

ELECTRONIC EVIDENCE DISCOVERY



by Andrew Law

www.AndrewLaw.com
www.TechLaw.com.hk

General forms of Electronic Evidence



- Email
- Wordprocessor, Electronic Spreadsheet files
- Relational database (record) file
- Software source code
- Various image files (.tiff, .jpeg, .pcx)
- Web browser bookmarks / cookies / cache memory
- Calendar; to-do-list, contact list
- Voice mail



Why EED ?

- Clients : Growing trend and volume of information in electronic form
 - One man's trash is another's treasure
 - Competitors no longer read your mind, they read your email
 - cf the Anti-trust case against Microsoft
- Lawyers : Possible mal-practice claim for wrongful handling of electronic evidence
- Judges



Some Cases Where EED is Relevant

- Employment - establish "unreasonable / wrongful" termination
 - Kelley vs Airborne Freight Corp 953 P.2d 200 Colo. App. 1998
- IP - validate copyright infringement or improper use of licensed software
- Insider Dealing
 - Smith vs SEC, 129 F.3d 356 (6th Cir. Tenn. 1997)
- Stolen Clients / Trade Secret
 - prove theft by employee or others
 - People vs Eubanks and Wang CR6748 Ca. Supr. Ct.



Plaintiff's Objectives

- Negotiating tool to settle
 - Small size Plaintiff vs Big size Defendant : cost
 - What if there are information Defendant never knew existed, or prefer to be covered
- Access to information which had never been printed
- Access to internal comments which do not appear on paper
- Access to the earlier draft versions, instead of only the final printout
- Electronic evidence (audio / multimedia format) is more persuasive to court



Challenges in Handling Electronic Evidence

- Document request : specific and relevant
- Non-discoverable information on grounds of confidentiality or privilege
- Magnitude of information volume
- Lack of organization of defendant's electronic information
- Information in proprietary, compressed or encrypted format



Defendant's Strategies

- Company-wide education
- Privilege
- Confidentiality : software source code : restrictive use
- “reasonable” document retention policy : destruction of document



Digital Identity, Authentication & Certification

- personal / corporate Digital Identity Certificate
- Intel's Processor Serial Number
- Microsoft's Office Global Unique Identifier “GUID”
 - cf virus “Melissa” and its creator David L Smith



Types of Electronic Information

- Active files
- Archival files
- Residual files



Printout vs Electronic File

- When the file was created, by which PC (and who), modified, deleted
- Annotate the text, including audio comments, which do not appear on printout
- Back-dating is difficult

BUT :

- Stored in compact size – vulnerable than paper-based documents
- Alteration of electronic data may be easier to cover up given superior technical knowledge



Records Retention Policy

- Unreasonable / “bad faith” finding :
 - Length of retention period
 - Frequency and magnitude of claims involving the types of document at issue
 - Reasons why the policy was adopted



Objectives of EED (1)

- Preserve it
 - Warning letter to the target party, and to seek agreement on cooperation, failing which,
 - Apply for court order to preserve information, with testimony of forensic expert :
 - Require the target company to cease all activities which may alter or destroy the relevant active, archival or residual data until a complete MIRROR-IMAGE copy is made; and
 - Grant direct access to target company’s computer system to search for key information



Objectives of EED (2)

- Seize it – Anton Pillar order
 - Yousif v Salama [1980] 3 All E.R. 405
 - Nintendo of America Inc v Coinex Video Games Inc [1983] 2 F.C. 189
- Find it – locations !!
 - Windows Recycle Bin / swap file / registry, .tmp file directory, “My Documents”, PC hard drives, file servers, floppy disk matching, remote control programs, backup tapes, print spoolers, fax server
 - Suggested procedure to conduct on-premises discovery of computer records



Sample EED Software Tools

- NeoTrace : internet route trace tool
- FileCNVT : catalog the contents of hard disk drives
- DM : database analysis tool, works with Net Threat Analyzer
- ShowFL : for timeline analysis of computer usage
- FILTER : binary data filtering
- NTAView : internet usage analysis tool
- SPACES : encryption pattern review aid



Computer Forensic Technologist Services

- Identifying, locating, retrieving and reviewing potentially relevant data in both client and opposing party systems
- Identifying the most cost-effective means for responding to electronic discovery requirements
- Developing and implementing strategic electronic discovery plans and assisting with the development of production requests and deposition outlines
- Formulating accurate and proper responses and objections to requests for production and interrogatories



Specialized Processing of Data for Litigation Purposes

- Extracting relevant information from electronic mail, various desktop applications and other electronic sources in a proper, timely and cost-effective manner
- Reading and recovering data from obsolete tapes and disks for which hardware and software is no longer available
- Conducting high speed searches of electronic data sets including e-mail and extracting relevant information for litigation
- Reducing huge data sets to a manageable size using data differential analysis tools
- Recovering data that has been deleted, tampered with, damaged or hidden
- Accessing password-protected and encrypted data
- Verifying dates and other file attributes and tracing user activity
- Providing data in printed or electronic formats that meet counsel's needs



Sample Documents

- Standard Definition of EED terms
- Sample Interrogatories : electronically stored records
- Sample language for deposition of custodian of electronic records
- Request for production of electronic media



References

- Electronic Evidence by Alan M Gahtan
ISBN 0-459-27070-2
- Forensic Computing Services by Lee & Allen