% of corporate communications are never printed! ([Jessen, 2000](#))

Electronic Evidence

Electronically Stored Information (ESI)

- **Dynamic**
 - The concept of a ‘temporary record’
- **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\$200!
- **Distributed Storage**
 - If I send you an e-mail, in how many geographic and electronic locations will the e-mail be stored and synchronised to?
- **Deletion without Human Intervention**
 - Routine system administration processes (e.g. Disk Cleanup) can delete or overwrite ESI without human intervention

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 – Storage and Deletion

- A **file system** is used to store, organise and retrieve data (i.e. ESI) on **storage media** (e.g. a 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, a ‘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

- The term ‘document’ is interpreted very broadly
- ***Acts Interpretation Act 1901*** (Cth) [s 25](#)
- ***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**
- ***Federal Court Rules*** ([O 1, r 4](#))
 - Commonwealth Evidence Act definition, and **expressly includes:**
 - ***“any other material data or information stored or recorded by ...electronic means”***

Electronic Evidence

Legal Interpretation – Victoria, Relevant Case Law

■ Victoria

- *Evidence Act 1958* (Vic) [s 3](#)
- *Interpretation of Legislation Act 1984* (Vic) [s 38](#)

■ Relevant Case Law – ESI as Documents

- The **medium itself** may also be considered a document
 - *Sony Music Entertainment (Australia) Ltd v University of Tasmania* [\[2003\] FCA 532](#), 48
- Includes '**metadata**'
 - *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [\[2006\] FCA 1802](#), 16

Electronic Evidence

Legal Considerations

- **Relevance**
 - Regardless of the form (i.e. physical, paper or electronic), 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 corporate IT or even legal 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](#)
- **Privilege Management**
 - **REMEMBER** privilege attaches to confidential communications as information, and not documents as such
- **Best Practice**
 - *Guidelines for the management of IT Evidence* ([HB171-2003](#)), Standards Australia

Computer Forensics

Introduction



- *“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 artefacts 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**: *Australian Administration Services v Korchinski* [\[2007\] FCA 12](#)
- **Appropriate Computer Usage**
 - 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
 - Federal Court of Australia **Practice Note 24** (5 May 2006)
 - Supreme Court of Victoria **Practice Note 2 of 2006** (1 September 2006)
 - Notable for introduction of the Independent Computer Expert (**ICE**) and increased range of obligations on all parties involved in a Search Order
- **Further Information**
 - '*Search Orders - Okay Computer?*', Australian Corporate Lawyer, March 2008

Search Orders

Recent Case Law

- ***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 Australia 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

- **Unfortunately, beyond the time constraints of this presentation**
 - **Search Warrants**
 - *Crimes Act* (Cth) [s 3E](#) warrants:
 - Three (3) conditions, seizure and removal (72 hour rule)
 - *Oke v Commissioner of AFP* [\[2007\] FCA 27](#); [\[2007\] FCAFC 94](#)
 - Highlighted practical issues
 - Liaison with AFP in relation to procedures
 - **Other Coercive Information Gathering Powers** (e.g. [s 263 ITAA](#), [s 155 TPA](#))
 - *JMA Accounting v Commissioner of Taxation* [\[2004\] FCAFC 274](#)
 - *Prescience Comms Ltd v Commissioner of Taxation* [\[2006\] FCA 1561](#)
 - The difference between ‘seizure’ as opposed to mere ‘copy’
 - **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*](#) (7th ed, 2007) p. 271)

■ Traditional Electronic Discovery

- Converting paper documents into electronic form for production

■ Modern Electronic Discovery

- Managing electronic documents in their native, electronic form for production

■ Today = Transitional Phase

Electronic Discovery

Practice Guidelines (Notes and Directions)

Jurisdiction	Practice Guideline
Supreme Court of New South Wales General Equity Division (Select Lists)	<u>PNSC Gen 7 (2008)</u> <u>PN Eq 3 (2007)</u>
Supreme Court of Victoria	<u>PN 1 (2007)</u>
Supreme Court of South Australia	<u>PD 2.1 (2006)</u>
Supreme Court of Queensland	<u>PD 8 (2004)</u>
Supreme Court of the Northern Territory	<u>PD 2 (2002)</u>
Federal Court of Australia	<u>PN 17 (2000)*</u>

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

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
- Has been widely ignored by litigators

▪ **Costs**

- Emphasis to *Supreme Court (General Civil Procedure) Rules 2005* (Vic), O 63:
 - “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” (s 63.02)
- Cost orders for an electronic trial:
 - *Kennedy Taylor (Vic) Pty Ltd v Grocon Pty Ltd* [2002] VSC 32

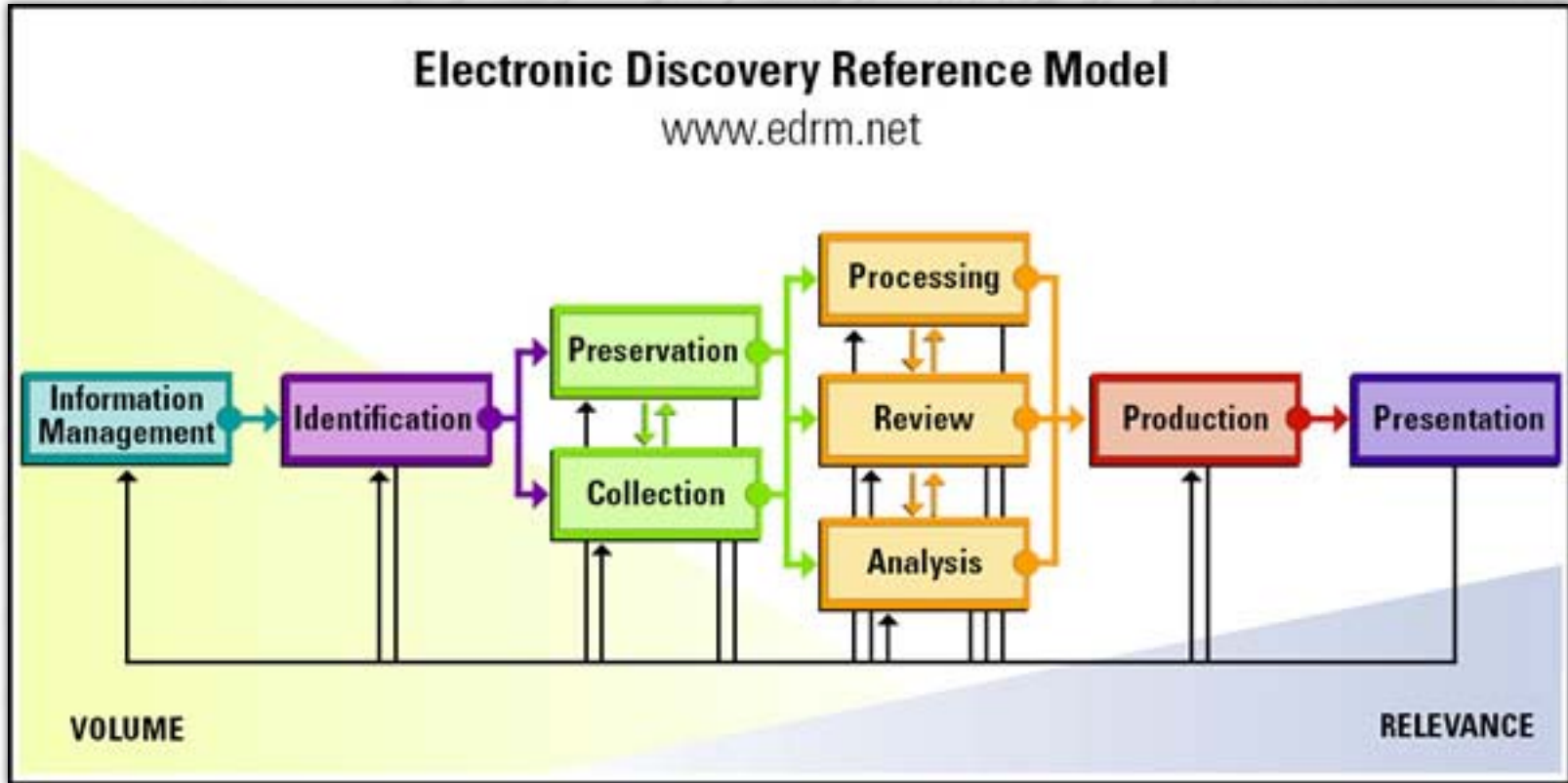
- Costs in respect of electronic discovery are currently under consideration

▪ **Further Information**

- Harris and Hughes, VSCL 2008 Conference Paper, *Taxation of Costs*

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!
- Any efficiency (and conversely, delay) to be derived from fulfilling you and your client's **discovery obligations** is largely dependent upon your client's information management practices, both paper and electronic
- Increasingly, if your client does not have their '**electronic house**' in order, a myriad of negative effects can follow

Electronic Discovery

Information Management

- **Proactive** (as opposed to reactive) **information management strategy** can be seen as a measure of good corporate governance and risk mitigation, particularly for the 'litigation prone'
- Ideally, require
 - Concise **Document Retention Policy**
 - Employee **Training**
 - **Technology Implementation** (e.g. [Enterprise Content Management System](#))
 - Regular **Review**
 - Defined eDiscovery **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](#), [1307](#)
 - *Financial Transactions Report Act* (Cth) [s 23](#)
 - *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) [Part 10](#)
 - **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 Australia common law test
 - *McCabe v BATAS* [\[2002\] VSC 73](#); [\[2002\] VSCA 197](#)
 - Victorian legislative response
 - *Crimes (Document Destruction) Act 2006* (Vic) → *Crimes Act 1958* (Vic) [ss 253-255](#)
 - *Evidence (Document Unavailability) Act 2006* (Vic) → *Evidence Act 1958* (Vic) [ss 89A-E](#)

Electronic Discovery

Information Management – 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

■ Media Report

- Sydney Morning Herald (27 September 2006)

Electronic Discovery

Information Management – C7 ‘Mega-Litigation’

▪ In Court

- News Limited (Hutley SC): *“What policy should a commercial organisation in the early 21st 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 (now retired) 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 July 2008

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**.*

- See also: **Practice Note 14** (3 December 1999)

Electronic Discovery

Identification - Types

- Consult the client's technology personnel, in-house legal and/or an external advisor (**as translator**) to assist in identifying **types** and **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

- Software as a Service (e.g. [Salesforce](#))

Electronic Discovery

Identification - Locations

- **Location** is both
 - Electronic; and
 - Physical (Geographical)
- **Synchronisation**
 - Understand common environmental synchronisations of ESI sources (i.e. multiple locations where the same ESI subsists in anticipation of having to advise upon accessibility and/or prioritise for collection)
- **Examples**
 - Microsoft Outlook (**Desktop**) 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 range of options and strategies available and the relative benefits of the same
- **Copy Type**
 - Physical Forensic Imaging
 - Logical Forensic Imaging
 - File Copy
- **Copy Method**
 - Dead (Traditional)
 - Live (Emerging)
- **Further Information**
 - VSC 2008 Conference, *Identification and Collection Methodologies for ESI*

Electronic Discovery

Processing

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

Electronic Discovery

Analysis

- Analyse processed documents and take steps to filter (i.e. cull) prior to detailed legal review
- May be undertaken in-house using eDiscovery analysis software or in collaboration with an external service provider
- **Filtering Methods**
 - **Search Queries**
 - Keywords
 - Phrases
 - Concept Searching
 - **De-Duplication**
 - Exact De-duplication
 - Near De-duplication
 - **Key Custodians or Repositories**
 - **File Types**
 - **Date Ranges**

Electronic Discovery

Review

- Legal team reviews the filtered document set
- Documents may be ‘**hosted**’ in-house using an **eDiscovery review platform** or via an external service provider
- Select an **online (i.e. web-based)** eDiscovery review platform which features simplified **document search, review and classification** for lawyers
- At this time, you will also need to consider **redaction** (i.e. masking) part-privileged and/or part-confidential documents

Electronic Discovery

Production

- **Produce a set of discoverable documents based on legal review**
- Typically, in accordance with Document Management Protocol
 - Assign Document Identifier (**Document ID**) to each document
 - Stamp the Document ID to (each page) of a document
 - Create **Load File**
 - Undertake validation and quality assurance
 - Draft **Affidavit** and **Document List** in appropriate form
- Technical elements of production (i.e. electronic document stamping and load file creation) may be undertaken in-house using eDiscovery processing software or by an external service provider

Electronic Discovery

Production - *GT Corporation v Amare Safety* [2007] VSC 123

- Inadvertent disclosure of privileged information, as electronic documents
- **Privilege not waived** under circumstances
- Documented 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 HollingworthJ)

Electronic Discovery



Presentation

- If the matter proceeds to trial, consider the use of an eCourtbook to efficiently manage and display documents within the Court

Closing Remarks

- Litigators are spending more of their time dealing with electronically stored information (**ESI**)
- Litigators will increasingly be required to address their obligations relating to ESI
- Technology **should** assist and provide efficiency – not hinder!
- **Be informed** and consult specialist advisory to assist in appropriately managing ESI

Thank You

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

Geoffrey Lambert

+61 (0)433 290 438

glambert@kordamentha.com

Seamus E. Byrne

+44 (0)207 193 8588

sbyrne@ediscovetrytools.com

seamus@seamusbyrne.com