Emerging Issues of Electronic Discovery in Civil Litigation

By Noppramart Prasitmonthon

Emerging Issues of Electronic Discovery in Civil Litigation

Noppramart Prasitmonthon*

Table of Contents

---

* LLB (Thammsat) Thailand, GradDip Business Law (Thammasat), Thai Barrister, LLM candidate at the University of Melbourne. An earlier draft of this article was submitted as a part of coursework undertaken for an LLM in the Faculty of Law, University of Melbourne.

A) Retention and Destruction of Electronic Records Policy
B) E-Mail Use Policy

6.2 Educating Employees Regarding the Use of IT and Legal Risks

6.3 Reviewing and Monitoring Policy Implementation

Conclusion

Introduction

"Ninety three per cent of all corporate communication is now created electronically, with only thirty per cent of that communication ever printed to paper. Clearly the vast majority of electronic data, seventy per cent, exist only electronically"[1]
(Nimsger et al., 2002)

The use of computers is ubiquitous in any areas of work today. Data, which have been produced and stored in paper form will gradually decrease and are increasingly in digital form. Some are printed out and some never exist in the physical form, but are stored as a binary file (i.e. zero and one) in a hard drive, diskette and server elsewhere. In the case of litigation, the revolution of the data form may raise various doubtful issues in terms of the discovery of evidence. At least the main players such as judges and litigants will be aware of the existence of electronic evidence. Litigants would have to think whether or not they should use or discover digital evidence, whereas judges would have to consider whether they should allow a search for electronic evidence. In addition, judges must decide how broad or narrow to allow an order for discovery they should permit the requesting party for this kind of evidence.

Many curious issues arise in the procedure of electronic discovery. This paper will define some issues for which there are as yet no clear answers in both the legal and

particle context with regard to electronic discovery in civil litigation. The paper also provides an analysis of the role of litigants as requesters and respondents, and the role of judges in the procedures of electronic discovery. American and Australian cases and their regulations involving digital discovery will be used to illustrate the issues. Australian cases, however, may be substantively less than the American cases used in this paper since there has not been much Australian legal literature written in the area of electronic discovery.

The first part of paper focuses on data preservation including the duties of data preservation and the methods of complying with court orders of preservation. In the second part, the allocation costs of electronic discovery will be discussed. The third part discusses the processes of digital discovery. A case study of Arthur Andersen is analyzed as the result of spoliation sanctions in the fourth part. Evidentiary issues such as authentication electronic evidence, the hearsay rule and the best evidence rule are studied in the fifth part. The final part will focus on the issue of electronic record risk management.

Background

Discovery processes are undertaken at a pre-trial stage where plaintiffs and defendants attempt to gather and to obtain relevant evidence, for example, information or documents in order to support their case in trial proceedings.[2] Parties must disclose categories of all documents and data compilations that are relevant to disputed facts alleged with particularity in the pleadings before discovery. These discovery processes may be undertaken in a few months of the commencement of the litigation.[3]

---

[1] Kristin M. Nimsger and Michele C.S. Lange, 'Examining the Data' (2002) *Security Products* p. 16 also, visited 29 May 2002 at <http://www.ontrack.com>

[2] Stephen Colbran et al., *Civil Procedure: Commentary and Materials,* Butterworths, Sydney, 1998 p. 471

[3] See The US Federal Rules of Civil Procedure section 26(a): Anthony J. Dreyer, 'When the Postman Beeps Twice: The Admissibility of Electronic Mail under the Business Records Exception of the Federal Rules of Evidence' (1996) 64 *Fordham Law Review* 2285.

Electronic discovery involving electronic documents, such as e-mail or software source code, poses many issues that do not arise as commonly as with traditional paper documents.[4]Electronic evidence is quickly becoming a central focus of litigation discovery in American courts, presenting enormous problems for lawyers. One commentator noted that "with changing discovery rules, rapid accumulation of electronic data, growing and uncontrolled use of electronic mail (e-mail), and increased use of sophisticated back up and archive systems, the problem is likely to intensify as the new millennium approaches."[5] The technological and practical aspects of electronic discovery distinguish it from traditional discovery.

I Data Preservation

1.1 Duties of Data Preservation

Generally, there are many statutory requirements for retaining "documents" or record keeping. One lawyer in Australia claimed that there were over 450 separate Acts of Parliament, which stipulated provisions with regard to the retention of records.[6] He also exemplified the following :

> "1) The *Annual Holidays Act 1944* (NSW) section 9 requires all employers to maintain annual leave records for at least 6 years. Failure to do so results in a fine of 10 per cent penalty units;
>
> 2) The *Customs and Excise Legislation Amendment Act 1989* (Cth), section 240 requires importers to retain all relevant commercial documents regarding proper description and value of duty for, among other things, goods ultimately

---

Also, see Australian Discovery and Inspection of document Rules in Supreme Court Rules(1996)(Vic) (O29) section 29.01-04 and case law regarding subpoena for production before trial: *Sharpe v Dalton(*1990) 14 Fam LR 339 at 342.

[4] Steve White, 'Comment: Discovery of Electronic Documents' *Digital Technology Law Journal* Volume 2 No. 1 visited on June 15, 2002 at <http://wwwlaw.murdoch.edu.au/dtlj/2000/vol2_1/white.pdf>

[5] Kimberly D. Richard, 'Electronic Evidence: to Produce or Not to Produce, That Is the Question' 21 *Whittier Law Review* 464.

for consumption in Australia. These records must be retained for 5 years after entry of the goods and failure to do so results in a penalty of $2,000; and

3) The *Lay-by Sales Act 1943* (NSW) section 4 requires Vendors who sell goods by lay-by to maintain a register of purchaser names and addresses along with other descriptive information relating to the date, sale No. and price. The records must be retained for at least one year and failure to do so results in a penalty of .5 of a penalty unit…"[7]

The above provisions are requirements for record keeping or data preservation in general situations. Common law[8] and statutory law[9] also impose a duty to preserve evidence in specific circumstances where service of a complaint may render parties on notice of a duty to preserve potentially relevant evidence.[10] In order for compliance with subpoenas and orders for discovery, parties serving such notices should be alert that all documents in their possession, custody or control may be relevant to issues in the proceedings.[11] The relevant documents will be gathered together and made available to both parties. Lawyers of parties will assist and provide certain advice to their clients in terms of whether or not such documents are relevant to the disputes.

In the U.S., some courts ruled that litigant might not have the duty to retain any documents in their possession unless there is a law requiring this. The litigant,

---

[6] Gillbert and Tobin, 'Legal Risk and Admissibility of Electronic Documents and Records' visited on December 06, 2002 at <http://www.gtlaw.com.au/t/publications/defult.jsp?pubid=149>

[7] *Ibid.*

[8] Australian Common law in the issue of preservation duty see Compagnie Financiere et *Commerciale du Pacifique v. Peruvian Guano Co* (1882) 11 QBD 55 and the U.S. case see *Bowmar Instruments Inc.,* 25 Fed. R. Serv. 2d (Callagnhan) 423, 427 (N.D. Ind. 1977)

[9] See Supreme Court (General Rules of Procedure in Civil Proceedings) Rules 1996 (Vic) O 29—Discovery and Inspection of Documents e.g. 29.02 and 29.03

[10] Tom Brow, 'Preservation: Analysis' visited on March 18, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/perservationanalysis.html>

however, is required to preserve what he knows or reasonably should know that (i) is relevant to the potential action, (ii) is reasonably foreseeable to become evidence in discovery, (iii) may be requested during discovery, and/or (iv) is the subject of a pending discovery request.[12] However, as the duty of data preservation arising is not yet certain in the U.S., the court in *Skeete v. McKinsey & Company, Inc*.[13] held that the duty arises "once a complaint is filed."

According to Australian civil procedure law, the issue of when the duty of preservation shall be served has no clear answer since each jurisdiction has different rules regarding the service of a notice-requiring discovery. For example, the Northern Territory (r29.02), Queensland (O 35r4) and South Australia (R 58.01) automatically impose the preserving obligation without approaching the court whereas Victoria requires a court order to do so.[14]

However, the Victorian Supreme Court decided that a company has the duty to preserve potential evidence, in a recent product liability case April, 2002 when Australia's biggest tobacco company, British American Tobacco Australia Services ("BATAS") had destroyed thousands of internal documents to deliberately subvert court process and to deny Melbourne lung cancer patient, Rolah McCabe, a fair Trial[15] The plaintiff was awarded $700,000 in damages after Justice Eames found that the company had obliterated CD-ROMs on which 30,000 documents were imaged together with lists of the documents. The judges stated that "the decision to destroy all

---

[11] Brendan Scott, 'Electronic Document Management- Some Traps for Young Players' visited on December 6, 2002 at <http://www.gtlaw.com.au/t/publications/default.jsp?public=275>

[12] Peter V. Lacouture, 'Discovery and the Use of Computer-Based Information in Litigation' (1996) *Rhode Island Bar Journal.*

[13] No. 9099 (S.D.NY. 1993 (LEXIS)

[14] Stephen Colbran et al., *Civil Procedure: Commentary and Materials,* Butterworths, Sydney, 1998 p. 473

[15] '$700,000 win to smoker after evidence destroyed', *The Age* (Melbourne, Australia) visited on April 13, 2002 at <http://www.theage.com.au/cgi-bin/common/printArticle.pl?path=/articles/2002/04/11/1018333398251.html>

such lists and records can only have been a deliberate tactic designed to hide information as to what was destroyed." [16]

In fact, those destroyed documents and records had been used as evidence in a previous smoking-related litigation which Phyllis Cremona, an Australian smoker, sued BATAS in 1996.[17] After the Cremona case, although the case had been settled, significant concerns to corporate counsels of BATAS were raised in regard to its document policy. Thus, many of the Cremona documents were destroyed, as the company's retention policy was to keep documents for five years only, according to the testimony of former BATAS's employees.[18] The destruction of potential evidence after Cremona was considered by Justice Eames told a calculated risk or an obstacle to a potential lawsuit. This case indicates that the obligation to preserve relevant documents would arise whenever litigants weight foresee potential lawsuits regardless of whether or not a complaint or notices had been served.

The U.S. and Australian courts seem to consider the obligation of preservation in terms of a reasonableness standard to be applied to litigants rather than the receiving notice standard. The reasonableness standard is quite broad in terms of defining the duty of data preservation, as most lawyers would be aware of what documents or information might be requested by potential opposing litigants. Such relevant materials, thus, should not be destroyed since the courts may not execute for the pretended innocent destruction of potential documents regardless of whether or not the destruction occurred prior to a lawsuit.

The duty of preservation might be a frustration to certain corporations using information technology (IT) e.g. computers and the Internet in the offices, especially large corporations having more than 100 employees. One U.S. leading computer forensic, Electronic Evidence Discovery has researched and reported that each

[16] *Ibid.*
[17] *Ibid.* n 15
[18] *Ibid.*

employee might receive more than 30 e-mails a day, which is not unusual. If a company had 1,000 employees, this would adds up to 210,000 e-mails weekly, or 10.9 million annually.[19] The research also estimated that a company with 10,000 employees, might receive up to 2.1 million each week or 109 million each year, while 100,000 employees create 21 million e-mails each week or over 1 billion a year![20] Furthermore, an Amway Corporation's general counsel (Amway is one of world's leading manufacturers and distributors of personal and home care products) stated that he usually received more than 100 e-mails per day.[21] "With more than 14,000 employees worldwide, the amount of e-mail created on a daily basis is remarkable," he added.[22]

Corporations employing IT for operating their daily businesses may find it on unbearably burdensome duty to preserve information. One U.S. court held that "a business which generates millions of files of evidence cannot frustrate discovery by creating an inadequate filing system."[23] In addition, courts would sanction document destruction in case of the absence of an effective document retention policy or of having intention to destroy potential evidence, which may be requested in a foreseeable lawsuit.[24] In *Mathias v. Jacobs*[25], for example, the court held that the plaintiff had the duty to preserve information in Palm Pilot that she knew might be relevant. Although information was deleted, it was still discoverable albeit in a more

---

[19] John Jessen, 'Special Issues Involving Electronic Discovery' (2000) 9 *Kan. J.L & Pub. Pol'y* 425. visited on March 18, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/tech/>

[20] *Ibid.*

[21] Timothy Q. Delaney, 'E-mail Discovery: The Duties, Danger and Expense' (1999) *Federal Lawyer*. visited on March 23, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/denlaney.html>

[22] *Ibid.*

[23] *Ibid.*

[24] *Ibid.*

[25] 197 F.R.D. 29, S.D.N.Y. ,2000

difficult way. The action of the plaintiff caused adverse interference.[26] Therefore, the court imposed monetary sanctions from cost as a consequence of spoliation.[27]

The present time may be when corporations should be seriously concerned about safeguarding themselves from potential penalties of the spoliation of evidence. Producing a clear and effective document retention policy and reviewing it regularly would be a safety measure to avoid being faced with the threat of litigation.

1.2 How to Comply with the Data Preservation Order

As discussed earlier with reference to the burdensome duty of data preservation, one may be doubtful about what advice should be offered to clients with respect to a broad court order. The court in *Linen v. A.H. Robins Co*.[28], for example, ordered that parties were prohibited from "discarding, destroying, erasing, purging or deleting any such documents including, but not limited to, computer memory, computer disks, data, compilations, e-mail messages sent and received and all back-up computer files or devices."

In the case of the absence of a document retention policy, corporations may simply not adopt a policy and continue to destroy their documents, which would be in favour of opposing parties. There are risks associated with the adoption of a record retention policy after the receipt of a notice of litigation, as one court stated that "a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy."[29]

Some corporations which already have a document retention policy would struggle with the above court order, since their policies usually require employees to routinely

---

[26] Discovery CLE Library: Preservation, visited on Mach 18, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/presevation/>

[27] *Ibid.*

[28] 10 Mass. L.Rptr. 189, 9 (Mass. Super. 1999)

purge e-mails. The routine deletion of e-mails or other electronic information established by most corporations today may have no intention of destroying any potential evidence in potential lawsuits. It is more likely be a reduction of the costs of storage of out of date information or unwanted junk mail. It is almost impossible to comply with the above court order that prevents parties from deleting any information from computers if parties read this literally. Merely turning on and off computers could cause their RAM to delete certain temporary information on hard drives, therefore, this might be considered as violating the court order. In addition, employees would not be able to clean up all unwanted information if their hard drives were out of space as well as reinstall an operating system in the case of the existing one not work.[30] Such routine work could unintentionally destroy potentially relevant information in compute memory, and could be considered to be a restriction in the data preservation as required by the court.[31]

Lawyers in such situations might request the judge for a limited scope of preservation that could cause a serious obstruction to routine business operation. The judge would require the requesting party to show how the order could negatively affect the daily business operation in order to grant a limitation of the order.[32]

Furthermore, after receiving a broad preservation order, lawyers should advise their clients to have an immediate meeting with their IT department.[33] An immediate backup of all computers networked with the corporate central server and suspension of any backup-tape recycling program would need to be done in an earlier stage. Clients should inform their employees with regard to the duty of preservation under the court

---

[29] Peter V. Lacouture, 'Discovery and the Use of Computer-Based Information in Litigation' (1996) Rhode Island Bar Journal. visited on March 24, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/preservation/lacourture.html>

[30] Tom Brown, 'Preservation: Analysis' visited on March 18, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/preservationanalysis.html>

[31] *Ibid.*

[32] *Ibid.*

[33] *Ibid.*

order and instruct them not to delete any "relevant" documents. Deletion of e-mail should be permitted after being backed up and this would include a completed backup of e-mail on employees' hard drives as well.[34]

II Allocation of Electronic Discovery Costs

2.1 Causes of Excessive Expenses in Electronic Discovery

Electronic evidence consists of four unique types of data subject to discovery: active, replicant, and archival and residual data.[35] Therefore, it is necessary to discuss the distinct features of paper-based evidence and computer-based evidence, in order to understand what are the real factors causing great expenditure in electronic discovery.

First, active data or data files that are currently being used or currently on hard drives, database and servers[36] are readily available and can be accessed from the users' personal computers.[37] Active data is searchable by using the Boolean techniques, which are employed for searching information in typical Internet search engines e.g. Google.com or Yahoo! and in paid electronic information like products of Lexis and Westlaw.[38] The active data is in the form of e-mail messages, word processing documents, spreadsheets, database or calendars which can be reviewed by the Windows Explorer or DOS file list.[39] The active data can be stored in the user's computer hard drive locally or remotely as well as being saved in a portable diskette or a storage device e.g. CDROMs or Zip disks somewhere else. Although the active data is easy to retrieve with the high capacity of storage devices today being able to contain voluminous electronic document lack of data management can cause a high expense in electronic discovery.

---

[34] *Ibid.*
[35] Barbara A. Caulfield and Zuzana Svihra, 'Requiring the Losing Party for the Costs of Digital' visited 23 June, 2002 at <http://www.fiosinc.com/wp-losing.html>
[36] John Jessen, 'Electronic Evidence Discovery' (2000) 9 Kan. J.L. Pol'y 424. visited 18 March, 2002 at<http://cyber.law.harvard.edu/digitaldiscovery/liabrary/tech/>
[37] Carey Sirota Meyer and Kari L. Wraspir, 'E-Discovery: Preparing Clients for (and Protecting Them Against) Discovery in the Electronic Information Age' (2000) William Michelle College of Law.
[38] *Ibid.* n 36.
[39] *Ibid.* n 37.

Second, replicant data that are sometimes called "temporary files" or "file clones" are computer-generated files, which are automatically created and periodically saved as copies of a file currently used by the user.[40] An example of a replicant file can be found when clicking on the "redo" or "undo" command.[41] The replicant file is not immediately accessible and can be expensive to retrieve.

Third, archival or legacy data are usually stored in backup tapes. Backup tapes record almost everything in the system at a given time.[42] The information on backup tapes is not immediately accessible since such tapes can be overwritten many times and the data are saved in a user-friendly format.[43] Archival data are rich with historical information allowing litigants to track an electronic tale otherwise beyond their reach. Retrieving and gathering data from backup tapes, however, requires a computer forensic expert to assist with such technical tasks, this can be a time consuming and prohibitively expensive task.

Finally, one of the most misunderstood beliefs is that clicking on the "delete" or "purge" button on the computer will cause destruction of such electronic messages. "Deleted" files or e-mails still exist in the form of "residual data" since hitting the delete button merely instructs the computer to write over the hard disk in order to make space for a new file. Thus, deleted files are not actually deleted or do not disappear forever akin to a destroyed paper counterpart, but virtually exist on the surface of the hard drive. Deleted files, however, can be completely wiped by a special program or overwritten with a computer program, which needs to use larger

---

[40] Shira A. Scheindlin and Jeffery Rabkin, 'Electronic Discovery in Federal Civil Litigation: Is Rule34 Up To the Task" 14 *Boston College Law Review* 327. visited 24 March, 2002 at <http://www.bc.edu/bc_org/avp/law/lwsch/journals/bclawr/41_2/03_FMS.htm>

[41] Barbara A. Caulfied and Zuzana Svihra, 'Requiring the Losing Party to Pay for the Costs of Digital Discovery' visited June 26, 2002 at <http://www.fiosinc.com/wp-losing.html>

[42] *Ibid.*

[43] *Ibid.*

space than the existing program. Residual data are also in the form of "inactive data" akin to data in backup tapes and is considered as the most expensive to recover this data.[44] Litigants need to hire a computer forensic expert to restore these previously deleted files even after years, but this can be extremely costly.[45]

Although inactive data such as backed-up data and residual data causes the excessive cost in the discovery process, it seems to be an attractive discovery resource for litigants due to its potential as a "smoking gun". Lawyers could take a risk and put a bullet in this "smoking gun" by requesting an opposite party to produce inactive data for them. Certainly, one dispute in the issue of who would bear the costs of recovering and producing this costly evidence will be raised by a respondent. Furthermore, whether or not the court could allow shifting the electronic discovery costs is unclear in today's circumstances, this will be discussed later.

2.2 Controversial Issues of Cost Shifting Models

The unique characteristic of electronic data raise certain dubious questions regarding the existing law in terms of the evidentiary issue, as well as the discoverable issue of electronic messages. Two important issues need to be analyzed under the civil procedures law and the law of evidence, before discussing whether or not the judges will shift the costs of producing electronic evidence from the respondent to the requesting party, or of which situations could give rise to the allocation of costs in the electronic discovery proceedings.

The first question is whether electronic messages such as e-mail, backed-up files or word processing documents are considered as evidence under existing law. The US Federal Civil Procedure Rule 34 provides that

---

[44] "[I]nactive data must be returned to active data status before it can be searched. This means finding used computer capacity to accommodate it and finding the software the generated it so that it can be read." See at <http://cyber.law.harvard.edu/digitaldiscovery/liability/tecth/>

> "any party to serve on any party to serve on any other party a request to produce and permit the party making the request… to inspect and copy, any designed documents including writings, drawings, graphs, charts, photographs, phonorecords, ***and other data compilations from which information can be obtained, translated,*** if necessary, …or contain within the scope of Rule 26(b)[46] and which are in possession, custody or control of the party whom the request is served." (Emphasis added and edited)]

The above provision has been amended since 1970 in order to comply with changing technology. The Notes to the amendment to Rule 34 impose an obligation on the respondent to provide a "print out" of electronic evidence pursuant to a request from the requesting party.[47] Although there is no such clear language to indicate words such as "electronic messages" or "e-mail", it can be implied that e-mail and other electronic records could fit in to the categories of "documents" and "other data compilations…" Throughout the 1980s and 1990s, the federal courts also ruled that the term "documents", under Rule 34 included e-mail.[48] Therefore, e-mail and other electronic messages are discoverable under the US law.

---

[45] Corinne L. Giacobbe, 'Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data' (2000) 57 *Washington and Lee Law Review* 257.

[46] Rule 26(b)(1) defines the scope of the discoverable information which provides that "parties may obtain discovery… including the existence, description, nature, custody, condition, and location of any books, documents, or other ***tangible things*** and the identity and location of persons having the electronic evidence could fall into any categories of discoverable information under Rule 26 (b)(1), the electronic information could be considered within the scope of documentary discovery under Rule 34.

[47] Shira A. Scheindlin and Jeffrey Rabkin, 'Electronic Discovery in Federal Civil Litigation: Is Rule 34Up To the Task?' (2000) 14 Boston College Law Review 327. visited 23 March, 2002 at <http://www.bc.edu/bc_org/avp/law/lwsch/journals/bclawr/41_2/03_FMS.htm>

[48] Ferris Research, 'Electronic Message Archiving' (2001) visited 25 June, 2002 at <http://www.mimesweeper.com/download/collateral/pdfs/whitepapers/achiving.pdf>

Under Australian law, the term "document" under the *Evidence Act 1995* (Cth) does not clearly refer to any computer recorded or any electronic messages.[49] The Commonwealth and State governments have introduced uniform evidence legislation providing for a presumption in favor of the reliability of evidence produced by process, machines[50] and other devices and documents in the course of business.[51] In addition, the Supreme Court of Victoria in *Murphy & Another v Lew & Others*[52] held that the term "document" in section 3 of the *Evidence Act 1985* (Vic) included computer records and computer-produced documents. E-mails and other electronic documents, thus, are discoverable documents regardless of technical sophistication or difficulty of discovery.[53]

Under Rule 34 of the U.S. and evidence law in Australia, however, there is no clear answer as to whether the newest forms of electronic messages automatically generated

---

[49] Under the *Evidence Act 1995* (Cth) provides the following definition:

> "**document**" means any record of information, and includes:
> (a) anything on which there is writing; or
> (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or
> (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
> (d) a map, plan or photograph.

In addition, Part 2 section 8 of the *Evidence Act 1995* broadens the definition of "document" by including the following:

> A reference in this Act to a document also refer to:
> (a) any part of the document; or
> (b) any copy, reproduction or duplicate of the document or of any part of the document; or
> (c) any part of such a copy, reproduction or duplicate.

[50] See the *Evidence Act 1995* (Cth) Part 4.3 Facilitation Proof Div 1 section 146

[51] *Ibid.* section 147

[52] Unreported, Sup Ct, Vic, No. 12377 of 1991, 12 September 1997.

[53] See *BT (Australia) Pty Ltd v State of New South Wales & Anor* (No.9) [1998] FCA 363. Also, *NT Power Generation Pty Ltd v Power & Water Authority* [1999] FCA 1669.

by a web site without the users' knowledge or consent, such as cookies[54] or cache[55] files, are included in the definition of "discoverable documents". Furthermore, it is doubtful whether "embedded data" and history files having been edited previously could be categorized as "data compilations under Rule 34 and as "discoverable documents" under evidence law in Australia.

E-mail and other electronic documents seem to fit the context of "discoverable document" under both the US and Australian law. As a result of such implications, requesting parties would be threatened by the potential excessive cost of producing "documents" pursuant to the other party's request. Whether or not the court will allow the requesting party to have an overly broad request, in which circumstances the court might limit the scope of discovery and the extent to which the court would consider shifting the cost of discovery, will be discussed later.

Not only might the requesting party ask for all types of electronic data which are in "possession, custody or control" of the respondent, but also their request might include those deleted files and deleted e-mails. It is quite certain in such a situation that the respondent would argue that "deleted" files are no longer exist and are not in the possession of the respondent anymore. Therefore, the respondent's lawyer would file the motion in order to ask the court to shift or allocate the cost if the requesting party requires to recover those deleted files. The other defense for the respondent in order to avoid the obligation to produce voluminous documents which would be, of course, highly expensive, would be to claim that the burden of providing such documents would constitute "undue burden or expense."

---

[54] Cookie means "bits of information about Web site visitors created by Web sites and stored on client computers. : Gary P. Schneider and James T. Perry, *Electronic Commerce*, (2 eds.), Thomson Learning, Canada, 2001.

[55] Cache means "a high-speed memory area set aside to store Web pages." : Gary P. Schneider and James T. Perry, *Electronic Commerce*, (2 eds.), Thomson Learning, Canada, 2001.

2.3 Judicial Reactions to Cost Shifting Rules

In the US, Rule 26(c) of the Federal Rules of Civil Procedures provides courts with ample discretion to protect a respondent against the undue burden or expense that might derive from an overly broad discovery request.[56] Courts, therefore, can shift the costs of the production of evidence for the respondent who has to bear the costs of preparing his own case under the general rule. However, the US courts seem to be reluctant to use this rule to shift cost of production of electronic evidence from the respondent and to compel the requesting party to bear the cost. In *Re Brand Name Prescription Drugs Antitrust Litigation*[57], for example, the class plaintiffs moved to force the defendant to disclose its e-mails. Although the defendant accepted that e-mails were discoverable, it argued that the plaintiffs' request was overly broad, burdensome, and expensive.[58] The defendant, thus, asked the plaintiffs to pay roughly $50,000-$70,000 to recover e-mails. The judges were unconvinced by the defendant's reason and ruled that expense was mainly due to the defendant's own record-keeping scheme. The court, therefore, did not order the cost shifting to the plaintiffs.[59]

Another important case where the court in *Bill v Kennecott*[60] considered that Rule 26(c) regarding shifting the costs of production should be used to solve cases on a case-by-case basis rather than by "iron-clad formula"[61] according to the fact that plaintiffs requested the production of document containing data of the defendant's employees. The defendants offered two options in order to supply the information either in electronic form (i.e. on a computer storage device) or in hard copy (i.e. the printout). However, the defendant had a condition pursuant to its offer that the plaintiff should pay the cost of producing information for $5,400. Although the plaintiffs chose to receive the hard copy information, they would not pay unless the court ordered

---

[56] *Ibid.* n 45.
[57] 1995 WL 360526, N.D. III.
[58] Alexi Maltas, 'Analysis by Digital Discovery CLE Teaching Fellow', visited 18 March, 2002 at <http://cyber.law.harvard.eud/digitaldiscovery/library/cost/>
[59] *Ibid.* n 58.
[60] 108 F.R.D. 459, 462 (D. Utah 1985)
[61] *Ibid.* n 40.

them to do so. The defendant produced the hard copy and filed the motion for shifting costs under Rule 26(c).[62]

The *Bill* court stated that both options of defendant were unreasonable and impractical with regard to electronic evidence since the opponent might be lack expertise or tools to assist him or her in an inspection.[63] The court also ruled that the requested party would not have to elect any choices, but could expect to inspect an intelligible form of evidence. Importantly, the court refused to grant the defendant's request to shift costs for four reasons: (1) the amount of money involved was not excessive or inordinate; (2) the relative expense or burden would be substantially greater to the substantial burden of the plaintiffs; and (4) the responding party derived some benefit by producing the data in question.[64]

The US courts appear to be questioning the defendant's request to shift costs for the production of electronic evidence. One court stated that "it would be a dangerous development in the law if new techniques for easing the use of information became a hindrance to discovery or disclosure in litigation."[65] The court pointed out in *Itzenson v Hardford Life and Accident Insurance Co.*[66]that "it is difficult to believe in the computer era" that the defendant could not identify files based on specific categories. The assertion of the defendants with regard to the complex and unique characteristics of technology seem to be unreasonable for shifting cost.

The cost shifting issue regarding production of electronic evidence in Australia is not expressed clearly elsewhere. Federal and State Courts provide their practice and procedures so that the court encourages the parties to use electronic evidence in the hearing and other procedures.[67] The parties, thus, should agree between themselves

---

[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid.* n 40.
[65] *Daewoo Elecs Co. v Untied States*, 650 F. Supp. 1003, 1006 (Ct. Int'l Trade 1986)
[66] 2000 U.S. Dist. LEXIS 14680, 3(E.D. Penn. October 10, 2000)
[67] Federal Court of Australia: Practice and Procedure Part 1 Discovery visited

about a protocol for exchanging electronic data. The court rules, however, do not provide any solution or guidance about what they should do that if parties cannot agree in producing cost of electronic evidence. It is certain that the court would be asked from them to solve such disputes.

However, there are certain clues in case law that suggest that the Australian court might have a similar agenda akin to the US court counterpart in the issue of shifting costs. In Joseph *Gersten v Australian Federal Police* [68], although the court did not directly point out the shifting cost issue, it warned the defendant that "It would be unreasonable for an agency to refuse a request on this basis [difficulty of discovery] if the problem in locating documents resides in poor record-keeping". Electronic records, thus, should be supplied regardless of the respondents' technological problems or system deficiencies. [69]

In *BT Australia Pty Ltd v State of NSW & Telstra Corp. Ltd*[70], the court ordered Telstra to retrieve existing backed-up tapes and produce the requested e-mail within a specific time. There was no shifting of the cost of producing electronic evidence in this case. The fact merely showed that Telstra carried its own costs in producing the requested electronic records.[71]

Some commentators argue that courts should not treat the electronic evidence as equivalent to a conventional discovery since the unique features of electronic evidence

---

3 June, 2002 at <http://www.fedcourt.gov.au/pracproc/practice_notes_cj17.htm>
See also Supreme Court of Victoria: Practice Note No. 3 of 1999 visited 3 June, 2002 at <http://www.supremecourt.vic.gov.au/pns/99pn3.htm>

[68] [1999] AATA 819

[69] Kathy Sinclair, 'Australian Law and Digital Records', visited 25 June, 2002 at <http://vers.imagineering.net.au/site-ver2/erecord_library/Document%20(pdf)/E-library/…)

[70] *BT Australia Pty Ltd v State of NSW & Telstra Corp. Ltd* (Cross Claimant to First Cross claim) *v BT Australia Pty Ltd. Telecommunications PLC (Second Cross Respondent to First Cross Claim*)…(see references for full citation) No. NG 572 of 1995 FED No. 363/98

[71] *Ibid.* n 69.

could open a new door for the abuse of proceedings by a requested party.[72] If there is no limitation on the scope of electronic discovery, the requested party might oppress the opponent by using an overly broad request.[73] Furthermore, these commentators suggest that not only do courts lack sufficient technological knowledge, but in addition, there is a lack of clear guidelines in both the statutory rules and case law in terms of shifting costs in the production of electronic evidence.[74] Mandatory shifting of costs at judgment[75] are suggested to prevent the exercise of judicial discretion.

In fact, establishing a shifting cost rule in specific detail might result in certain disadvantages since courts would unable to provide an appropriate solution to the allocation cost for both parties. The reason why courts do not allow shifting the cost of production of evidence to the requesting party would be justifiable where most defendants were giant corporations and had superior resources in technology and finance, but were not prepared to deal with their information systematically. Thus, they should not permit pushing their burden on to a plaintiff having no decision making power over the defendants' document retention schemes. In addition, the respondent wanting to shift the production cost might provide insufficient information regarding the causes of excessive cost that did not derive from a lack of responsibility of the respondent, other than from the nature of the electronic evidence itself or from an overly broad request of the requested party. The party who can take advantage of the court order would be the one who could well educate the judges in the unfamiliar matters like the issue of electronic discovery.

---

[72] *Ibid.* n 40.

[73] Alesxi Maltas, 'Cost: Aalysis' visited 19 March, 2002 at <http://cyber.law.harvard.edu/ditigaldiscovery/library/cost/costanalysis.html>

[74] *Ibid.* n 40.

[75] Barbara A. Caulfield and Zuzana Svihra, 'Requiring the Losing Party to Pay for the Costs of Digital Discovery' , visited 26 June, 2002 at <http://www.fiosinc.com/wp-losing.html>

III Processes for Digital Discovery

3.1 Sources of Electronic Evidence

Electronic information is typically stored on magnetic or optical storage devices such as diskettes (including floppy disks and Zip disks) backup tapes, and CD-ROM.[76] Other backup tapes may be available, for example in systems that are no longer in use as well as off-site backups or store media.[77] Hard drives including portable drives and laptops off-site certainly store a lot of significant information in hidden files and residual files.

The operating systems in particular the PC or network servers related to the manner in which electronic data is organized, stored, deleted and accessed should not be overlooked.[78] All e-mail servers and their backup schedules are also essential and a possible source of such Internet related files can be obtained from a third party such as Internet service providers (e.g. AOL or Compuserv) or specific Network servers. Electronic discovery should not include only on-site searches of office use of computers and storage devices, but it should also include off-site discovery (e.g., at employees' home or corporate information warehouses elsewhere) or personal use of electronic devices such as personal digital assistants (PDA), digital cameras, cellular phones, pagers and PCMCIA memory cards.

3.2 How to Search and Obtain E-Evidence

A) Send Preservation Notice to Adversary

Since electronic data is very sensitive and crucial information can be destroyed simply by booting the computer[79], the sooner the notice is sent the better.[80] The party serving on the notice has legal obligations to preserve all relevant documents including

---

[76] Deborah Schepers, 'The Power and the Dangers of E-Discovery' visited 20 March, 2002 at<http://www.legalmediagroup.com/techlawlive/includes/print…>

[77] *Ibid.*

[78] David H. Schultz, 'Beyond Fingerprints: Recovery of Electronic Evidence' visited 29 May, 2002 at <http://www.ontrack.com>

[79] *Ibid.*

electronic documents as demonstrated in *Turner v Hudson Transit Lines, Inc.*[81] However, the obligation of preservation arises if a party foresee that relevant documents might be requested in litigation. In *Applied Telematices, Inc. v Sprint Communications Company, L.P.*[82], the court ruled that although the plaintiff failed to send a preservation notice to the defendant, this did not relieve defendant of his affirmative duty to do so.

The notice should be drafted carefully in order to cover all necessary types of potential electronic evidence. The notice should indicate the type of electronic data to be preserved for example, e-mail, files created by word processing, electronic calendars, etc.[83] The scope of locations should be cited in the notice, that is, where information may exist e.g., servers, hard drives or off-site storage should not be overwritten. In particular, the practice of recycling backup tapes used for backup purposes must cease.[84] Both parties may need to ensure preserving potential information with integrity by agreeing to be bound by a protocol indicating the manner of preservation and production of evidence either in hard copy or in electronic forms.[85]

B) Requirements of Technological and Expertise Assistance

Efficiency and speed of discovery processes are required for a good search-term list provided by the parties. The key-words list accounts for alternate spellings or terms for relevant issues regarding the case.[86] A sophisticated software program incorporated with the key-word list is designed to scan and sort data. A powerful program can assist

---

[80] Joan E. Feldman and Rodger I. Kohn, 'Collecting Computer-Based Evidence' visited 24 March, 2002 at <http://www6.law.com/ny/tech/012698t6.html>
[81] S.D.N.Y. 1991
[82] E.D. Pa. 1996
[83] Adam I. Ohen and David J. Lender, 'Electronic Discovery Practice Guidelines' visited 26 June, 2002 at<http://www.weil.com/weil/EDPGWHOLE.pdf>
[84]Deborah Schepers, 'The Power and the Dangers of E-Discovery' visited 20 March, 2002 at<http://www.legalmediagroup.com/techlawlive/includes/print…>
[85] Josh Solomon, 'Process: Analysis' visited 19 March, 2002 at<http://cyber.law.harvard.edu/digitaldiscovery/library/process/processanalysis.html>
[86] Jeff Lendino, 'Practical Guidance for Conducting Electronic Discovery' visited 29 May, 2002 at <http://www.ontrack.com>

not only in the finding of relevant information, but also has the capacity to segregate privileged data, to index items and to automatically open and convert files to "read-only" formats to ensure data authenticity.[87]

A fully automated approach and half-electronic and traditional methods can be combined. Each method will be discussed in detail later. Fully automated processes can reduce time, labor and expense compared to a purely manual approach. Employment of a combined approach involves printing information for reviewing. However, one must be concerned about the opponent party's and the court's expectations.[88] Once selected files are printed and re-scanned, the residual and embedded data are gone. In such circumstances, discovery may not occur.[89]

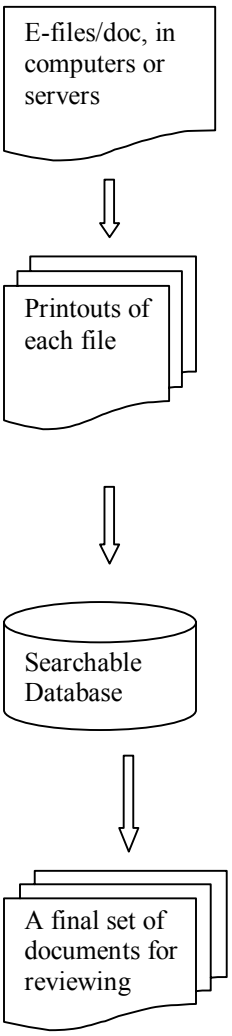
To accomplish electronic discovery processes, for important reasons lawyers may need assistance from computer forensic experts. For example, recovering such inactive or residual data on a hard drive is not possible if data collectors lack appropriate expertise in computer forensics. Imaging copies of residual data including deleted files, fragments and other data remaining on the disk surface is capturing such data and all data on the disk surface and transferring it to the target drive.[90] Making imaged copies is known as mirroring computer files. This is done sector by sector of the hard drive and this method is better than selecting a file-by-file copy, which will not capture any residual data.[91] Such complicated data imaging, and the collection of hidden data must be performed by computer forensic experts having experience in the field.

---

[87] *Ibid.*
[88] *Ibid.* n 85.
[89] *Ibid.*
[90] Joan E. Feldman and Rodger I. Kohn, 'Collecting Computer-Based Evidence' visited 24 March, 2002 at <http://www6.law.com/ny/tech/012698t6.html>
[91] *Ibid.*

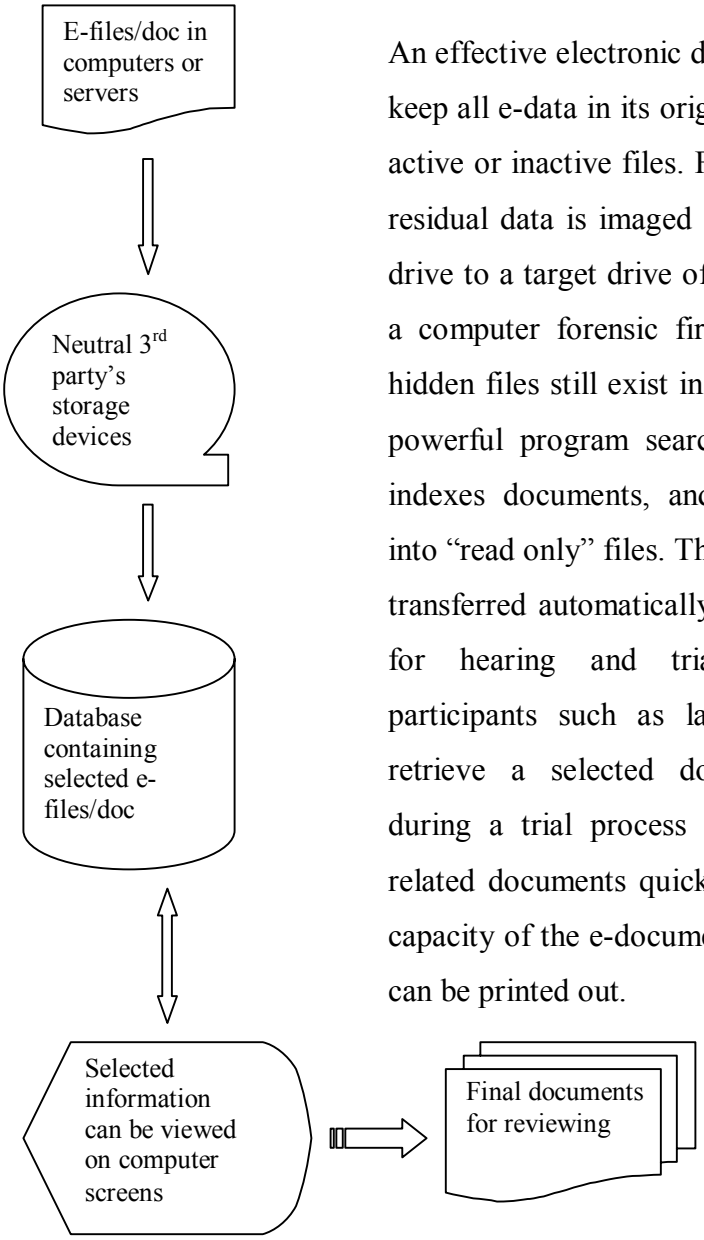
C) Traditional Electronic Discovery vs. Effective Electronic Discovery

Traditional Model of Electronic Discovery



Typically, litigation support firms have used the following steps. First, all electronic files are opened and inspected by a client and his lawyers. Second, selected files are printed out, and residual files, hidden information or metadata is lost in this process. Third, printouts are manually re-classified, numbered and re-scanned into a searchable database. Finally, in hearing and trial processes, a final set of documents can be printed out again for reviewing or alternatively can be viewed on the computer screen. Most re-scanned documents appeared in the form of image files, e.g., PDF, JPEG and GIF files. Such imaged files are not searchable without numbering. This traditional e-discovery creates great expense in respect to a manually classified document process as well as creating excessive paper work. Therefore, this method is not efficient for use in highly complicated cases with much e-information involved.

Effective Model of Electronic Discovery



An effective electronic discovery method aims to keep all e-data in its original form either through active or inactive files. First, all e-data including residual data is imaged or mirrored from a hard drive to a target drive of neutral third party (e.g. a computer forensic firm). Metadata and such hidden files still exist in e-documents. Second, a powerful program searches for relevant items, indexes documents, and convert selected files into "read only" files. These selected files will be transferred automatically to a database prepared for hearing and trial processes. Finally, participants such as lawyers and judges can retrieve a selected document for reviewing during a trial process as well as referring to related documents quickly due to the seachable capacity of the e-documents. Alternatively, there can be printed out.

IV Spoliation Data: A Case Study of Arthur Andersen

Spoliation is the term using for destruction or alteration of evidence. The destruction of paper based evidence or digital evidence is associated with legal liability and harsh sanction from courts.[92] A corporation can be penalized ranging from monetary fines to a default judgment if there is a wilful destruction of evidence. In particular, if the defendant acting in a bad faith has shredded e-mail, for example, the harshest sanctions, e.g., default judgment and criminal punishment will be imposed on him.[93] Sometimes, negligent conduct is also accounted as acting in a bad faith. Thus, litigants and their lawyers have a duty to preserve evidence.

Misconception in the nature of electronic data i.e., that it is easy to destroy by simply hitting the "delete" button, can lead to a disastrous result by a party intending to destroy such evidence. At this moment, Arthur Andersen ("Andersen") would know the test of spoliation's sanction better than anybody else. Andersen was the one of top five accounting firms in the U.S. It was also an accountant for the Enron Corporation, the seventh largest US corporation, during the past 16 years, until Enron bankrupted in December 2001.[94]

For unspecified reasons, Andersen intended to cover up Enron's information under its control. Thus, Andersen employees on the Enron engagement team were ordered to shred physical documentation and delete computer files related to Enron's information.[95] Later on, the US Securities Exchange Commission ("SEC") served Andersen with a subpoena relating to its work for Enron. There was no more shredding since the firm had been "officially served" for documents. On or about November 2001, Andersen was charged with the action of obstruction of justice and

---

[92] Matt Delmero, 'Spoliation: Analysis' visited 19 March, 2002 at<http://cyber.law.harvard.edu/digitaldiscovery/library/spoliation/spoilationanalysis.html>

[93] *Ibid.*

[94] Indictment: U.S. v Arthur Andersen, visited 18 March, 2002 at<http://news.findlaw.com/scripts/printer_friendly.pl?>

[95] *Ibid.*

intentional spoliation of evidence.[96] Andersen, however, claimed that its document destruction was pursuant to its retention policy. Recently on 15th June, a federal jury convicted Arthur Anderson of obstruction of justice for impeding an investigation by the SEC in the case of Enron. Sentencing has been scheduled for October 11st , 2002 and Andersen faces the possibility of fines up to $500,000.[97]

The fine sanction for Anderson seems not as bad as the end of the 88 years old giant accounting firm employing 83,000 people worldwide and having 2,300 corporate clients in the US. Andersen will cease practising by August 31, 2002.[98] The firm has lost 690 of its 2,311 public corporate clients since January 2002.[99] Most of its overseas branches have merged with other firms. Loss of reputation in the professional field for Andersen with regard to spoliation of data would be a great lesson for other professional businesses attempting to cover up the truth by shredding information, in particular electronic information, that could return to haunt the defendant in litigation. One commentator stated that "Their strategy to me has been very curious, and I don't think it's been very smart. They have been publicly predicting their own demise to scare the Justice Department."[100]

V Evidentiary Issues

Once discovery and gathering of all electronic documents or records is complete, and then lawyers then need to introduce such evidence before the court. There are three important issues in regard of the admissibility of electronic evidence:

- whether electronic evidence can be appropriately authenticated;
- whether electronic evidence is hearsay and is subject to any exception; and

---

[96] *Ibid.* n 94.
[97] Kurt Eichenwald, 'Andersen Guilty of Shedding Files in Enron Scandal' visited 17 June, 2002 at<http://www.nytimes.com/2002/06/16/business/16AUDI.ht..>
[98] *Ibid.*
[99] *Ibid.*
[100] Caroline Overignton, 'Andersen Slams Charges' visited 18 March, 2002 at <http://www.theage.com.au/cgi-bin/common/printArticle.pl?..>

- whether the best evident rule requiring the original document is applied to electronic documents.

The lawyer tendering electronic evidence should answer these questions in order to ensure admissibility of such evidence by establishing 1) who created the document; 2) its contents; 3) how it was created; and 4) that it has not been altered, either intentionally or unintentionally.[101]

However, it is important to note that the evidentiary issues discussed here refer to electronic messages or records, excluding electronic evidence in commercial transactions, for example, online purchasing goods and services, electronic funds transfer (EFT) or electronic data interchange (EDI). Electronic documents in such commercial transactions are admissible as electronic evidence under the individual specific legislation of each country such as the US Uniform Electronic Transaction Act (1999), US Electronic Signatures in Global and National Commerce Act, Australian Electronic Transaction Act (1999)(Cth) and State Electronic Transaction Act (2000), e.g., Victoria, New South Wales, and Tasmania.[102] Such electronic records fall within the scope of this legislation, thus, they are no longer an issue.

5.1 Authentication

Authentication requires 1) that the contents of documents have remained unaltered; 2) that the information in the document does indeed originate from its intended source either human or machine; 3) "extraneous information" for example, the affixed date on the document is correct.[103] In the paper based world, the documentary evidence would prove its authentication by identified items from witnesses such as autographs, fingerprints, and photographic identification cards, acknowledgments before notaries, letters of introduction, signature guarantees from banks, postmarks on envelopes,

[101] Michael R. Overly, 'The Admissibility of Electronic Documents' visited 26 June, 2002 at <http://www.forensics.com/resources/admiss.htm>

[102] Queensland, Northern Territory and Australian Capital Territory have passed their Electronic Transaction Act since 2001.

records of returned receipt and so on.[104] Reed suggested that these traditional authentication modes of paper based evidence should apply equally to electronic evidence. Authentication of electronic evidence, however, seems to be problematic since electronic messages are easily tampered with and forged, and such activities are almost undetectable. For example, an anonymous computer hacker intercepts e-mail and then changes its content. If the opposition challenges the identity of the originator or the contents of electronic documents, this would be very difficult to authenticate.

The proponent desiring to admit electronic documents into evidence or to prove the authenticity of these documents essentially needs to show two factors: *origin,* that is, who or what created the document; and *integrity,* that is, whether its contents are complete and in the form proposed and without error or forgery.[105] Traditionally, the authentication of a handwritten document can be proved by comparing the author's handwriting with the text of the document.[106] By analogy, electronic documents may be authenticated by technological assistance in three methods such as using encryption authentication (i.e., digital signatures), audit trails[107], and transmission via an intermediary.[108]

The above facilitating tools for the authentication of electronic documents seem to be sophisticated. Some commentators even think that, the courts would raise the standard of admission in electronic evidence marking tougher than other traditional forms of

---

[103] Chris Reed, 'The Admissibility and Authentication of Computer Evidence- A Confusion of Issues' visited 25 January, 2002 at <http://www.bileta.ac.uk/90papers/reed.html>

[104] *Ibid.*

[105] Jane K. Winn and Benjamin Wright, *Law of Electronic Commerce.* (4th eds.), Aspen Law & Business, New York, 2002. p. 20-12

[106] Michael R. Overly, 'The Admissibility of Electronic Documents' visited 26 June, 2002 at <http://www.forensices.com/resources/admiss.htm>

[107] Audit trails can trace back the log in or log out times via large computer networks, e.g., the Unix or Window NT operation systems. There are some limitations for audit trails that they can only identifies the computer sending the message, but not the sender. Computers can also create a false audit trail. Audit trails cannot tell whether information in the message has been altered.

evidence. This has proved to be wrong since US courts, in particular, take a flexible approach to admission of electronic evidence. In *United States v. Catabran*[109], for example, the court stated that "it was immaterial that the evidence had been contained in a computer rather than a more traditional medium such as books, assuming the proponent laid a proper foundation for admissibility."[110]

Many technologically related cases seem to require an expert witness to introduce special evidence such as electronic documents. Interestingly, in *United States v. Linn*[111], the court held that a computer-records foundation witness need not necessarily be a computer expert. As long as the witness personally knew the source of the records and could show that the records qualified as a business record, the court was satisfied.[112]

The *US Federal Rules of Evidence* ("FRE") section 901(a) is equally applied to computer generated records as traditional evidence. The provision merely requires "evidence…showing that the process or system process or system produces an accurate result" that would be different from the requirements for the conventional forms of evidence. Generally, the standard for admitting electronic evidence remains unchanged. The above sophisticated tools for authentication, thus, would not be considered as crucial as the accuracy of the document itself. In *Perfect 10, Inc. v. Cybernet Ventures, Inc*[113]., the court was not convinced in the intellectual property infringement litigation that all evidence printed from web sites was inauthentic and inadmissible. The court, nevertheless, ruled that the printouts were properly authenticated under Fed.R.Evid. 901(a) where the plaintiff's CEO sufficiently showed

---

[108] *Ibid.* n 106.
[109] 836, F. 2d 453, 457 (9th Cir. 1988)
[110] David H. Schulz, 'Beyond Fingerprints: Recovery of Electronic Evidence' visited 29 May, 2002 at <http://www.ontrack.com>
[111] 880 F.2d 209 (9th Cir. 1989)
[112] *Ibid.* pp 20-05.
[113] 2002 WL 731721 (C.D. Cal. April 22, 2002)

"true and correct copies of pages printed from the Internet that were printed by [him] or under his direction."[114]

5.2 Hearsay Rule

Hearsay is defined as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence ***to prove the truth*** [emphasis added] of the matter asserted." [115] It also notes that a statement can be "an oral or written assertion." Additionally, FRE 802 states that "hearsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress."[116]

The main purpose of hearsay is to prevent an out-of-court statement or evidence, which may lack reliability and completeness, as an out-of-court statement is not tested by cross-examination. Unlike a witness in court, the person owning an out-of-court statement does not take an oath to tell the truth. However, this does not mean that all out-of-court statements are hearsay. If a statement is merely stated to show that it was made, rather than it was *true*.[117] The statement, therefore, is not hearsay.[118]

---

[114] Ontract.com, 'Electronic Discovery and Computer Forensics: Case Law' visited 29 May, 2002 at <http://www.ontrack.com>

[115] FRE 801(c)

[116] Anthony J. Dreyer, 'When the Postman Beeps Twice: the Admissibility of Electronic Mail under the Business Records Exception of the Federal Rules of Evidence'(1996) 64 *Fordham Law Review* 2285.

[117] *Ibid.* n 105 pp. 20-06.

[118] *For example*, Anne says to Bob that "I has hacked into our school's computer network last weekend." If Anne's statement was made out-of-court, Bob testified in court what Anne said could be considered as hearsay. Since Bob offered to show the truth is what Anne has done, it is an attempting to prove the truth. However, if Bob merely offers to identify the fact that Anne was the teller's statement. This is not to prove what Anne's statement, but merely showing the fact by Bob that he was an witness of Anne's statement. Therefore, the latter is not hearsay and admissible as an evidence.

The "hearsay Rule" is the most notorious bar to admissibility.[119] There are two sides to the argument as to whether or not an electronic record, e-mail and printouts of such records would be considered as hearsay. On the one hand, because the author of an electronic record is usually not available; thus any submission to prove the truth of the matter asserted is hearsay.[120] In a corporation, for example, electronic documents may be created, edited and make copious copies may be demand by different employees. Therefore, employees could forget which documents were created by them or they are no longer be working for the corporation.

On the other hand, electronic documents generated by a computer, e.g. a receipt statement of a banks form an ATM, without human intervention is considered not to be hearsay and will be admitted. Load Hoffmann in *R v Governor of Brixton Prison and Another, ex parte Levin*[121] *reasoned* that if the computer printout is not adduced to prove any fact claimed in it, then it is not hearsay. His Honor also suggested that:[122]

"The printouts are tendered to prove the transfers of funds which they record. They do not *assert* [emphasis added] that such transfers took place. They record the transfer themselves, created by the interaction between whoever purported to request the transfers and the computer program in [the bank]."[123]

Lord Hoffmann's opinion may well be justified in its application to conventional legal principles in relation to modern disputes concerned with law and technology. In fact, hearsay rules preventing doubtful out-of-court evidence which was not witnessed by anybody may be difficult to apply to the product of an automatic machine, for example, automatic e-mail reply programming or IP address[124] issued by the

---

[119] Kimberly D. Richard, 'Electronic Evidence: to Produce or Not to Produce, That Is the Question' 21 *Whittier Law Review* 464.
[120] *Ibid.*
[121] [1997] 3 WLR 117
[122] Ben Fitzpatrick, 'Computers, hearsay, and the status of extradition proceedings', visited 25 January, 2002 at <http://webjcli.ncl.ac.uk/1998/isssue1/fitzpatrick.html>
[123] *Ibid.*
[124] IP (Internet Protocol) or TCP/IP: The set of protocols that provide the basis for the operation of the Internet. The TCP protocol includes rules that computers on a

transmitted computer when sending e-mail or other electronic messages. There is no point in raising the question of the computer witness since it can be concluded that there was "no such witness". Fitzpatrick also pointed out that "…some statements, although in form assertive and inadmissible if they were to originate in the minds of human beings, in fact originate in some purely mechanical function of a machine and can be used circumstantially to prove what they appear to assert."[125]

However, whether electronic messages or their production (i.e. printouts) being hearsay, are not longer to be an argument of admissibility under the hearsay rule. In both the US and Australia, the statute and case law of evidence exempt the bar from hearsay rule for electronic messages as well as printouts, provided they qualified as "business records." In US case law, for example, in *State of Wash v. Ben-Neth*[126] the court held that computer-generated evidence is hearsay, but might be admitted as a business record provided a proper foundation was laid. In *Sea-Land Service, Inc. v Lozen Int'l*, the court admitted an internal company e-mail, which an employee of the plaintiff had forwarded to the defendant. The defense convincingly argued on appeal that the e-mail was not excludable hearsay, since her remarks in forwarding the e-mail showed that an adoption or belief in truth of the information contained in the original e-mail. The court held that this satisfied the requirements for an adoptive admission under FRE. 801(d)(2)(B).

In Australia, the *Evidence Act 1995* (Cth) has unified the law of evidence of the Commonwealth and the states in order to admit documentary and computer-generated evidence, as an exception to the hearsay rule.[127] E-mail or other electronic messages, therefore, fall under the exception of hearsay evidence under section 69: business

---

network use to establish and break connections. The IP protocol determines routing of data packaging.: Gary P. Scheider and James T. Terry, *Electronic Commerce*, Thomson Learning, Canada, 2001.

[125] *Ibid.* n 122.

[126] *Ibid.*

[127] Andrew Ligertwood, *Australian Evidence: Cases and Materials,* Butterworths, Sydney, 1995.

records and section 71: telecommunication of the *Evidence Act.* [128] Australian case law also laid down in the admissibility of print outs in *Henry John Tasman Rook v Lucas Richard Maynard* [129], that there was no doubt in the accuracy of the printouts and there was no difference between information represented on the computer screen and on the printouts.[130] The court, thus, admitted the printouts as evidence through the exception of the hearsay rule even though the appellant argued that "the printed material was different in appearance from the information as presented on-screen, and in fact was a deficient representation."[131]

Not all electronic messages, however, will fall under the exception of hearsay rule as business records. The court in *Monotype Corp. v Int'l Typeface Corp.*[132] denied the admission of a detrimental e-mail in a licence infringement action, because of the prejudicial nature of the message and fact that the e-mail was not admissible under the business record exception. The ultimate goal of hearsay exception still remains in the trustworthiness of electronic records themselves. Courts have sometimes employed this common law exception to admit records failing to qualify as business records.[133] In *Karme v Commissioner*[134] , the court accepted foreign bank records, which proved to have appropriate trustworthiness although the foundation witness seemed to fall outside the scope of the business records.[135]

---

[128] *Ibid.*
[129] No. LCA 112/1993 Judgment No. A97/1993 Evidence (1994) 70A Crim R 133 (1993) 2 Tas R 97, (1993) 126 ALR 150.
[130] Kathy Sinclair, 'Australian Law and Digital Records', visited 26 June, 2002 at <http://ves.imagineering.net.au/site-ver2/erecord_library/Document%20(pdf)/E-library…>
[131] *Ibid.*
[132] 43 F. 3d 443 (9th Cir.1994)
[133] *Ibid.* pp. 20-06.
[134] 673 F. 2d 1062, 1064-1065 (9th Cir. 1982)

5.3 Best Evidence Rule

The best evidence rule requires the "original" writing, recording, or photograph in order to prove the *content* of writing.[136] Since information traditionally is based on paper, the best evidence is considered to be the same as the "original document rule."[137] The proponent attempting to prove the truth of the contents need to show the original documents if such documents exist. Duplication of the original documents can also be admitted as evidence to prove the truth of the information, but courts would weight the duplication of documents less than the original one.

The best evidence rule aims to prevent the use of copies of original documents, so called secondary evidence, which may contain error and incomplete information. Furthermore, it also aims to prevent fraud from misleading information, which is edited or summarized from the original contents. The rule is in favor of direct observation.

An "original" for the purpose of the best evidence rule becomes a problematic concept in an electronic environment. Most questions concern whether a printout of computer data is an original under the best evidence rule. If the printout is considered a mere duplication of information in the computer, the question arises, whether a proponent of such computer information need to turn on a computer to show the courts such information. This seems to be impractical. Moreover, it is doubtful as if a printout is considered to be equal to the original, every printout is almost identical, and the question is which one is the original.

It is, however, no longer in question that any computer printout or data containing in computers under the US law may be regarded the best evidence rule. Since the FRE section 1001(3) provides that "data are stored in a computer or similar device, any

---

[135] *Ibid*. n 133.
[136] US Department of Justice, ' Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal' visited 18 February, 2002 at <http://www.cybercrime.gov/searchmanual.html>
[137] *Ibid.* n 105 pp. 20-30

printout or other output readable by sight, show to reflect the data accurately constitutes an "original" of the electronic information. Not only are computer printouts treated as equal to the original under the best evidence rule, but also summaries of computer-generated data are admissible such may be otherwise barred by the hearsay rule.[138] The US approach to the computer-generated information under the best evidence rule may be a good solution in order to avoid argument about the original of printouts.

The best evidence rule in Australia, however, lacks certainty with regard to the original of electronic documents and their printouts.[139] Of course, Australian courts could admit the copy as evidence if the proponent fails to offer the original. In *Butera v Director of Public Prosecutions for the State of Victoria*[140], the court stated that the best evidence rule was not the rule for exclusion evidence; therefore, copies of audio tapes were admissible if " the provenance of the copy tape of the original tape, the accuracy of the copying process and the provenance of the copy tape are satisfactorily proved." The *Butera* court noted further that "some modes of proof are better than others, but that…goes to weight rather than admissibility."[141]

As a result of above case law, computer printouts may be admissible, but courts would weigh them less than the original on the ground of the best evidence rule. There is no clear answer for this since the *Commonwealth Evidence Act* (1995) and case law do not explicitly define the term "original" to include computer generated printouts.

In *Amstrong v Executive of the President* [142], for example, the court rejected printouts of e-mail as evidence. The court reasoned that "the printed version of contained less

---

[138] *See* FRE 1006
[139] Alan Davison, 'Retaining Electronic Mail for Evidentiary Purposes' visited 23 March, 2002 at <http://www.uq.edu.au/~laadvaid/cyberlaw/july1999.html>
[140] (1987) 164 CLR 180, 186
[141] *Ibid.*
[142] 810 F Supp (1993)

information than the electronic version."[143] There was no information for example, about the transmitted date, the received date, detailed list of recipients and there was no linkages of sent messages and replies received. The court seems to rely on the originality and accuracy of the "original" which is merely in the electronic version. This could be a danger associated with computer related cases that proponents would need to offer courts both electronic and printed versions. It would be a heavy burden for businesses to retain huge amount of e-mails for potential evidence. Certain solutions should be recommended such as abolishing the secondary evidence for electronic records by amendment of the law of evidence and clarifying the term "original" including computer printouts.[144]

VI Electronic Record Risk Management

6.1 Establishing Electronic Media Use Policies

A. Retention and Destruction of Electronic Records Policy

Unlike, paper documents, electronic documents seem to be space saving and convenient for storage. However, it is not a good idea to save everything as useless corporate documents could damage corporations in litigation. An effective and comprehensive policy of electronic records' retention and destruction should be established by cooperation of legal counsels, administrative managers and IT officers.

A cost-benefit analysis in respect of retaining electronic records is required to ensure that certain records will be completely destroyed after a certain period of time has elapsed.[145] The document retention policy should include all copies of electronic records for example, archival e-mail, backups of hard drives and networks files.

Non-essential information should be periodically purged. The policy, however, should avoid selective purging of information since the selective destruction of information

---

[143] *Ibid.* n 139.
[144] *Ibid.*
[145] Adam I. Ohen and David J. Lender, 'Electronic Discovery Practice Guidelines' visited 26 June, 2002 at<http://www.weil.com/weil/EDPGWHOLE.pdf>

can seem to be a suspicious activity and may be challenged in litigation.[146] The policy must be up to the standard of general business and industry practice.

Document management systems should be able to perform the following features. They should extract or filter unwanted or out-of-date messages from the computer server. Archived messages including 1) message matadata; 2) message body and 3) attachments should be indexed in order to be searchable, retrievable, and accessible in both summary forms and full text forms.[147] It is also necessary that the document management system segregate privilege files such as lawyer-client e-mail, trade secrets and that patent of businesses be kept in a separated section in order to prevent unnecessary discovery.[148]

B. E-Mail Use Policy

E-mail communication has become a common tool for exchanging information. The growth of e-mail use has been fostered by industry analysts so that by 2005 up to 35 billion e-mails would be sent daily.[149] The widespread use of e-mail results from its ease, cheapness, convenience and speed; therefore, people employ e-mail for facilitating their businesses and personal activities. In electronic discovery, e-mail becomes the prime target of lawyers pursuing corporation cases for two reasons: 1) employees recklessly send conversation-like messages containing gossip, personal opinions and even a company's secrets to colleagues or friends outside the corporation; and 2) e-mail is easily discoverable once it has been recorded.[150] The mixing of work and private use of e-mail by employees can create serious problems

---

[146] *Ibid.*

[147] Ferris Research, 'Electronic Message Archiving' visited 25 June, 2002 at <http://www.mimesweeper.com/download/collateral/pdfs/whitepapers/archiving.pdf>

[148] James H. A. Pooley and David M. Shaw, 'Finding Out What's There: Techincal and Legal Aspects of Discovery', (1995) 4 *Texas Intellectual Property Law Journal* 57.

[149] Susan L. Cisco and Patricia K. Galloway, 'Managing E-mail Records: The State of the Art', visited 26 June, 2002 at <http://www.armavancourver.org/Proceedings/T32%20Susan%20Cisco.PDF>

[150] *Ibid.*

for their employers if corporation related litigation for example, sexual harassment, product liability or even anti trust cases takes place, and internal employees' e-mail may be requested as potential evidence by opposing lawyers. According to Pricewaterhouse Cooper's survey in the "Digital Discovery", e-mails (48 per cent) were the most requested electronic information in litigation, followed by company financial records (26.1 per cent).[151] Thus, an effective and comprehensive e-mail use policy is required in workplaces before litigation occurs.

An e-mail system should automatically purge all historic e-mail (e.g., every 30 days or 60 days) depending upon business needs.[152] Corporate records or administrative departments should ensure the erasure of out unwanted hidden information on hard drives at the time set pursuant to the policy. Huge discovery burdens in litigation could arise from the retention of unnecessary copies of e-mails on backup tapes. One good example, showing how a corporation which failed to have an effective e-mail policy proved to be costly to the corporation in litigation was that of *Re Brand Name Prescription Drugs Antitrust Litigation.*[153] Ciba-Geigy, a major of pharmaceuticals, was requested to search 30 million of its internal employees' e-mails on backup tapes to produce evidence. Ciba-Geigy requested the court to shift its production cost of about $60,000 to the plaintiff. The court, however, held that Ciba-Geigy also benefited from the production of e-mail; thus, it had to bear its own cost. Ciba-Geigy commented that it had to develop a customized application program to search the backup tapes this was the cause of the cost. If such messages had been archived in a searchable format, the cost would have been minimal.[154]

---

[151] PricewaterhouseCoopers and The American Bar Association, 'Survey: Digital Discovery and its Important on the Practice Litigation' visited 18 June, 2002 at <http://www.pwcglobal.com/extweb/ncsurves.nsf/0cc1191c627d157d852565060…>

[152] Adam I. Ohen and David J. Lender, 'Electronic Discovery Practice Guidelines' visited 26 June, 2002 at<http://www.weil.com/weil/EDPGWHOLE.pdf>

[153] 1995 WL 360526 (N.D. III)

[154] *Ibid.* n 147.

An e-mail policy should require employees to separate official and personal e-mail.[155] Distinguishing between e-mail could reduce the risk that employees personal e-mail could be used against employers or corporations in a lawsuit.

Moreover, sensitive or confidential corporate information should be encrypted before being sent via e-mail. However, the encryption of e-mail might cause difficulty in management and access since it needs to be decoded into readable forms. One commentator noted that "if you're trying to keep your information secret, most companies feel that having a secure network, rather than an encryption program, is more effective."[156] The use of encryption e-mail to protect privacy and security remains controversial.

Importantly, corporations should inform their employees about their e-mail policy. Employees may be required to sign off on the policy. The following provisions should be indicated in the e-mail policy: 1) that the employee has received a copy of the policy; 2) the employee understands the policy and has been given an opportunity to ask for an explanation of the policy; 3) the employee understands that he or she has no reasonable expectation of privacy regarding communications transmitted or received using employer-provided technology; and the employee's signature indicates consent by the employer to any surveillance or monitoring the company deems appropriate for business reasons.[157]

6.2 Educating Employees Regarding the Use of IT and its Legal Risk

All employees should be educated that e-mail could be used as evidence against them as well as against corporations in courts. In particular, when the company has been served with notice to preserve relevant documents for litigation, employees should be

---

[155] *Ibid.* n 145.

[156] Wendy R. Leibowitz, 'E-Document Management Guide' (2002) Vol.2 No. 6 *Digital Discovery & e-Evidence*.

[157] Susan C. Sears, 'Electronic Discovery in Litigation-Issue Highlights' visited 26 June, 2002 at <http://www.kybar.org/PDF_files/KLU_2001_materials/Electronic_Discovery.pdf>

notified immediacy to cease deleting any electronic records including e-mails and backups such records before wiping them. They should be educated that "deleting" or "purging" e-mail or other electronic messages does not mean destruction of such information forever.[158] Such electronic information, thus, can be discoverable and return to haunt or to embarrass authors if e-mail or electronic records contain confidential, offensive or derogatory contents once they have been read by a stranger.[159] Thus, employees must be careful about what they communicate via e-mail, at least undertaking the legal risks associated with the use of IT tools, and also that they have obligations to comply with the policy.

6.3 Reviewing and Monitoring Policy Implementation

Once the policy above is in force, administrative managers should monitor the effectiveness of such a policy and review that it is appropriately implements by all departments. It would be too late to learn after litigation begins that information has been destroyed, that was not "deleted" according to the destruction policy, or that it should have been preserved.[160]

Conclusion

Not only has technology changed the manner of business practices but it has also affected legal practice. More and more evidence will be in an electronic form. Some lawyers even consider such electronic evidence as their "gold mine" for discovery. Other lawyers may disagree with this opinion since electronic discovery can be a land mine of excessive costly discovery. The cost of electronic discovery is not only the important issue that most litigants are concerned about. Clients are also afraid that their disputes would not be properly handled by traditional legal practitioners. Technological knowledge, therefore, should be acquired sufficiently by lawyers and

---

158 *Ibid.*

159 Betty Ann Olmsted, 'Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delte' 63 *Defense Counsel Journal* 523.

160 *Ibid.* n 145.

judges in order to deal with this cutting edge evidence properly without, incurring unnecessary cost in electronic discovery processes.

In particular, lawyers should be aware that legal obstacles arising from existing law may not be appropriate to apply to electronic discovery. In the digital age, lawyers should be ready cooperate with IT people in order to help them in the preventative process before litigation, e.g., drafting electronic document management policy or e-mail use policy as well as assisting them during litigation, e.g., recovering electronic data. In addition, whether or not lawyers would be able to discover potential electronic evidence or to use electronic data effectively to support their cases would be dependent on how well lawyers can educate courts to understand the distinct nature of electronic evidence. Many issues emerging electronic discovery will be the challenging task for legal practitioners in the computer era.

Bibliography

Books

Abu Baker Munir, *Cyber Law Policies and Challenges*, Butterworht Asia, Kuala Lumpur, 1999.

Andrew Ligertwood, *Australian Evidence: Cases and Materials*, Butterworths, Sydney, 1995.

Chris Reed (ed.), *Computer Law*, (2nd, eds.), Blackstone Press Ltd., London, 1993.

Christina McAlhone, *Nutshells Evidence in a Nutshell,* Sweet & Maxwell, London, 1996.

D. P. Van Der Merwe, *Computers and the Law*, Jata & Co. Ltd., Cape Town, 1986.

Gordon Hughes, *Essays on Computer Law*, Longman Professional, Melbourne, 1999.

Jane K. Winn and Benjamin Wright, *Law of Electronic Commerce*, (4th, eds.), Aspen Law & Business, New York, 2002.

Jonathan Rosenoer, *Cyber Law: The Law of the Internet*, Springer, CA, 1997.

Olujoke Akindemowo, *Information Technology Law in Australia*, LBC, Sydney, 1999.

P.J. Blazey Ayoub et al., *Concise: Evidence Law*, The Federation Press, Sydney, 1996.

Tracey Aquino, *Essential Evidence*, Cavandish Publish, London, 1997.

Law Journals

Andrew Jablon, ' "God Mail": Authentication and Admissibility of Electronic Mail in Federal Courts' (1997) 34 *American Criminal Law Review* 1387.

Anthony J. Dreyer, 'When the Postman Beeps Twice: the Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence' (1996) 64 *Fordham Law Review* 2285.

Betty Ann Olmsted, 'Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete' (1996) 63 *Defense Counsel Journal* 523.

Bruce Rubenstein, 'Electronic Discovery Costs Are Leveraging Settlements' (1997) 7 *Corporate Legal Times.*

Carey Sirota Meyer and Kari L. Wraspir, 'E-Discovery: Preparing Clients for (And Protecting Them Against) Discovery in the Electronic Information Age' (2000) *William Mitchell College of Law Journal.*

Christine Sgarlata Chung and David J. Byer, 'The Electronic Trail: Evidence Obstacles to Discovery and Admission of Electronic Evidence' (1998) 4 *Boston University Journal of Science & Technology Law* 5.

Christopher V. Cotton, 'Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era' (1999) *The Journal of Corporation Law.*

Corinne L. Giacobbe, 'Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronic of Electronically Stored Data' (2000) 57 *Washington and Lee Law Review* 257.

Debra S. Katz and Alan R. Kabat, 'Electronic Discovery in Employment Discrimination Cases' (1998) 34 *Trial* 28.

Dein Murphy, 'The Discovery of Electronic Data in Litigation: What Practitioners and Their Clients Need To Know' (2001) 27 *William Mitchell College of Law* 1825.

Digital Discovery & e-Evidence, Vol. 2 No. 6, June, 2002

Eric Goldman and Max P. Ochoa, 'New E-Mail Laws Create New Legal Issues' (1999) *Cyber Lawyer.*

Glasser LegalWorks, 'The Best Practices for Seizing Electronic Evidence' (2000) *Cyberspace Lawyer.*

James E. Carbine and Lynn McLain, 'Proposed Model Rules Governing the Admissibility of Computer-Generated Evidence'(1999) 15 *Santa Clara Computer and High Technology Law Journal.*

James H.A. Pooley and David M. Shaw, 'Finding Out What's There: Technical and Legal Aspects of Discovery' (1995) 4 *Texas Intellectual Property Law Journal* 57.

Jay E. Grenig, 'Electronic Discovery: Marking Your Opponent's Computer a Vital Part of Your Legal Team' (1997) *American Journal of Trial Advocacy.*

Joan E. Feldman and Rodger I. Kohn, 'Collecting Computer-Based Evidence' visited 27 January, 2002 at<http://www6.law.com/ny/tech/012698t6.html>

John Jessen, 'Special Issues Involving Electronic Discovery' (2000) 9 *Kan. J.L. & Pub. Pol'y* 425, 2000.

Kimberly D. Richard, 'Electronic Evidence: To Produce or Not to Produce, That Is The Question' (1999) 21 *Whittier Law Review* 453.

Kimberly D. Richard, 'Electronic Evidence: To Produce or Not to Produce, that is the Question' 21 *Whittier Law Review* 463.

Lisa A. Dolak, 'Patents without Papers: Proving a Date of Invention with Electronic Evidence' (1999) 36 *Houston Law Review* 471.

Mark D. Robins, 'Computers and The Discovery of Evidence—A New Dimension to Civil Procedure' (1999) 17 *John Marshall Journal of Computer and Information Law* 411.

Martin H. Redish, 'Electronic Discovery and the Litigation Matrix'(2001) 51 *Duck Law Journal* 561.

Patrick R. Grady, 'Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give Up More Than Necessary' (1996) *John Marshall Journal of Computer and Information Law.*

Peter v. Lacouture, 'Discovery and The Use of Computer-Based Information in Litigation' (1996) *Rhode Island Bar Journal.*

Pike & Fischer, Inc., Digital Discovery & e-Evidence, Vol. 1, No. 12

Randell C. Ogg, 'Aggressive Pursuit of Spoliation Reaps Rewards' (1997) *Product Liability Law and Strategy*.

Robert L. Paddock, 'Utilizing E-Mail As Business Records Under The Texas Rules of Evidence' (2000) 19 *Review of Litigation* 61.

Steve Bauer et al., 'Lawyers Online: Discovery, Privilege, and the Prudent Practitioner' (1997) 3 *Boston University of Science and Technology Law* 5.

Susan W. Brenner and Barara A. Frederiksen, 'Computer Searches and Seizures: Some Unresolved Issue' (2002) 8 *Michigan Telecommunications and Technology Law Review* 39.

Timothy Q. Delaney, 'E-mail Discovery: The Duties, Danger and Expense' (1999) *The Federal Bar Association.*

Walter D. Alley, 'Electronic Discovery Tool for Litigators' visited 18 March, 2002 at<http://www.foisinc.com/wp-product.html>

William DeCoste, 'The Discoverability and Admissibility of E-Mail' (2000) 2 *Vanderbilt Journal of Entertainment Law & Practice* 79.

Internet Resources

Adam I. Ohen and David J. Lender, 'Electronic Discovery Practice Guidelines' visited 26 June, 2002 at <http://www.weil.com/well/EDPGWHOLE.pdf>

Agec, 'Issues Paper: Evidence and the Internet' visited 20 March, 2002 at<http://www.agec.gov.ac>

Alan Davidson, 'Retaining Electronic Mail for Evidentiary Purposes' visited 23 March, 2002 at <http://www.up.edu.au/~laadavid/cyberlaw/july1999.html>

Alan Gahtan, 'Discovery of Electronic Evidence' visited 27 January, 2002 at<http://gahtan.com/alan/expert/C17A.HTM>

Alex Salkever, 'Hot on the E-Trail of Evidence at Enron' visited 29 January, 2003 at <http://www.businessweek.com/bwdaily/dnflash/jan2002/nf..>

Alexi Maltas, 'Cost: Analysis' visited 18 March, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/costanalysis.html>

American Bar Association, 'Electronic Evidence Working Group Tool Kit' visited 18 March, 2002 at <http://www.abanet.org/buslaw/cyber/ecommerce/toolkit.html>

American Bar Association, 'The Need for Reform of the Uniform Rules of Evidence to Accommodate the Admission into Evidence of Electronic Records' visited 03 June, 2002 at<http://www.abanet.org/buslaw/cyber/archive/reform.html>

Andy Johnson Laird, 'Discovery in Computer Software Patent Litigation' visited 19 January, 2002 at <http://www.fclr.org/articles/1998fedctslrev1(main).htm>

Andy Johnson-Laird and Barbrara A. Frederiksen, 'Smoking Guns and Spinning Disks Redux' visited 24 March, 2002 at<http://www.jli.com/papers/sgasd.htm>

Barbara A. Caulfield and Zuzana Svihra, 'Requiring the Losing Party to Party to Pay for the Costs of Digital Discovery' visited 26 March, 2002 at<http://www.fiosinc.com/wp-losing.html>

Ben Fitzpatrick, 'Computers, Hearsay, and the Status of Extradition Proceedings' visited 25 January, 2002 at<http://webjcli.ncl.ac.uk/1998/issue1/fitzpatrick1.html>

Brendan Scott, 'Electronic Document Management-Some Traps for Young Players' visited 12 June, 2002 at<http://www.gtlaw.com.au/t/publications/default.jsp?pubid=275>

Brian Robinson, 'Think You Have a Handle on Your E-mail? Think Again' visited 18 March, 2002 at<http://www.fcw.com/print.asp>

C. Bryson Hull, 'Andersen Guilty in Obstruction Trial' visited 17 June, 2002 at <http://news.findlaw.com/scripts/printer_friendly.pl?page=/…>

CERT Coordination Center, 'How the FBI Investigates Computer Crime' visited 27 June, 2002 at <http://www.cert.org/tech_tips/FBI_investigates_crime.htm…>

Charles Nesson, 'Introduction to Digital Discovery' visited 18 March, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/nesson.html>

Chris Reed, 'The Admissibility and Authentication of Computer Evidence- A Confusion of Issues' visited 25 January, 2002 at <http://www.bileta.ac.uk/90papers/reed.html>

Daniel Shap, 'Search and Seizure of Canadian Computer Environment' visited 27 May, 2002 at<http://www.catalaw.com/logic/docs/ds-srch.htm>

David A. Wallace, 'Recordkeeping and Electronic Mail Policy: the State of Thought and the State of the Practice' visited 18 January, 2002 at <http://www.rbaryy.com/dwallace.html>

David H. Schultz, 'Beyond Fingerprints: Recovery of Electronic Evidence' visited 29 May, 2002 at<http://www.ontrack.com>

Deborah Schepers, 'The Power And the Dangers of E-Discovery' visited 20 March, 2002 at <http://www.legalmediagroup.com/techlawlive/includes/print…>

DuPont Legal Model, 'DuPont Legal Model' visited 26 June, 2002 at <http://www.duponglegalmode.com/default.asp?p=1>

Ferris Research, 'Electronic Message Archiving' visited 25 June, 2002 at <http://www.mimesweeper.com/download/collteral/pdfs/whitepapers/archiving.pdf>

George J. Socho, 'Once You Have the Evidence-Then What?' visited 18 March, 2002 at <http://www.fiosinc.com/wp-once.html>

George Socha, 'Electronic Discovery-Or, the Byte that Bit' visited 28 June, 2002 at<http://www.llrx.com/features/byte.htm>

Gillbert & Tobin, 'Legal Risk and Admissibility of Electronic Documents and Records' visited 12 June, 2002 at<http://www.gtlaw.com.au/t/publications/default.jsp?..>

Guerts, 'Evidence on the Internet: Where do you find it?' visited 21 June, 2002 at<http://www.austlii.edu.au/au/other/CyberLRes/2001/28/>

Ian C. Ballon, 'Spoliation of E-Mail Evidence: Proposed Intranet Policies and a Framework for Analysis' visited 24 March, 2002 at <http://library.lp.findlaw.com/scrips/getfile.pl?FILE=legpub/glass/glass000020>

Ian Springsteel, 'Are You Sure You Want to Save That?' visited 23 March, 2002 at <http://www.cio.com/archive/091501_content.htm.?printversion=yes>

Indictment: United States of America v Arthur Andersen, LLP. , visited 18 March, 2002 at<http:/.news.findlaw.com/scripts/printer_friendly.pl?page=..>

J. Roger Tamer, 'Preparing for Electronic Discovery' visited 26 July, 2002 at <http://www6.law.com/ny/tech/012599t7.html>

James H.A. Pooley and David M. Shaw, 'The Emerging Law of Computer Networks' visited, 2002 at<http://www.utexas.edu/law/journals/tiplj/vol4iss1/pooley.htm>

Jeff Lendino and Jennifer Zeller, 'The Coming of Age of Electronic Discovery' visited 29 May, 2002 at<http://www.ontrack.com>

Jeff Lendino, 'Practical Guidance for Conducting Electronic Discovery' visited 29 May, 2002 at<http://www.ontrack.com>

Josh Solomon, 'Process: Analysis' visited 18 March, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/process/processanalysis.html>

Kathy Sinclair, 'Australian Law and Digital Records' visited 26 June, 2002 at <http://vers.imagineering.net.au/site-ver2/erecord_library/Documents%20..>

Kenneth J. Withers, 'Computer-Based Disclosure and Discovery in Civil Litigation' visited 18 January, 2002 at<http://www.bileta.ac.uk/01papers/withers.html>

Kenneth J. Withers, 'Federal Courts Law Review' visited 18 January, 2002 at <http://www.fclr.org/articles/2000fedctslrev2(main).htm>

Kristen Hays, 'Enron Answer Criticism of Lockdown' visited 14 December, 2002 at <http://news.findlaw.com/scripts/printer_friendly.pl?page=/ap_stories/f/13..>

Kristin M. Nimsger and Michele C.S. Lange, 'Examining the Data' visited29 May, 2002 at<http://www.ontrack.com>

Kurt Eichenwald, 'A Victory, and A Signal' visited 16 June, 2002 at<http://www.nytimes.com/2002/06/16/business/16LEGA.h…>

Kurt Eichenwald, 'Andersen Guilty of Shedding Files in Enron Scandal' visited 16 June, 2002 at<http://www.nytimes.com/2002/06/16/business/16AUDI.ht..>

Larry G. Johnson and Tim Stenvens, 'Due Diligence in the Digital Age' visited 26 March, 2002 at <http://www.fiosinc.com/wp-due.html>

Lawrence Aragon, 'E-mail Is Not Beyond the Law' visited 24 March, 2002 at<http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/aragon.html>

Matt Delmero, 'Spoliation: Analysis' visited 19 March, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/spolicaition/spoliationanalysis.html>

Michael Bartlett, 'Companies Must Prepare for E-Discovery' visited 28 May, 2002 at<http://www.newsbytes.com/cgi-bin/udt/im.display/printable?…>

Michael R. Overly, 'The Admissibility of Electronic Documents' visited 26 June, 2002 at<http://www.forensics.com/resources/admiss.htm>

National Archives of Australia, 'Email is a record!' visited 23 March, 2002 at<http://www.naa.gov.au/recordkeeping/advice.html>

National Archives of Australia, 'Managing Electronic Messages as Records' visited 23 March, 2002 at<http://www.naa.gov.au/reocordkeeping/er/elec_messages/guidelines.html#emai>

National Archives of Australia, 'Managing Electronic Records' visited 23 March, 2002 at<http://www.naa.gov.au/recordkeeping/er/manage_er/intro.htm>

National Archives of Australia, 'Records in Evidence' visited 23 March, 2002 at <http://www.naa.gov.au/recordkeeping/overview/evidence/records_in_evidence.hm>

National Archives of Australia, 'The Impact of the Evidence Act on Commonwealth Recordkeeping' visited 23 March, 2002 at<http://www.naa.gov.au/recordkeeping/overview/evidence/records.htm>

Orin S. Kerr, 'Computer Records and the Federal Rules of Evidence' visited 03 March, 2002 at<http://www.cybercrime.gov/usamarch2001_4.htm>

Pricewaterhouse Coopers and ABA, ' Survey: Digital Discovery and Its Importance on the Practice of Litigation' visited 23 March, 2002 at<http://www.pwcglobal.com/extweb/ncsurves.nsf..>

Queensland Law Reform Commission, 'The Receipt of Evidence By Queensland Courts: Electronic Records' visited 01 June, 2002 at<http://www.qlrc.qld.gov.au>

Rehman Technology Services, Inc., 'Electronic Discovery Case Law' visited 27 January, 2002 at <http://www.surveil.com/case_law.htm>

Richard E. Barry, 'Recordmaking Systems that Aren't Sure IT Doesn't Get Blindsided' visited 26 June, 2002 at<http://www.rbarry.com>

Shira A. Scheindlin and Jeffery Rabkin, 'Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up To the Task' visited 24 March, 2002 at<http://www.bc.edu/bc_org/avp/law/lawsch/journals/bclawr/41_2/03_FMS.htm>

Solomon E. Salako, 'Computer Printout as Admissible Evidence: A Critical Legal Study of Section 24 of the Criminal Justice Act 1988' at <http://www.bileta.ac.uk/90papers/salako.html>

Steve White, 'Comment: Discovery of Electronic Documents' visited 15 June, 2002 at <http://wwwlaw.murdoch.edu.au/dtlj/2000/vol12_1;white.pdf>

Susan C. Sears, 'Electronic Discovery in Litigation-Issue Highlights' visited 26 June, 2002 at<http://www.kybar.org/PDF_files/KLU_2001_materials/Electronic_Discovery.pd

Susan L. Cisco et al., 'Managing E-mail Records: the State of the Art' visited 26 June, 2003 at <http://www.armavancouver.org/Proceedings/T32%20Susan%20Cisco.PDF>

The Australian Law Reform Commission, 'Costs Shifting-Who Pays for Litigation' visited 21 June, 2002 at<http://www.austlii.edu.au/au/other/alrc/publicaiton/report…>

Tom Brown, 'Preservation:Analysis' visited 18 March, 2002 at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservationanalysis.html>

U.S. Department of the Treasury, 'Best Practices for Seizing Electronic Evidence' visited 23 March, 2002 at<http://www.secrestservice.gov/electronic_evidence.shtml>

US Department of Justice, 'Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigation' visited 18 February, 2002.

William Birnbauer, '$7,000 Win to Smoker After Evidence Destroyed' visited 13 April, 2002 at<http://www.theage.com.au/egi-bin/common/printArticle.pl?path=/articles/2002/..>

William Birnbauer, 'The Smoking Gun' visited 13 April, 2002 at<http://www.theage.com.au/cgi-bin/common/printArticle.pl?path=/articles/2002>

ZDNet, 'When e-mail comes back to haunt you' visited 26 June, 2002 at <http://www.zdnet.com.au/printfrinedly?AT=200..>

Related Laws

Australian Laws and Regulations:

Federal Court of Australia: No. 17. Guidelines for the use of information technology in litigation in any civil matter, visited 03 June, 2002 at<http://www.fedcourt.gov.au/practice_notes_cj17.htm>

Supreme Court of Victoria: Practice No.3 of 1999 Guidelines for the use of technology in litigation in any civil matter, visited 03 June, 2002 at <http://www.supremecourt.vic.gov.au/pns/99pn3.htm>

The Evidence Act 1995 (Cth)

The U.S. Laws and Regulations:

- **Federal Rules of Civil Procedure Rule 26(b) Discovery Scope and Limits**
- Rule 30(b)
- Rule 34 Production of Documents and Things and Entry upon Land for Inspection and Other Purposes
- **Federal Rules of Evidence**
- Article VIII, Hearsay
- Article IX, Authentication and Identification
- Article X, Contents, of Writings, Recordings and Photographs
- **Uniforms Laws**
- Business Records as Evidence Act
- Uniform Preservation of Private Business Record Act
- Uniform Rules of Evidence