


**Computer Forensics and  
Electronic Disclosure**

Seamus E. Byrne  
Director, Forensic Technology  
Vincents Chartered Accountants

13 June 2007

Bar Association of Queensland – 1 CPD



1

---

---

---

---

---


---

---

---

**Overview  
Computer Forensics**

- **Defining Computer Forensics**
- **Technical**
  - Data Storage and Deletion
  - Metadata
  - Acquisition
- **Legal Issues**
  - Rules of Evidence
  - Best Practice
  - Anton Pillar (Search Orders)
  - Dealing with Regulators
  - Privilege
- **Recent Case Law**
  - Electronic Document Authenticity
  - E-mail Analysis
  - Data Recovery
  - Reconstruction of 'Electronic Events'



2

---

---

---

---

---


---

---

---

**Overview  
Electronic Disclosure**

- **The Document Revolution**
  - Information
  - Document
  - Electronically Stored Information (ESI)
- **Your Client and Information Management**
  - Litigation Readiness
- **Defining Electronic Disclosure**
- **Practice Guidelines and Document Protocols**
  - Queensland: PD 8/2004
  - Shortcomings?
  - Costs and Recovery
  - The Future
- **Stages of Electronic Disclosure**



3

---

---

---

---

---

---

---

---

### Vincents Forensic Technology Defining Computer Forensics



*“the process of identifying, preserving, analysing and presenting **electronic evidence** in a manner that is legally acceptable in any judicial or administrative hearing”*

Adapted from Australian Institute of Criminology, 1999



4

---

---

---

---

---

---

---

---

### Vincents Forensic Technology Defining Computer Forensics

- Not limited to ‘mere computers’:
  - Computer networks and the Internet
  - Communication devices
    - Mobile Phones
    - Personal Digital Assistants (PDA)
    - Satellite Navigation Systems
    - Modern Photocopiers with internal hard drives
  - Consumer electronics
    - iPod/MP3 Players
    - Digital Cameras
    - Digital Voice Recorders
  - Video recording devices
    - Closed Circuit Television (CCTV)



5

---

---

---

---

---

---

---

---

### Vincents Forensic Technology Understanding Data

*“data is inherently copyable,  
just as water is inherently wet”*

Adapted from Bruce Schneier



6

---

---

---

---

---

---

---

---

### Understanding Data Storage

- A **file system** is a method of storing and retrieving data on a computer system
- File systems generally reference data using an **index table**
- The **index table** acts as a central directory which lists where all active data (i.e. not deleted) is located



7

---

---

---

---

---

---

---

---

### Understanding Data Storage

1	2	3									
	File 1										
							File 3				
			File 2								

- Three (3) active files are presented



8

---

---

---

---

---

---

---

---

### Understanding Data Deletion

- Generally, **when data is deleted**, only the directory listing in the index table is deleted - not the actual data
- Dependent on a number of variables, **deleted data may be recovered** – providing the file system has not re-allocated the storage location of the deleted data to newer data
- In contrast, **overwriting** or **secure deletion** utilities aim to completely overwrite the directory listing and actual data – making data recovery a difficult, if not impossible, process



9

---

---

---

---

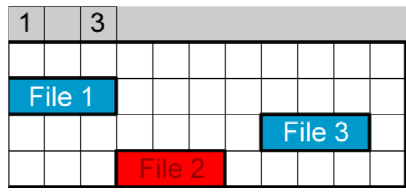
---

---

---

---

### Understanding Data Deletion



- File 2 has been deleted, yet still appears recoverable




---

---

---

---

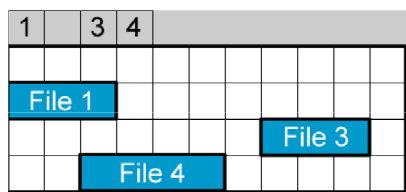
---

---

---

---

### Understanding Data Deletion



- File 2 now appears overwritten by File 4




---

---

---

---

---

---

---

---

### Understanding Data Metadata

#### Word Document

- Formatting
- Text
- **Metadata**
  - Title/Subject
  - Author
  - Creation Date
  - Last Modified Date
  - Last Saved Date
  - Last Saved By
  - Last Printed Date
  - Revisions and 'Track Changes'

#### E-mail Message

- Formatting
- Text
- **Metadata**
  - Sender
  - Recipients
  - Subject
  - Sent Date/Time
  - Attachment Information




---

---

---

---

---

---

---

---

## Understanding Data Acquisition – Today

### Forensic Imaging

- An **exact** copy (bitstream) of all **data** from the **physically imaged** media
  - Relevant and Non-Relevant
  - **Privileged and Confidential**
  - Active and Deleted
  - Residue and Unused
- Generally requires as much data storage capacity as the physically imaged media
- Relatively slow but provides flexibility for in-depth analysis
- **Creation of a 'forensic image' for an average hard drive generally takes 40 – 120 minutes.**

### File Copy

- A **logical** copy of one or more **specific active data files** (e.g. all Word documents within a folder)
- Unless data is copied using a proven copying method, data will be altered
- Relatively fast but only allows the data files specifically copied to be analysed

---

---

---

---

---

---

---

---

## Understanding Data Acquisition - Emerging

### Logical Forensic Imaging

- An **exact** copy of **specific data** (e.g. all Word documents on a Server computer returning search hits to 'wages')
- Uses a proven copying method to ensure data integrity
- Awaiting widespread adoption by forensic practitioners

### Live Computer Forensics

- Creating a forensic image when a **computer is on** (as opposed to pulling the plug/shutting down); OR
- Creating a forensic image **covertly over a computer network**
- Avoids liability issues associated with shutting down mission-critical computers (e.g. Servers)
- Allows capture of most encrypted electronic evidence

---

---

---

---

---

---

---

---

## Legal Issues Rules of Evidence

- **Relevance = Admissibility**
  - It is generally possible to perform a forensic preview (e.g. keyword search) to ascertain relevance: *Kennedy v Baker* [2004] FCA 562
- **Chain of Custody and Evidence Copies**
  - Managing electronic evidence in a documented manner without (or with minimal) alteration
- **Expert Opinion and Testimony**
  - Highly specialised discipline and **NOT** a skill possessed by 'everyday' or corporate IT personnel
  - **DO NOT** turn on computers without the assistance of an expert - may result in alteration or loss of data: *Egglisshaw v ACC* [2006] FCA 819
- **Best Practice**
  - *Guidelines for the Management of IT Evidence* (HB171-2003), Standards Australia

---

---

---

---

---

---

---

---

Legal Issues

Anton Piller (Search Orders)

- Recently revised Federal Court and Queensland Supreme Court practice guidelines allow for an **independent computer expert** (ICE) to assist in forensic imaging, computer searching, etc.
- If **privilege** is claimed during execution, the ICE is limited to providing the computer to the independent solicitor until further determination is made.




---

---

---

---

---

---

---

---

Legal Issues

Dealing with Regulators

- ATO Access and Information Gathering Manual
  - ASIC and ACCC yet to release similar manual
- *JMA Accounting v Cmr of Taxation* [2004] ATC 4916
  - Argued ATO access (per s 263 IATA) was unreasonable
    - Must only seize documents as statutory power permits
    - Must carry out search and seizure reasonably
    - Must do no more than reasonably necessary to satisfy that permitted documents have been seized
  - Court ordered return of document categories (e.g. e-mails) that had been copied in bulk without **'some effort'** to test for **relevance**
- See also: *Prescience Comms v Cmr of ATO* [2006] FCA 1561




---

---

---

---

---

---

---

---

Legal Issues

Privilege

- Privilege attaches to confidential communications as information, and not documents as such
- Privileged information in ESI may be contained not only in active and readily accessible electronic files, but may also be present on a hard drive in a deleted form
- **Does the diligent practitioner claim privilege?**




---

---

---

---

---

---

---

---

### Recent Case Law

#### Electronic Document Authenticity

- **Creation date** of an electronic document:
  - *ASIC v Loiterton & Ors* [2004] NSWSC 172
    - *Corporations Act*: Contravention of Directors Duties, Misleading P&L, etc.
    - Electronic documents purporting to evidence an agreement to charge fees and a subsequent number of invoices **dated between July 1996 and April 1997** were forensically analysed with **creation dates** reflecting **March 1997**
- **Alteration** to an electronic document:
  - *Hudson Investment Group v Australian Hardboards Limited & Ors* [2005] NSWSC 716
    - Contractual dispute relating to validity of purported amendments to an Entitlement Deed
    - Allegation that certain company minutes were falsified just prior to being submitted to the auditors based on **'last modified date'** metadata entry.



19

---

---

---

---

---

---

---

---

### Recent Case Law

#### E-mail Analysis

- **Defamatory e-mails** and a 'rogue employee':
  - *Boniface v SMEC Holdings Limited & Ors* [2006] NSWCA 351
- **Corruption allegation** from a **public library**:
  - *Grant v Marshall* [2003] FCA 1161
- **Spam**:
  - *AMCA v Clarity1 Pty Ltd* [2006] FCA 410



20

---

---

---

---

---

---

---

---

### Recent Case Law

#### Data Recovery

- Recovery of **deleted instant messaging (IM) communications**:
  - *Sony Computer Entertainment Aust v Jakopcevic* [2001] FCA 1520
- Recovery of **archived e-mails**:
  - *Ingot Capital Investments & Ors v Macquarie Equity Capital Markets & Ors* [2005] NSWSC 1174
- Reconstruction of legacy e-mail system to **verify completeness of discovery**:
  - *Slick v Westpac Banking Corporation* [2006] FCA 1712



21

---

---

---

---

---


---

---

---

**Recent Case Law**  
**Reconstruction of 'Electronic Events'**

- **Employment dispute or termination:**
  - *Australian Administration Services v Korchinski* [2007] FCA 12
    - Downloaded confidential documents to a portable hard drive
    - Attempted to reformat and overwrite documents with large video files
  - *Austress Freyssinet v Joseph* [2006] NSWSC 77
    - Confidential documents sent to a personal e-mail address
  - *Portal Software v Bodsworth* [2005] NSWSC 1179
    - Identifying the usage of 'clean-up' and 'secure deletion' software utilities

 22

---

---

---

---

---

---

---


---

---

---

**Vincents Forensic Technology**  
**The Document Revolution**

- **Information**
  - Almost all of civilisation has relied on physical information storage
- **Document**
  - *Documentum* = proof
  - Basic unit of information storage
  - Late 19<sup>th</sup> century
    - Modern form of business document
    - Typewriters, carbon paper and filing cabinets
  - Certain assumptions
    - Original Records
    - Altered Records (Non-authentic)
  - Legal Interpretation
    - Paper, disc, tape, etc: *Acts Interpretation Act 1954* (Qld) s 36; *AIA 1901* (Cth) s 25.
    - Includes a Server: *TLC Consulting Services v White* [2003] QCA 131.

 23

---

---

---

---

---

---

---


---

---

---

**Vincents Forensic Technology**  
**The Document Revolution**

- **Electronically Stored Information (ESI)**
  - ESI is dynamic
  - ESI is ever-increasing in volume
  - ESI is in many distributed locations
  - Routine processes can delete or overwrite ESI without human intervention

 24

---

---

---

---

---

---

---

---

---

---

### Vincents Forensic Technology The Document Revolution

- **Perspective – United States**
  - December 2006: E-Discovery Amendments to the *Federal Rules of Civil Procedure*
  - Rule 34 – Production of Documents **AND ESI**  
*“including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in **any medium from which information can be obtained**”*



25

---

---

---

---

---

---

---

---

### Information Management Your Client - Litigation Readiness

- **What** information is held by your client?
  - General Business Records
  - Industry-Specific
- **Where** is the information located?
- **How** will you **identify** and **preserve** the ‘potentially relevant’ information for disclosure?
  - Hard Copy (Paper)
  - Electronically Stored Information (ESI)



26

---

---

---

---

---

---

---

---

### Information Management Your Client - Litigation Readiness

- **Document Retention and Destruction - Current Australian Test:**
  - *McCabe v British American Tobacco Australia Services Ltd* [2002] VSC 73; [2002] VSCA 197.
    - Documents destroyed before litigation commencement may attract adverse inference and criminal contempt sanctions.
- **Queensland:**
  - *R v Ensbej* [2004] QCA 335.
    - Guilty of shredding document under *Criminal Code Act 1899* (Qld) s 125.
- **Corporate Criminal Liability?**
  - ‘Corporate culture’ that encourages or tolerates destruction of relevant documents, including proceedings which **may be** commenced in future: *Crimes (Document Destruction) Act 2006* (Vic).



27

---

---

---

---

---

---

---

---

### Information Management Your Client - Litigation Readiness

- **Document Retention and Destruction - United States**
  - Rule 37(f): Established 'safe harbour' with no penalty for deleting electronically stored information (ESI) due to **routine operation** of computer systems if:
    - Established, documented and operational procedures
    - Reasonable preservation steps taken
    - In good faith



28

---

---

---

---

---

---

---

---

### Information Management Your Client – News Limited

- *Seven Network Limited v News Limited*
- Evidence of News Limited In-House Counsel:
  - Outlined 'print or delete' retention policy
  - Produced only 49 relevant internal e-mails for the five (5) year period (in hard copy)
  - Backups of deleted e-mails were retained for three (3) days only
  - Admitted to destroying relevant handwritten faxes



29

---

---

---

---

---

---

---

---

### Information Management Your Client – News Limited

- **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 forthcoming – Watch this space!**



30

---

---

---

---

---

---

---

---

### Information Management Your Client – Exxon Mobil

**Physical World**

- 200 countries
- 306 offices worldwide
- Data backups at 45 worldwide locations
- Thousands of pending and on-going litigations

**Electronic World**

- 5.2 million e-mails daily
- 65,000 desktop computers
- 30,000 notebook computers
- 20,000 BlackBerry/PDA's
- 100,000 USB flash drives
- 7,000 servers
- 121,000 backup tapes monthly

**Total electronic storage: 800TB (Terabytes) = 400 billion typewritten pages**  
Source: ExxonMobile (04-CV-002), Hearing on Proposed Amendments to FRCP, 2005.



31

---

---

---

---

---

---

---

---

---

---

### Information Management Your Client - Litigation Readiness

**• Proper Information Management**

– Four Steps

- Policy
- Training
- Implementation (Document/E-mail Management)
- Regular Review

– **Goal:** Legal and regulatory compliance

– **Additional Result:** Manage client disclosure with reduced cost, less stress and increased efficiency



32

---

---

---

---

---

---

---

---

---

---

### Electronic Disclosure Defining Electronic Disclosure

**• Traditional Electronic Disclosure**

– Converting hard-copy (paper) documents into an electronic format

**• Modern Electronic Disclosure**

– Dealing with electronic documents and e-mail in their original, electronic form

**• Today = Transitional Phase**



33

---

---

---

---

---

---

---

---

---

---

### Electronic Disclosure Court Practice Guidelines

Jurisdiction	Current Practice Direction/Note
Supreme Court of Victoria	1/2007
Supreme Court of South Australia	2.1/2006
Supreme Court of New South Wales	SC Gen 7/2006
<b>Supreme Court of Queensland</b>	<b>8/2004</b>
Supreme Court of the Northern Territory	2/2002
Federal Court of Australia	17/2000

The Supreme Courts of Western Australia, Tasmania and the ACT are yet to formally release similar practice guidelines (i.e. Use of technology to support litigation).



---

---

---

---

---

---

---

---

---

---

### Electronic Disclosure Queensland - PD 8/2004

- Parties agree upon written Document Protocol to manage and exchange documents
  - Electronically
  - Generally using a Database
- Document Protocol may include:
  - Court Documents and Witness Statements
  - **Disclosure**
  - **Exchange of Agreed Bundle and Electronic Trial**
- Default Document Protocol is based on UCPR Form 19 ('List of Documents')



---

---

---

---

---

---

---

---

---

---

### Electronic Disclosure PD 8/2004 – Shortcomings?

- When should you use technology to assist litigation?
  - At first instance, 500+ documents (Paper and/or Electronic)
- **Use of Technology and Document Protocols**
  - What information do you need?
  - When should you meet with the other party/parties?
  - Who can provide assistance to legal counsel in negotiations?
  - Have you agreed upon a 'matter-appropriate' Document Protocol?



---

---

---

---

---

---

---

---

---

---

## Electronic Disclosure PD 8/2004 – Shortcomings?

### • Technical Formats

- *Shannon & Anor v Park Equipment Pty Ltd* [2006] QSC 284
  - “Disclosure by production requires production of the original documents, electronically if the original was in electronic form”
- What format is appropriate?
  - Native Format
  - Image Format (TIFF, PDF)
- Some data files aren’t meant for complete printing
  - Spreadsheets
  - Databases
- What about proprietary data files?
- What about data files you can’t read?

---

---

---

---

---

---

---

---

## Electronic Disclosure Costs and Recovery

### • Queensland

- Default: **Each party pays costs**
- Limited Scale: *Uniform Civil Procedure Rules 1999*, Schedule 1.
- *Iron Gates Pty Ltd v Richmond River Shire Council* [2006] QSC 141.
  - Estimated electronic trial costs in security for costs application
  - Court ordered disclosure to be undertaken electronically

### • Australia

- Victorian Society for Computers and the Law Focus Group recently released updated scale items/tasks for Taxation of Costs

---

---

---

---

---

---

---

---

## Electronic Disclosure The Future

- Federal Court to **strongly recommend** ‘electronic’ from late 2007
- Likely harmonised by Supreme Court of Queensland in 2008
- Consequently, electronic exchange of discoverable documents must be made easy, efficient and accessible to all (beyond top-tier)

---

---

---

---

---

---

---

---

### Electronic Disclosure The Future

- Will include a 'Discovery Directions' conference
  - United States - Rule 26(f):
    - 'Meet and Confer' to negotiate and agree upon how discovery will be managed
  - Latest Supreme Court of Victoria PN
    - 'Consultative Committee' with representatives from all parties
  - May include a member of the 'Court E-Discovery Panel' to assist in the preliminary resolution of technical and procedural issues
  - **Document Management Protocol** is filed with the Court



40

---

---

---

---

---

---

---

---

### Electronic Disclosure Stages of Electronic Disclosure



41

---

---

---

---

---

---

---

---

### Electronic Disclosure Step One – Identify

- How do you identify 'potentially relevant' information in hundreds of lever arch files, backup tapes, and servers containing millions of e-mails?
- **Sources of ESI**
  - File Servers
  - E-mail Servers
  - Personal Computers (Desktop, Notebook, PDA)
  - Backups



42

---

---

---

---

---

---

---

---

### Electronic Disclosure Step One – Identify

- Engaging a **technical advisor to assist:**
  - Scoping the time, cost, volume and accessibility of ESI
  - Acting as **translator** between the clients internal IT team or outsourced technology provider
  - Understanding and resolving technical hurdles:
    - Dealing with **legacy/superseded computer systems:** *Davies & Anor v Chicago Boot Company* [2006] SASC 241 (Lunn J, 22/06/06).
    - The time and difficulty to restore and review **backup tapes:** *BT (Australasia) Pty Ltd v State of New South Wales & Anor* (No 9) [1998] 363 FCA (Sackville J, 09/04/1998).
    - The **best technology method** for disclosure: *Sony Music Entertainment (Australia) Limited v University of Tasmania* [2003] FCA 532.



43

---

---

---

---

---

---

---

---

---

---

### Electronic Disclosure Step Two – Acquire

- **Acquire** ‘potentially relevant’ ESI in a manner compliant with best practice
  - Forensic Imaging
  - File Copy
- **Scan** hard copy (paper) into electronic form
  - Using Optical Character Recognition (**OCR**) to ensure searchable text
  - Image format (TIFF, PDF)



44

---

---

---

---

---

---

---

---

---

---

### Electronic Disclosure Step Three - Restore

- **Restore** ‘potentially relevant’ ESI to readable and usable form
- This may include:
  - Deleted data
  - Encrypted or password-protected data
  - Compressed data (i.e. from tape backups)



45

---

---

---

---

---

---

---

---

---

---

## Electronic Disclosure

### Step Four - Filter

- **Filter** 'potentially relevant' ESI:
  - De-duplication
    - Removing duplicate files and e-mails
  - Key storage locations and/or key custodians
  - Keywords and search terms
    - *ASIC v Citigroup Global Markets Australia*
  - File types
    - Word documents, Excel spreadsheets
  - Date ranges



46

---

---

---

---

---

---

---

---

## Electronic Disclosure

### Step Five - Review

- **Review** by legal team:
  - Offline Review
    - via CD/DVD using ISYS Search
  - Online Review using a Litigation Support Database
    - FTI Ringtail Legal (formerly CaseBook)



47

---

---

---

---

---

---

---

---

## Electronic Disclosure

### Step Five - Review

- **Redaction** for privilege and confidentiality
- **Inadvertent Disclosure?**
  - *Burton and Eising v Wright Trading* [2007] QSC 017:
    - Privileged e-mails inadvertently sent to other side – not waived
  - *GT Corporation v Amare Safety* [2007] VSC 123:
    - Inadvertent disclosure of electronic documents – promptly requested return - not waived
    - Opposing lawyers who had inspected were prevented from acting
  - United States - Rule 26(b)(5):
    - Recognised inadvertent production is difficult to avoid
    - Allows party to notify the other party who are then legally obligated to return until privilege claim is resolved



48

---

---

---

---

---

---

---

---

Electronic Disclosure  
**Step Six - Produce**

- **Produce** and present filtered and reviewed ESI
  - Stamp and number each document
  - Perform final validation and quality control
  - Supply in desired format (or specific format if a Document Protocol exists)



49

---

---

---

---

---

---

---

---

Electronic Disclosure  
**Closing Remarks**

- Lawyers are spending more of their time dealing with electronically stored information (ESI), electronic documents and e-mail
- Technology **should** assist and provide efficiency – not hinder!
- Consult specialist technical advisory when dealing with ESI



50

---

---

---

---

---

---

---

---

Vincents Forensic Technology  
**Thank You**

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

Seamus E. Byrne  
 Director, Forensic Technology  
 Vincents Chartered Accountants  
 +61 7 3854 4555 / 0416 214 388 (24x7)  
[sbyrne@vincents.com.au](mailto:sbyrne@vincents.com.au)  
[www.seamusbyrne.com](http://www.seamusbyrne.com)



51

---

---

---

---

---

---

---

---