Discovery in the Digital Age:
A Primer on e-Discovery and Computer Forensics

Presented by:

Rodney B. Hastings, Esq. (EnCE)
Deputy Disciplinary Counsel
Office of the Disciplinary Counsel
Louisiana Attorney Disciplinary Board
4000 S. Sherwood Forest Boulevard, Suite 607
Baton Rogue, Louisiana 70816
(225) 293-3900 or (800) 326-8022
Email: rodneyh@ladb.org

Discovery in the Digital Age: A Primer on e-Discovery and Computer Forensics

Presented by:

Rodney B. Hastings, Esq. (EnCE)
Deputy Disciplinary Counsel
Office of the Disciplinary Counsel
Louisiana Attorney Disciplinary Board
4000 S. Sherwood Forest Boulevard, Suite 607
Baton Rogue, Louisiana 70816
(225) 293-3900 or (800) 326-8022
Email: rodneyh@ladb.org

Introduction

The vast majority of documents produced today are in electronic, or digital, form. Electronic documents consist of any information created, stored, or utilized with computer technology. Electronic documents include business applications, such as word processing, databases, and spreadsheets; Internet application, such as e-mail and the World Wide Web; devices attached to or peripheral to computers, such as printers and fax machines; web-enabled portable devices and cell phones; and media used to store computer data, such as disks, tapes, removable drives, and CDs. Researchers at Berkeley University estimate that between the years 2000 and 2003 the amount of original data stored annually on magnetic media doubled. This digital information is handled differently then the conventional paper documents most of us are accustomed to dealing with on a routine basis. Key areas of divergence include volume, accessibility, and custodianship.

Volume

In a study conducted at Berkeley University in 2000, researchers estimated that almost 800 megabytes of recorded information is produced per person each year. It would take about 30 feet of books to store the equivalent information on paper. It is important to note that not all of this recorded information consists of original information. In fact, the primary cause of the volume associated with electronically stored information is replication. When electronic data is moved from one point to another, such as sending an e-mail or copying a Word document, the information is not physical moved from Point "A" to Point "B". Instead, the information is replicated. Along the way, particularly with e-mail messages, the information is likely to be replicated at various points. For instance, when you send an e-mail message out, a copy of the e-mail is usually saved on your hard drive and the hard drive of the recipient. Additionally, the e-mail message will be replicated on any network e-mail servers located along its transmission route, as well as any backup media associated with the servers or the hard drives.

A second contributing factor to the increasing volume of electronic data is societal. Today, we are much more comfortable with the idea of working with computers and making it our primary means of communication. We have grown equally as comfortable with other means of electronic communications, such as instant messaging, text messaging, Voice Over Internet Protocol (VoIP), and web-based meeting technology. Each use of these devices generates its own digital record. Oftentimes, this digital record is subject to the same replication as the e-mail messages we send.

The durability of electronic information also plays a role in the burgeoning growth of electronic data. As most of you have learned by now, deleting an electronic file by hitting the "Delete" key does not truly delete, or destroy, the file. Hitting the "Delete" key renames the file and eliminates any reference to it in the computer operating system's active files. Then, the operating system is notified that the disk space containing the "deleted" file is available for re-use when needed. Hitting the "Delete" key also places a renamed copy – not the original – of the file into the "Recycle Bin". This copy is "deleted" when the "Recycle Bin" is emptied.

So, in effect, deleting a file does not remove the file. The file may be completely or partially overwritten at some point in the future. Any portion of the file not overwritten can be recovered using various computer forensics methodologies. It is also important to remember that "deletion" of one file does not result in the "deletion" of any copies or alternate versions of the file existing in other locations, either on the same hard drive or elsewhere.

The creation of an electronic file also generates the creation of ancillary information necessary for the proper function of the operating system and software. This information is generally referred to as "metadata". Metadata may include information such as the date of creation, author, source, or history.

Furthermore, word processing programs generally save each version of an electronic file, and operating system software needs to generate its own information to manage input and output devices. All of this ancillary information contributes to the increasing volume of electronic data.

Other factors playing a significant role in the increase of electronic data include legacy data and backup media. Legacy data is electronically stored information associated with out-dated operating systems or application software. Backup media refers to the practice of replicating electronically stored information in wholesale fashion at regular intervals for the purpose of restoring the information in wholesale fashion in the event of catastrophic computer system failure.

Accessibility

Accessible information is electronically-stored information that is easily retrievable in the ordinary course of business without undue cost and burden. Examples of information that may not be reasonably accessible in all instances include data stored on back-up tapes or legacy systems; material that has been deleted; and residual data. Unlike paper-based information, electronically-stored information must be rendered intelligible by the use of technology.

Custodianship

When you are dealing with paper documents custodianship of records and correspondence is generally clear. Custodianship of electronically-stored information is less clear. In general, custodianship of electronically-stored information may exist on several levels.

People who work or create the data directly are the primary custodians. Systems analysts and business process engineers are the custodians of the information management system, but may actually know little about the specific content of the information. The information technology staff may serve as the physical custodian of the electronically-stored information. Again, they may have little knowledge of the specific content of the information. Others, such as internet service providers or other service providers, represent another level of custodianship.

e-discovery

Electronic discovery (or e-discovery) refers to any process in which electronic data is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network. Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery.

In the process of e-discovery, data of all types can serve as evidence. This can include text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites, and computer programs. Even malware such as viruses, Trojans, and spyware can be secured and investigated. E-mail can be an especially valuable source of evidence in civil or criminal litigation.

It is estimated the e-discovery technology spending will grow from $1.4 billion in 2006 to more than $4.8 billion in 2011. A comprehensive e-discovery plan requires the integration of legal analysis, records management and information technology.

Federal Rules of Civil Procedure

Rule 34 of the Federal Rules of Civil Procedure defines the term "document" to include information in any tangible format. In 1970, Rule 34 was modified to encompass "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably useable form." The recently amended Rule 34 now provides:

> **Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes**
> **(a) Scope.** Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained – translated, if necessary, by the respondent into reasonably useable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, with the scope of Rule 26(b).

Other major revisions address the following areas:

(1) **Early attention to electronic discovery.**

a. Rules 16 and 26 are amended to provide the court early notice of potential electronic discovery issues. Specific changes include:

b. The Rule 16(b) scheduling order must include "provisions for disclosure or discovery of electronically stored information" and "any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production."

c. Rule 26(a) requires that the parties' initial disclosures include descriptions by category and location of all "electronically stored information," as opposed to the former rule's use of "data compilations."

d. Rule 26(f) requires the parties, as part of their mandatory discovery conference, "to discuss any issues relating to preserving discoverable information," and, in particular: "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."

i. The committee note says that the issues to be addressed during the conference will vary from case to case and will "depend on the nature and extent of the contemplated discovery and of the parties' information systems."

ii. Other changes to Rule 26(f) require the parties to discuss:

1. The form in which electronically stored information is to be produced.
2. Any issues regarding preservation of discoverable information.
3. Any issues relating to assertions of privilege or of protection as trial-preparation materials, including whether the parties can agree on procedures for asserting claims of privilege or protection after production.

(2) Undue burden posed by electronic discovery.

a. Rule 26(b)(2) authorizes a party to seek protection from electronic discovery based on undue burden or cost.

b. The new rule adds the following subparagraph B: "A party need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery."

c. The committee note adds: "[S]ome sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible."

(3) Privilege and work product protection.

a. The voluminous scope of electronic discovery creates a risk of inadvertent transmission of privileged and protected materials. Rule 26(b)(5) provides a procedure for addressing this.
b. The amendments add a new subparagraph B: "If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information after being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved."

(4) Interrogatories and production requests.

a. The amendments make several changes to Rules 33 and 34.
b. Rule 33(d) is amended to include electronically stored information as among the types of business records that may be produced in lieu of answers to interrogatories.
c. Rule 34 is amended to allow for production of "documents, electronically stored information, and things."
d. A party may request "to inspect, copy, test, or sample any designated documents or electronically stored information – including writings, drawings, graphs, charges, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained – translated, if necessary, by the respondent into reasonably usable form."
e. Rule 34(b) says: "The request may specify the form or forms in which electronically stored information is to be produced."
f. Rule 34(b) permits the responding party to object to the requested form, explaining its grounds. If it objects, or if the request specified no form, the responding party must state the form it intends to use.
g. Rule 34(b)(ii) says that if the request does not state a form for producing the information, the responding party must produce it "in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."
h. Rule 34(b)(iii) says that a party need not produce the same electronically stored information in more than one form.

(5) Safe harbor from sanctions.

a. Rule 37(f) provides a safe harbor for "routine, good-faith" loss of data.
b. Rule 37(b) provides: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

(6) Subpoenas.

a. For parties issuing subpoenas:
    i. Rule 45(a)(1)(C) now authorizes the subpoena to include electronically stored information.
    ii. Rule 45(a)(1)(D) specifies that the subpoena "may specify the form or forms in which electronically stored information is to be produced."

b. For parties responding to a subpoena:
    i. Rule 45(d)(1)(B) provides that if the subpoena does not specify the form for production, the respondent "must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable."
    ii. Rule 45(d)(1)(C) says that the respondent "need not produce the same electronically stored information in more than one form."
    iii. Rule 45(d)(1)(D) says that the respondent need not provide information "from sources that the person identifies as not reasonably accessible because of undue burden or cost." Even if the respondent makes this showing, the court may still order discovery "if the requesting party shows good cause."
    iv. Rule 45(d)(2)(B) adds a procedure for addressing information that is claimed to be privileged or protected. It parallels the procedure under Rule 26(b)(5).

Preservation of Relevant Evidence

A party has a duty to preserve potentially relevant evidence. The responding party must determine the potential sources and locations of responsive information. The respondent party must, then, conduct a diligent search for responsive materials.

The duty to preserve relevant evidence may arise in pre-litigation, after service of the complaint, or once the discovery process has begun. Relevant evidence to be preserved includes what a litigant knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.

The consequences for failing to preserve relevant evidence include:

(1) Ethical – Conduct prejudicial to the administration of justice; engaging in conduct involving misrepresentation or fraud; unlawful obstruction or destruction of evidence.

(2) Sanctions – Monetary; exclusion of evidence; adverse inference jury instructions; dismissal or default judgment

(3) Criminal penalties (Federal)

Allocating Costs

For purposes of determining cost-shifting issues, the world of electronic information is divided into two distinct categories: (1) data kept in an accessible format; and (2) data that is relatively inaccessible. The usual rules of discovery, including that the responding party should pay the costs of producing responsive data, apply to electronic information falling into the first

category. In *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003), the U.S. District Court for the Southern District of New York devised the following approach to the cost-shifting analysis:

> Once a small sample of inaccessible data has been produced "in conducting the cost-shifting analysis the following factors should be considered, weighted more-or-less in the following order":
>
> (1) The extent to which the request is specifically tailored to discover relevant information;
> (2) The availability of such information from other sources;
> (3) The total cost of production, compared to the amount in controversy;
> (4) The total cost of production, compared to the resources available to each party;
> (5) The relative ability of each party to control costs and its incentive to do so;
> (6) The importance of the issues at stake in the litigation; and
> (7) The relative benefits to the parties of obtaining the information.

Requesting Electronic Information

How much time and effort you devote to seeking discovery of electronic information depends upon various factors, including the size of the case, the matters at issue, and the time and resources you have available for the case. In the initial stages of the case, you should consider what types of electronic information are likely to exist and are needed to prove the case. Before asking for the production of electronic information, such as back-up tapes and deleted files, weigh the costs against the potential benefits.

If you determine that electronic information is important to your case, promptly notify the opposing party of your intent to request it. A sample form spoliation letter is attached as Appendix A. Even though the duty to preserve evidence exists independently of a court order, you may want to also consider obtaining a preservation order from the trial court. In order to formulate your requests for electronic information you should consider expedited or early depositions of the opposing party's employees who are most knowledgeable about the opponent's information technology uses and systems.

When requesting electronic information you should avoid using general definitions. Be specific about what you are seeking. If you want e-mails, spreadsheets, or specific databases, then specify those items in your request.

Your earliest negotiations with counsel for the opposing party should include a discussion of the logistics of electronic discovery. Each side should be prepared to discuss whether they possess information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issues, and how to allocate costs. You should also try to obtain information concerning your opponent's computer system, including its functionality, breadth, scope and number of users.

Your course of action should include initially serving interrogatories, and then following up with a document request and/or a deposition notice accompanied by a list of requested

documents and data. Interrogatories can also be used to obtain preliminary information about the layout of an opponent's computer system.

In order to assess the adequacy of your opponent's electronic production it is suggested that at a deposition you ask the witness whether he or she:

(1) searched his or her computer and to delineate the types of information stored thereon;
(2) was instructed to preserve information, including electronic information;
(3) possesses floppy disks, zip disks, flash memory devices and/or CD-ROMs containing pertinent information;
(4) uses a laptop and/or other home computer for work purposes;
(5) the configuration of the deponent's computer or workstation (what it is used for and what information is saved to a storage device); and
(6) the identity of others who have retained and still retain the deponent's electronic information.

Appendix B contains sample electronic discovery interrogatories and requests for production.

Computer Forensics

Computer forensics, also called cyberforensics, is a specialized form of e-discovery in which an investigation is carried out on the contents of the hard drive of a specific computer. After physically isolating the computer, investigators make a digital copy of the hard drive. Then the original computer is locked in a secure facility to maintain its pristine condition. All investigation is done on the digital copy.

As previously noted, "deleted" does not necessarily mean the file cannot be accessed. Computer files that are deleted by the user are designated for deletion but remain on the system until they are overwritten randomly as the system needs the space. At any given time, a computer's hard drive may have "deleted" data that can be recovered. A digital copy of a hard drive or other digital media made using computer forensics software will pick up any deleted files or file fragments that remain. A digital copy of a drive made by transferring each file will not include deleted files or file fragments. Additionally, some imaging programs overwrite some of the deleted files, potentially destroying valuable evidence.

Case law does not provide a definite answer as to whether the obligation to search for and produce responsive electronic information requires a search for "deleted" files. There are cases in which a party successfully obtained access to his opponent's computer to search for deleted files. However, the tendency of the courts is to appoint a neutral computer forensics expert to copy hard drives and to attempt to recover deleted data. In cases where the neutral expert located evidence of spoliation by deletion of files the courts have been prone to impose sanctions, even in the absence of a preservation order. The courts also look askance at a party's failure to preserve back-up tapes.

Louisiana Law

C.C.P. Art. 1461. Production of documents and things; entry upon land; scope

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on his behalf, to inspect, copy, test, and sample any designated documents or electronically stored information, including writings, drawings, graphs, charts, photographs, phono-records, sound recordings, images, and other data or data compilations in any medium from which information can be obtained, translated, if necessary, by the respondent through detection and other devices into reasonably usable form, or except as provided in Article 1462(E), to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Articles 1422 through 1425 and which are in the possession, custody, or control of the party upon whom the request is served; or (2) except as provided in Article 1462(E), to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Articles 1422 through 1425.

La. Code of Evidence Art. 1003.1. Electronic duplicate

A duplicate may not be deemed inadmissible or excluded from evidence solely because it is in electronic form or is a reproduction of electronically imaged or stored records, documents, date, or other information.

In re Vioxx Products Liability Litigation, ____ F.Supp.2d _____, 2007 WL 2390877 (E.D. La.)

The emergence of the internet and electronic methods of communication present significant challenges for traditional discovery practices. These challenges are exacerbated in MDL proceedings and otherwise complex cases where, because of their vastness, no one counsel can be expected to keep up with everything that transpires. Discovery is often handled by a discovery committee in such cases, and trial preparation by a separate committee. This presents opportunities for disconnects.

With the ever-expanding use of, if not dependence on, e-mail technology, courts will increasingly be called upon to review electronic communications to determine whether they are protected by the attorney-client privilege. A primary challenge for the courts in this area is one of organization and administration. … Another challenge is created by the sheer volume of documents that must be reviewed in complex cases. The number of potentially relevant documents often reaches into the millions. It takes a legion of attorneys and paralegals to cull through the documents and recommend or decide whether each document is

> responsive to a request and should be produced, or whether it is instead non-responsive or privileged. In such a milieu, there is a strong bias in favor of non-production. Such circumstances also create opportunities for the attorney who concludes that delay is strategically desirable.
>
> When privilege is claimed on 30,000 documents, amounting to nearly 500,000 pages, as occurred in this case, the courts are severely taxed. When the task of review is shifted to outside experts, the costs mount. In the long run, such a situation is detrimental to the litigants, the courts, and our system of justice. Some acceptable solution must be devised, one which fully protects the rights of the litigants to claim privilege and at the same time is more feasible for the courts, less expensive for the parties, and less time consuming for everyone involved.

Id. at *21

Appendix A -- Form spoliation letter to opposing counsel

[date]

[address]

re: [matter (, case number)]

Dear: _____,

By this letter, you and your client{s} are hereby given notice not to destroy, conceal or alter any paper or electronic files and other data generated by and/or stored on your client's {clients'} computers and storage media (e.g., hard disks, floppy disks, backup tapes), or any other electronic data, such as voice mail. As you know, your client's {clients'} failure to comply with this notice can result in severe sanctions being imposed by the Court {and liability in tort} for spoliation of evidence or potential evidence.

Through discovery we expect to obtain from you a number of documents and things, including files stored on your client's {clients'} computers and your client's {clients'} computer storage media. {As part of our initial discovery efforts, you [are hereby served with/will soon receive] [initial/supplemental] interrogatories and requests for documents and things.}

In order to avoid spoliation, you will need to provide the data requested on the original media. Do not reuse any media to provide this data.

{Although [we may bring/have brought] a motion for an order preserving documents and things from destruction or alteration, your client's {clients'} obligation to preserve documents and things for discovery in this case arises in law and equity independently from any order on such motion.}

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond that which may be found in printed documents. Therefore, even where a paper copy exists, we [seek/will seek] all documents in their electronic form along with information about those documents contained on the media. We also [seek/will seek] paper printouts of only those documents that contain unique information after they were printed out (such as paper documents containing handwriting, signatures, marginalia, drawings, annotations, highlighting and redactions) along with any paper documents for which no corresponding electronic files exist.
Our discovery requests [ask/will ask] for certain data on the hard disks, floppy disks and backup media used in your client's {clients'} computers, some of which data are not readily available to an ordinary computer user, such as "deleted" files and "file fragments." As you may know, although a user may "erase" or "delete" a file, all that is really erased is a reference to that file in a table on the hard disk; unless overwritten with new data, a "deleted" file can be as intact on the disk as any "active" file you would see in a directory listing.

{Courts have made it clear that all information available on electronic storage media is discoverable, whether readily readable ("active") or "deleted" but recoverable. See, e.g., Easley, McCaleb & Assocs., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994; "deleted" files on a party's computer hard drive held to be discoverable, and plaintiff's expert was allowed to retrieve all recoverable files); Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N.Y. 1988; a request for "raw information in computer banks" was proper and obtainable under the discovery rules); Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90, 112 (D. Colo. 1996; mirror-image copy of everything on a hard drive "the method which would yield the most complete and accurate results," chastising a party's expert for failing to do so); and Northwest Airlines, Inc. v. Teamsters Local 2000, et al., 163 L.R.R.M. (BNA) 2460, (USDC Minn. 1999); court ordered image-copying by Northwest's expert of home computer hard drives of employees suspected of orchestrating an illegal "sick-out" on the Internet).}

Accordingly, electronic data and storage media that may be subject to our discovery requests and that your client{s} are obligated to maintain and not alter or destroy, include but are not limited to the following:

Introduction: description of files and file types sought

All digital or analog electronic files, including “deleted” files and file fragments, stored in machine-readable format on magnetic, optical or other storage media, including the hard drives or floppy disks used by your client’s {clients’} computers and their backup media (e.g., other hard drives, backup tapes, floppies, Jaz cartridges, CD-ROMs) or otherwise, whether such files have been reduced to paper printouts or not. More specifically, your client{s} is {are} to preserve all of your e-mails, both sent and received, whether internally or externally; all word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all CAD (computer-aided design) files, including drafts and revisions; all presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint); all graphs, charts and other data produced by project management software (such as Microsoft Project); all data generated by calendaring, task management and personal information management (PIM) software (such as Microsoft Outlook or Lotus Notes); all data created with the use of personal data assistants (PDAs), such as PalmPilot, HP Jornada, Cassiopeia or other Windows CE-based or Pocket PC devices; all data created with the use of document management software; all data created with the use of paper and electronic mail logging and routing software; all Internet and Web-browser-generated history files, caches and “cookies” files generated at the workstation of each employee and/or agent in your client’s {clients’} employ and on any and all backup storage media; and any and all other files generated by users through the use of computers and/or telecommunications, including but not limited to voice mail. Further, you are to preserve any log or logs of network use by employees or otherwise, whether kept in paper or electronic form, and to preserve all copies of your backup tapes and the software necessary to reconstruct the data on those tapes, so that there can be made a complete, bit-by-bit “mirror” evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from _____ to the present.

Your client{s} is {are} also not to pack, compress, purge or otherwise dispose of files and parts of files unless a true and correct copy of such files is made.

Your client{s} is {are} also to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files); network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view and (if necessary) reconstruct the electronic data we [are requesting/will request] through discovery.

1. **Business Records:** [All documents and information about documents containing backup and/or archive policy and/or procedure, document retention policy, names of backup and/or archive software, names and addresses of any offsite storage provider.]

a. All e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) {sent or received} by the following persons:

   [list names, job titles]

b. All other e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) containing information about or related to:

   [insert detail]

c. All databases (including all records and fields and structural information in such databases), containing any reference to and/or information about or related to:

   [insert detail]

d. All logs of activity (both in paper and electronic formats) on computer systems and networks that have or may have been used to process or store electronic data containing information about or related to:

[insert detail]

e. All word processing files, including prior drafts, “deleted” files and file fragments, containing information about or related to:

[insert detail]

f. With regard to electronic data created by application programs which process financial, accounting and billing information, all electronic data files, including prior drafts, “deleted” files and file fragments, containing information about or related to:

[insert detail]

g. All files, including prior drafts, “deleted” files and file fragments, containing information from electronic calendars and scheduling programs regarding or related to:

[insert detail]

h. All electronic data files, including prior drafts, “deleted” files and file fragments about or related to:

[insert detail]

2. **Online Data Storage on Mainframes and Minicomputers:** With regard to online storage and/or direct access storage devices attached to your client’s {clients’} mainframe computers and/or minicomputers: they are not to modify or delete any electronic data files, “deleted” files and file fragments existing at the time of this letter’s delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps have been taken to assure that such a copy will be preserved and accessible for purposes of this litigation.

3. **Offline Data Storage, Backups and Archives, Floppy Diskettes, Tapes and Other Removable Electronic Media:** With regard to all electronic media used for offline storage, including magnetic tapes and cartridges and other media that, at the time of this letter’s delivery, contained any electronic data meeting the criteria listed in paragraph 1 above: Your client {clients} is {are} to stop any activity that may result in the loss of such electronic data, including rotation, destruction, overwriting and/or erasure of such media in whole or in part. This request is intended to cover all removable electronic media used for data storage in connection with their computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes and all other media, whether used with personal computers, minicomputers or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data, for all of their computer systems.

4. **Replacement of Data Storage Devices:** Your client {clients} is {are} not to dispose of any electronic data storage devices and/or media that may be replaced due to failure and/or upgrade and/or other reasons that may contain electronic data meeting the criteria listed in paragraph 1 above.

5. **Fixed Drives on Stand-Alone Personal Computers and Network Workstations:** With regard to electronic data meeting the criteria listed in paragraph 1 above, which existed on fixed drives attached to stand-alone microcomputers and/or network workstations at the time of this letter’s delivery: Your client {clients} is {are} not to alter or erase such electronic data, and not to perform other procedures (such as data compression and disk de-fragmentation or optimization routines) that may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listings (including

hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve copies during the pendency of this litigation.

6. **Programs and Utilities:** Your client {clients} is {are} to preserve copies of all application programs and utilities, which may be used to process electronic data covered by this letter.

7. **Log of System Modifications:** Your client {clients} is {are} to maintain an activity log to document modifications made to any electronic data processing system that may affect the system's capability to process any electronic data meeting the criteria listed in paragraph 1 above, regardless of whether such modifications were made by employees, contractors, vendors and/or any other third parties.

8. **Personal Computers Used by Your Employees and/or Their Secretaries and Assistants:** The following steps should immediately be taken in regard to all personal computers used by your client's {clients'} employees and/or their secretaries and assistants.

a. As to fixed drives attached to such computers: (i) a true and correct copy is to be made of all electronic data on such fixed drives relating to this matter, including all active files and completely restored versions of all deleted electronic files and file fragments; (ii) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and (iii) such copies and listings are to be preserved until this matter reaches its final resolution.

b. All floppy diskettes, magnetic tapes and cartridges, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to this matter are to be collected and put into storage for the duration of this lawsuit.

9. **Evidence Created Subsequent to This Letter:** With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence is not be destroyed and your client {clients} is {are} to take whatever steps are appropriate to avoid destruction of evidence.

In order to assure that your and your client's {clients'} obligation to preserve documents and things will be met, please forward a copy of this letter to all persons and entities with custodial responsibility for the items referred to in this letter.

Sincerely, etc.

Appendix B -- Sample electronic discovery interrogatories and requests for production

Below are suggested interrogatories and requests for production that are meant to be complementary (i.e., any devices or electronic files that are identified in answer to an interrogatory or interrogatories are usually immediately requested in the follow-up request[s] for production).

For more detailed questions that you might want to include in interrogatories rather than in a deposition, see the sample deposition questions.

Sample Interrogatories and Requests for Production

[Note: The precise format for the following suggested interrogatories and requests for production of documents and things should be in accordance with the applicable civil and local rules of the court where the matter is filed.]

[suggested language for inclusion in preamble:]

I. Definitions

For the purposes of the following interrogatories and requests for production of documents and things, the following definitions apply:

Application Software: A set of electronic instructions, also known as a program, which instructs a computer to perform a specific set of processes.

Archive: A copy of data on a computer drive, or on a portion of a drive, maintained for historical reference.

Backup: A copy of active data, intended for use in restoration of data.

Computer: Includes but is not limited to network servers, desktops, laptops, notebook computers, employees' home computers, mainframes, the PDAs of [party name] and its employees (personal digital assistants, such as PalmPilot, Cassiopeia, HP Jornada and other such handheld computing devices), digital cell phones and pagers.

Data: Any and all information stored on media that may be accessed by a computer.

Digital Camera: A camera that stores still or moving pictures in a digital format (TIFF, GIF, etc.).

Document: Includes but is not limited to any electronically stored data on magnetic or optical storage media as an "active" file or files (readily readable by one or more computer applications or forensics software); any "deleted" but recoverable electronic files on said media; any electronic file fragments (files that have been deleted and partially overwritten with new data); and slack (data fragments stored randomly from random access memory on a hard drive during the normal operation of a computer [RAM slack] or residual data left on the hard drive after new data has overwritten some but not all of previously stored data).

Hard Drive: The primary hardware that a computer uses to store information, typically magnetized media on rotating disks.

Help Features/Documentation: Instructions that assist a user on how to set up and use a product including but not limited to software, manuals and instruction files.

Imaged Copy: A "mirror image" bit-by-bit copy of a hard drive (i.e., a complete replication of the physical drive).

Input Device: Any object that allows a user to communicate with a computer by entering information or issuing commands (e.g., keyboard, mouse or joystick).

Magnetic or Optical Storage Media: Include but are not limited to hard drives (also known as "hard disks"), backup tapes, CD-ROMs, DVD-ROMs, JAZ and Zip drives, and floppy disks.

Network: A group of connected computers that allow people to share information and equipment (e.g., local area network [LAN], wide area network [WAN], metropolitan area network [MAN], storage area network [SAN], peer-to-peer network, client-server network).

Operating System: Software that directs the overall activity of a computer (e.g., MS-DOS, Windows, Linux).

Network Operating System: Software that directs the overall activity of networked computers.

Software: Any set of instructions stored on computer-readable media that tells a computer what to do. Includes operating systems and applications.

Storage Devices: Any device that a computer uses to store information.

Storage Media: Storage media are any removable devices that store data.

II. Spoliation: getting information on preservation of information.

S1. Written policies on preservation of records

Interrogatory No._____:

Do you have a written policy for the retention of documents, including but not limited to business records?

Request for Production No._____:

Please produce copies of any and all written policies for the retention of documents, for the time period of _____ to _____ inclusive.

S2. Destruction of documents

Interrogatory No._____:

Do you have a written policy for the destruction of documents, including but not limited to business records?

Request for Production No._____:

Please produce copies of any and all written policies for the destruction of documents, for the time period of _____ to _____ inclusive.

Interrogatory No._____:

Has destruction or overwriting of documents been suspended? If so, on what date did suspension begin?

S3. Persons in charge of maintaining document retention and destruction policies

Interrogatory No._____:

Identified by job title, job description and business address and telephone number, who are all persons in charge of implementing the policies identified in your answer to Interrogatories 1 and 2 above?

Interrogatory No._____ :

If not the same person(s) as identified in your answer to the immediately preceding interrogatory, identify by job title, job description, and business address and telephone number, the person at [party name] who is the most knowledgeable about the retention and destruction of documents at [party name]?

Interrogatory No._____:

With respect to preventing the spoliation of documents and things that may potentially become evidence in litigation, please identify with particularity and in detail:

a. Whether the minutes of the meetings of the Board of Directors, from [date] to [date] contain any references to considerations or discussions of preventing such spoliation of potential evidence.

b. If so, state the dates of the meetings for which minutes were taken.

c. If so, state the name, title, job description, business address and telephone number of the person or persons with custody of those minutes.

Request for Production No._____:

Please produce all documents referenced in the immediately preceding interrogatory.

S4. Preservation of evidence

Interrogatory No._____:

Since [date of opposing party's awareness of client's claim or counterclaim, if not date of complaint, cross-claim or counterclaim], have any documents at [party name] been destroyed? If so, please state which electronic files have been deleted from the magnetic or optical storage media of [party name] or overwritten from that date to the present, and dates of destruction or overwriting.

S5. Storage of documents

Interrogatory No._____:

As to the storage of data generated by the users of your computers (such as word-processed files and e-mail), please state whether:

A. The data are backed up on tape or other media?

1. If so:

a. How many such media currently exist with backup data on them?
b. What is the maximum storage size in megabytes for each such media?
c. What is the brand name for each such media?
d. When was the last time each such media was backed up with data?
e. What was the computer or other hardware (e.g., individual workstation, server) for each such backup?
f. With respect to the immediately foregoing question, state the physical location and current user of each computer or other hardware listed.

Request for Production No._____:

Please produce all backup and/or archive media, for the time period of _____ to _____ inclusive.

III. Data Universe – identifying it

Interrogatory No._____:

Does or did [party name] maintain, or contract with another party to maintain, an overall inventory of data resources such as a Year 2000 Plan or Disaster Recovery Plan? If so, please provide the name, address, phone number and other contact information for the individuals primarily responsible for maintenance of the inventory and/or plan.

Request No._____:

Produce any and all company organizational and policy information in its entirety, including but not limited to organizational charts, corporate policy and procedure manuals, policy memoranda, system schematic, network topology, system restart procedures, e-mail retention policies, Year 2000 Plan, Disaster Recovery Plan, and other related items.

IV. Information personnel

Interrogatory No._____:

Provide a list of all personnel responsible for maintaining computer hardware, data or information systems on computers for [party name]. Include name, position title, contact information, and official job description and list of duties.

Request No._____:

Produce all formal and informal contact lists and duty rosters for personnel in Information Technology (IT) and Information Services (IS), or equivalent divisions within [party name]. Specifically include rosters for groups such as Incident Response Teams, Data Recovery Units, Audit/Investigation Teams, etc.

Request No._____:

Produce all formal job descriptions, assignments and personnel lists for IT and IS personnel, including revisions, for the period _____ to _____.

V. Loose media (including Backup and Archive)

Interrogatory No._____:

Does [party name] maintain a policy regarding use of loose or removable media in its workstations, computers or networks? If so, state the name of the person(s) responsible for creating and enforcing that policy.

Request No._____:

Provide a copy of the policy mentioned in the preceding interrogatory, as well as any revisions, records or logs related to formulation or enforcement of that policy for the period _____ to _____.

Request No._____:

Produce any and all devices used to place information on loose or removable storage media, including but not limited to hard drives, floppy drives, CD-ROM drives, tape drives, recordable DVD-ROM drives, and removable drives (e.g., Jaz, Syjet, Zip, SuperDisk). Include all instructions for use and maintenance of those devices.

Request No._____:

Produce any and all loose or removable media used to store data, including but not limited to floppy disks, CD-ROM discs and tape drive cartridges, that have been used by personnel or contractors of [party name] to perform work for [party name].

Request No._____:

Produce any and all backup and/or archived data [describe scope of data].

Request No._____:

All slack, wherever located, even if media contains nonproduced data.

VI. Computer hardware

Interrogatory No._____:

List all computer equipment provided by [party name] or used by employees of [party name] to perform work for [party name], including but not limited to hardware and/or peripherals attached to a computer such as computer cases [desktop, tower, portable/batteries, all-in-one], monitors, modems [internal, external], printers, keyboards, printers, scanners, mice [cord and cordless], pointing devices [joystick, touchpad, trackball] and speakers. Include description of equipment, serial number, all users for the period _____ to _____ and dates used, and all locations where the equipment was located for the period _____ to _____.

Interrogatory No._____:

Will [party name] permit, without an order therefore, inspection of the equipment mentioned in the preceding interrogatory?

Request No. [follow-up, if response to preceding interrogatory is negative] _____:

Please produce the following computers, including their magnetic or optical storage media, for inspection and copying, on or before [date], at the offices of [law firm] at [address]:

[list of computers you want image-copied, previously identified in discovery; alternatively, if you know the computer population is relatively small]:

Please produce your computers, including their magnetic or optical storage media, for inspection and copying, on or before [date], at the offices of [law firm] at [address]:

Interrogatory No._____:

List all hardware components (e.g., motherboard, modem, NIC, etc.) installed internally or externally to the PC(s) used by _____ during the period _____ to _____.

Request No._____:

Provide any and all documentation of software and hardware modifications to the PC(s) used by _____ during the period _____ to _____, including but not limited to modification dates, software/hardware titles and version numbers, names of persons performing modifications, location of any backup of the data on the computer performed prior to modification, and disposition of replaced software and hardware.

Request No._____:

Produce any and all documentation instructing in setup and use of the PC(s) used by _____ during the period _____ to _____, and hardware and software installed on that/those PC(s). Include any and all documentation reflecting communication with a computer professional or help desk for help in setting up and using the PC(s).

Interrogatory No._____:

List discarded or replaced hardware and software for the PC(s) (including entire PCs) used by _____ during the period _____ to _____. If the hardware or software is no longer in your control, then include the name and contact information of last known custodian.

VII. Computer Software

Request No._____:

Produce any and all software installed or used on the PC(s) used by _____ during the period ____ to _____. Include all titles and version numbers. Include authors and contact information for authors of custom or customized software. Include operating system(s) software.

VIII. Operating Systems

Interrogatory No._____:

List all operating systems (including but not limited to UNIX, Windows, DOS, Linux and PDA operating systems) installed on all computers used by [party name], the specific equipment the OS was installed on and the period during which it was installed on the specific equipment.

Request No._____:

Provide copies of all operating system software listed in the preceding interrogatory, and all supporting documentation provided with the software, and any manuals and tutorials acquired by [party name] to support use of the software.

IX. Telephony

Interrogatory No._____:

Do you have any graphic representation of the components of your telephone and voice messaging system, and the relationship of those components to each other, including but not limited to flow charts, videos or photos, and diagrams?

Interrogatory No._____:

If so, where are the documents located? Include logical paths for electronic documents.

Request No._____:

Produce copies of any and all graphic representations of your telephone and voice messaging network, and the relationship of those components to each other, including any revisions, for the period of _____ to _____ inclusive. If the documents are electronic, please produce them in their native form, as they existed at the time they were drafted, based on archive or back-up data.

Interrogatory No._____:

List all telephone equipment provided by [party name] or used by employees of [party name] to perform work for [party name], including but not limited to desktop telephones, cell phones, pagers, PDA and laptop modems, calling cards, telephony software and contact management software. Include description of equipment and software, serial number, all users for the period of _____ to _____ inclusive and dates used, and all locations where the equipment was located for the period of _____ to _____ inclusive.

Interrogatory No._____:

Will [party name] permit, without an order therefore, inspection of the equipment mentioned in the preceding interrogatory?

Request No._____:

Produce any and all voice messaging records including but not limited to caller message recordings, digital voice recordings, interactive voice response unit (IVR/VRV) recordings, unified messaging files, and computer-based voice mail files to or from [specified parties] for the period _____ to _____.

Request No._____:

Produce all phone use records for [party name] including but not limited to logs of incoming and outgoing calls, invoices and contact management records, manually or automatically created or generated for the period from _____ to _____ inclusive.

X. Other sources of electronic evidence

Interrogatory No._____:

List all log files (files with suffixes) found on computers in [party name]'s network, and the equipment and logical path where the log files may be found.

Request No._____:

Provide copies of the following log files: [this is a follow-up request to the preceding interrogatory, issued after the list of log files has been reviewed]

Request No._____:

Produce any and all manual and automatic records of equipment use, including but not limited to fax, access, audit, security, e-mail, printing, error and transmission records.

Interrogatory No._____:

Do any employees of [party name] subscribe to or participate in Internet newsgroups or chat groups in the course of their employment? If so, list all users and the services that they subscribe to or participate in.

Request No._____:

Produce any and all information related to newsgroups or chat groups, including but not limited to names and passwords for each and every service, newsgroup messages, text files and programs used to access messages.

Interrogatory No._____:

Do any employees of [party name] use portable devices in the course of their employment that are not connected to [party name]'s network, and that are not backed up or archived? If so, list all users and the devices they use.

Request No._____:

Produce any and all portable devices not backed up or archived, including but not limited to handheld devices, set-top boxes, notebook devices, CE devices, digital recorders, digital cameras and external storage devices.

Interrogatory No._____:

Does [party name] provide Internet access for any of its employees or has [party name] done so at any time during the period from ____ to _____ inclusive? If so, list the employees who had Internet access, the Internet service provider (ISP) used, and describe the method(s) used to connect to the Internet.

Request No._____:

Produce any and all documentation describing installation and use of hardware and software used by [party name] to provide Internet access for its employees during the period from _____ to _____ inclusive.

Request No._____:

Produce copies of all manuals, policies and other guidelines for employee access and use of Internet resources.

Interrogatory No._____:

Describe any restrictions on, controls over or monitoring of employee use of Internet resources.

Request No._____:

Provide any records generated as a result of restrictions on, controls over and monitoring of employee use of Internet resources.

Interrogatory No._____:

Provide a list of any and all Internet-related data on the PCs used by [specific employees or classes of employees], including but not limited to saved Web pages, lists of Web sites, URL addresses, Web browser software and settings, bookmarks, favorites, history lists, caches, cookies.

XI. Data security measures

Interrogatory No._____:

List any and all user identification numbers and passwords necessary to access computers or programs addressed in interrogatories and requests. Your response to this interrogatory must be updated with responses to future sets of interrogatories and requests and updated responses to any set of interrogatories and requests.

Interrogatory No._____:

Please provide copies of your computer security policies and procedures and the name and contact information for the person responsible for security.

Interrogatory No._____:

Please provide information about the security settings for the [program]. For example, please provide the security settings for the Exchange Server, noting who has administrative rights.

XII. Network questions

Request No._____:

Produce any and all documents and things related to networks or groups of connected computers that allow people to share information and equipment, including but not limited to local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), storage area networks (SANs), peer-to-peer networks, client-server networks, integrated services digital networks and VPNs.

Request No._____:

Produce any and all components related to networks, including but not limited to information exchange components (e.g., Ethernet, token-ring, ATM), network work file servers, traffic, hubs, network interface cards, cables, firewalls, user names, passwords and intranet.

N1. System overview

Interrogatory No._____:

Do you have any graphic representation of the components of your computer network, and the relationship of those components to each other, including but not limited to flow charts, videos or photos, and drawings? Include network topology documents and network schemas in your response.

Interrogatory No._____:

If so, where are the documents located? Include logical paths and physical locations for electronic representations.

Request No._____:

Produce copies of any and all graphic representations of your computer network, and the relationship of those components to each other, including any revisions, for the period of _____ to _____ inclusive. If the documents are electronic, produce them in their native form, as they existed at the time they were drafted, based on version or backup data.

XIII. Electronic mail (e-mail)

Request No._____:

Produce any and all information related to e-mail, including but not limited to current, backed-up and archived programs, accounts, unified messaging, server-based e-mail, Web-based e-mail, dial-up e-mail, user names and addresses, domain names and addresses, e-mail messages, attachments, manual and automated mailing lists and mailing list addresses.

BIOGRAPHICAL DATA

RODNEY B. HASTINGS
Deputy Disciplinary Counsel
Office of the Disciplinary Counsel
Louisiana Attorney Disciplinary Board

Since 1998, **Rodney B. Hastings** has been employed by the Louisiana Attorney Disciplinary Board in various capacities. His duties have included serving as publications editor, assisting with the coordination of Disciplinary Board's public outreach programs, and assisting with the coordination of CLE seminars presented by the Disciplinary Board. Following his graduation from Loyola University School of Law and admission to practice in April 2003, Rodney served as one of the Disciplinary Board's staff attorneys until August 2005, when he began working as a deputy disciplinary counsel. He is a member of the American Bar Association, the Louisiana State Bar Association, and the National Organization of Bar Counsel. Rodney serves as a member of the LSBA's Technology Committee, and is a former member of the LSBA's Legal Services for Persons with Disabilities Committee.

Rodney has completed specialized training in the field of computer forensics, culminating in his certification as an "EnCase Certified Examiner" in May 2006. The EnCase Certified Examiner (EnCE) program certifies both public and private sector professionals in the use of Guidance Software's EnCase computer forensic software. EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase during complex computer examinations. Recognized by both the law enforcement and corporate communities as a symbol of in-depth computer forensics knowledge, EnCE certification illustrates that an investigator is a skilled computer examiner.