

Bill Dean

Subject: Knoxville's EDiscovery Newsletter - September 2007

Welcome to Knoxville's EDiscovery and Computer Forensics Newsletter. Keeping you and your practice informed of the ever-changing realm of Electronic Discovery and Computer Forensics is the purpose of this newsletter. If you have a colleague that may be interested in subscribing, the link to subscribe is <http://www.forensicdiscoveries.com/newsletter.html> . If you choose not to continue receiving this newsletter, please reply to this e-mail with "Remove" in the subject line and accept my apologies for intruding.

Inside this Edition

- Preparing your clients for EDiscovery (part 1)
- New Act Addresses Timely Issue of Electronic Discovery
- Discoverability Case Law
- Computer Forensics Case Law
- New (free) Legal Research website
- Onsite Presentations and Obligation free consultation
- Next Month's Topics

Preparing your clients for EDiscovery

It has been almost 10 months since the updated Federal Rules of Civil Procedure went into effect that many feel put ESI on the level with paper with regards to discovery. Independent surveys of corporate preparation to comply with these rules have been labeled "abysmal" by Forrester.com. The differentiator between those companies that are and are not prepared is often clear; companies that have had to produce ESI in litigation have vowed not to endure the fire drill again. To complicate matters for attorneys, the following excerpt was given in *Zubulake V. UBS Warburg* opinion, "*[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.*" Specifically, the court concluded that attorneys are obligated to ensure all relevant documents are discovered, retained, and produced. Additionally, the court declared that litigators must guarantee that identified relevant documents are preserved by placing a "litigation hold" on the documents, communicating the need to preserve them, and arranging for safeguarding of

relevant archival media. The good news is that the basic framework to prepare for electronic discovery can be simplified when broken down into manageable steps and most IT departments already have much of the information needed.

When the new Federal Rules of Civil Procedure were on the horizon, there were many software vendors modifying their products to solve what they considered to be all EDiscovery problems. The majority of the vendors were email archiving vendors that had been working in environments that were under Sarbanes-Oxley regulation. Email archiving can provide value to electronic discovery, but responding to electronic discovery requests and complying with Sarbanes-Oxley regulations require different approaches. For example in September of 2005, The *National Law Journal* reported that more than 50 percent of evidence found in electronic discovery is e-mail. Companies and attorneys must ensure that the remaining portion is also produced. The other portion of electronic data could be located on personal computers, laptops, file servers, personnel databases, client databases, and web servers, just to name a few. In addition, email archiving systems only provide email that is stored *in* the email archive system. In summary, email archiving systems are not a full solution for Electronic Discovery. In fact, there is no “black box” solution to EDiscovery. Each company’s data systems are unique and require different approaches based on proactive planning and preparation.

The steps to respond to an electronic discovery request are to identify, preserve, collect, process, and produce relevant ESI. It is my opinion that the foundation for a successful process for providing ESI in discovery begins with the identification phase. Without proper location and identification of the data, compliance with the discovery request will be difficult at best. The good news is that your client likely already has information in place to provide this information. The identification phase revolves around what many call a “data map”. In a simplified explanation, a data map simply consists of the locations of ESI. Here (<http://www.forensicdiscoveries.com/datamap.jpg>) is a link to my website with a template data map for a fictitious financial company that can be used with your clients to begin the preparations for EDiscovery. As you can see, the map designates where information is located, the data flow, and takes the additional step of determining the classification of data as to whether it is data that is reasonably accessible or data that is not reasonably accessible. The IT departments of your clients can modify this map or create a new map that contains the information needed for your files. This data map will provide great benefit when conducting your meet and confer conferences.

Next month I will provide the next installment in this discussion to include the preservation, collection, processing, and production of relevant ESI.

New Act Addresses Timely Issue of Electronic Discovery

From a release posted by the Uniform Law Commission on August 2nd:

By some recent estimates, more than 90% of business information is now stored electronically. The state rules concerning discovery of information in civil cases were written at a time when information was mostly stored on paper. A new act approved today by a national law group addresses the growing concern over the rules of discovery that courts must follow to access electronic information in civil cases. The **Uniform Rules Relating to Discovery of Electronically Stored Information** was approved today by the Uniform Law Commission (ULC) at its 116th Annual Meeting in Pasadena, California.

The primary purpose of the new uniform rules is to provide states with up-to-date rules for the discovery of electronic documents in civil cases.

“With the emergence of electronic technology, the extent to which information is stored electronically has vastly increased, and will continue to do so,” says Rex Blackburn, chair of the committee that drafted the new uniform rules. “These new uniform rules should provide states with the necessary guidance governing discovery of electronically stored information.”

In 2006, the Advisory Committee on the Federal Rules of Civil Procedure amended the federal rules governing discovery of electronic documents. The Uniform Rules conform as closely as possible to comparable provisions in the Federal Rules. The Uniform Rules are modified, where necessary, to accommodate the varying state procedures.

The Uniform Rules provide procedures for parties in a civil case to jointly follow relating to a number of issues, including the preservation of the electronic information; the form in which the information will be produced; and the period of time in which the information must be produced.

The Uniform Rules limit the sanctions which may be imposed on a party for failure to provide electronic information that has been lost as the result of routine operation of an electronic information system. This rule applies to information lost due to the routine operation of an information system only if the system was operated in good faith.

The Uniform Rules address the unique difficulties in accessing some electronic information by providing certain restrictions on its discovery. For instance, a party may object to discovery of electronically stored information on the grounds that the information is not reasonably accessible because of undue burden or expense. However, the court may order discovery of such information if it is shown that the likely benefit of the proposed discovery outweighs the likely burden or expense, and may allocate between the parties the expense of conducting the discovery.

More information on the Uniform Rules Relating to Discovery of Electronically Stored Information Act can be found at ULC’s website at www.nccusl.org.

Discoverability Case Law

[Wife Allowed to Access Husband's Email in Marital Dissolution Action](#)

***White v. White*, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001).** In a divorce action, the husband filed a motion to suppress his email that had been stored on the hard drive of the family computer. The court held that the wife did not unlawfully access stored electronic communications in violation of the New Jersey Wiretap Act and did not intrude on his seclusion by accessing those emails. "Having a legitimate reason for being in the files, plaintiff had a right to seize evidence she believed indicated her husband was being unfaithful....Is rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cabinet...Not really."

Computer Experts Ordered to Create Computer Tape Containing Information Previously Produced in Paper

***National Union Elec. Corp. v. Matsushita Elec. Ind. Co.*, 494 F. Supp. 1257 (E.D. Pa. 1980).** The defendant filed a motion to compel production of a computer tape containing the information that the plaintiff previously produced in a hard copy. The court required the plaintiff to have computer experts create a computer-readable tape containing data previously supplied to the defendant in printed form

[Summary Judgment Granted for Failure to Conduct Computer Examination](#)

***Tempco Elec. Heater Corp. v. Temperature Eng'g Co.* 2004 WL 1254134 (N.D.Ill. Jun. 3, 2004), vacated and rev'd in part, Case No. 02 C 3572 (Jun. 29, 2004).** In response to the plaintiff's claims of trademark infringement, breach of contract, and misappropriation of trade secrets, the defendant moved for partial summary judgment arguing that the plaintiff presented no evidence to support its claims. In support of its motion, the defendant submitted findings by a computer company, who inspected the defendant's computers and determined that no remnants of the plaintiff's confidential database existed on the defendant's computers. Arguing that the court should deny the summary judgment motion, the plaintiff declared that the computer company had performed a minimal inspection and that a more complete computer forensic investigation might have revealed evidence of the database. The court granted the defendant's summary judgment motion declaring that the plaintiff "has the burden of proof, and therefore the responsibility to conduct a thorough investigation. [The plaintiff] cannot simply sit back and complain about the inadequacy and/or bias of [the defendant's] inspection efforts." The plaintiff appealed this decision claiming testimony from one of the defendant's employees revealed the defendant did not remove all copies of a computer program at issue from its computers as it claimed it did. Finding this established enough evidence to overcome summary judgment, the court vacated and reversed its original summary judgment finding.

[Court Defines E-mail as a Document, Therefore Subject to Inspection](#)

***Kasten v. Doral Dental USA, LLC*, 2007 WL 1791226 (Wis. June 22, 2007)** In a suit by a non-managing member of a limited liability company seeking to review company records, the district court held email was neither a record nor a company document. The district court determined that email was just a communication like a telephone call, not a document or record. The plaintiff appealed this distinction, and the Wisconsin Supreme Court reversed.

Court Appoints Neutral Computer Forensics Expert to Assist in Discovery Process

***Antioch v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D.Minn. 2002).** In a copyright infringement action, the plaintiff moved for issuance of an order directing the defendant to: preserve records, expedite discovery, compel discovery, and appoint a neutral computer forensics expert. Emphasizing the potential for spoliation of the computer data, the court stated “we conclude that the defendants may have relevant information, on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the plaintiff’s claims, or the defendants’ defenses.”

Court Approves Keyword Searching in Uncovering Relevant Emails

***Tulip Computers Int’l v. Dell Computer Corp.*, 2002 WL 818061 (D.Del. Apr. 30, 2002).** On the plaintiff’s motion to compel in a patent infringement case, the court stated that “[T]he procedure that Tulip has suggested for the discovery of email documents seems fair, efficient, and reasonable.” The court ordered the defendant to produce the hard disks of certain company executives to the plaintiff’s electronic discovery expert for keyword searching. After the expert completed the keyword search, the plaintiff would be required to give the defendant a list of the emails that contain those search terms. The defendant would then produce the emails to the plaintiff, subject to its own review for privilege and confidentiality.

Court Declares Discoverability of Electronically-Stored Information

***Rowe Entertainment, Inc. v. The William Morris Agency*, 2002 WL 975713 (S.D.N.Y. May 9, 2002).** “Rules 26(b) and 34 for the Federal Rules of Civil Procedure instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials.”

Court Determines Electronic Data is Discoverable Even if Paper Copies Were Already Produced

***Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995).** “The law is clear that data in computerized form is discoverable even if paper ‘hard copies’ of the information have been produced...[T]oday it is black letter law that computerized data is discoverable if relevant.”

Computer Forensics Case Law

For a quick review, Computer forensic experts are most adept at performing the following activities:

- Determining dates and times of logon and log-off on the computer
- Locating files and information about when they were created, accessed, modified and deleted
- Retrieving e-mails and information about when they were sent, received and drafted
- Creating a list of Internet Web sites visited and the activities performed on those Web sites
- Finding key words and key data, whether contained in active or deleted files
- Searching for the existence of certain programs such as file deletion and wiping programs
- Issuing official, expert opinions based on their experience and knowledge of best practices

Court Issues Adverse Jury Instruction Where Plaintiff Disposed of Home Computer after Filing Discrimination Suit

***Teague v. Target Corp.*, 2007 WL 1041191 (W.D.N.C. Apr. 4, 2007).** In a gender discrimination suit, the defendant brought a motion for sanctions against the plaintiff for spoliation of evidence, specifically seeking dismissal of the suit because the plaintiff disposed of her home computer after filing an EEOC claim against the defendant. The plaintiff's home computer contained evidence relating to her lawsuit against the defendant. The plaintiff claimed that she disposed of her computer after the hard drive crashed and was unable to be repaired by her brother. The court held that sanctions were appropriate since the computer contained evidence directly related to the plaintiff's claims and her efforts to mitigate her damages by finding another job after leaving the defendant's company. The court determined that she disposed of the computer with a "culpable state of mind" and an adverse inference jury instruction at trial was proper.

Court Issues Spoliation Sanctions for "Crashed" Hard Drive and Appoints Special Master at Defendant's Expense

***Padgett v. City of Monte Sereno*, 2007 WL 878575 (N.D. Cal. Mar. 20, 2007).** In a case alleging civil rights violations and infliction of emotional distress, the plaintiff sought to explore claims about the authorship of a harassing letter he received from a city employee. The court initially denied the plaintiff's request to compel inspection of the city's computers but ordered the defendant to preserve "everything." The city assured the court it would abide by the preservation order. However, after a subsequent court order for production of three of its employee's hard drives, the defendant acknowledged it had destroyed one of them. The defendant explained that the hard drive in question had been inadvertently discarded after the user's laptop "crashed." However, at a hearing before the court, the city explained the laptop had "appeared". Unsatisfied with the city's explanation, the plaintiff moved for terminating sanctions, monetary sanctions and default judgment. In turn, the defendant moved for clarification of the court's previous order to allow inspection or, in the alternative, for a protective order. The court found the defendant had discarded the laptop with notice of its potential relevance, causing delay and additional expense to the plaintiff. While reserving judgment as to whether the defendant's actions warranted terminating sanctions, the court ordered monetary sanctions against the defendant in the amount of the plaintiff's attorney fees and traveling costs associated with bringing the motion. It also ordered the defendant to pay the plaintiff's expert's fees and to bear the cost of a court-appointed special master. The court declined to consider the defendant's motion for clarification, directing the defendant to seek further direction from the special master.

New (free) Legal Research website

Many of you already use the valuable PACER website (<http://pacer.psc.uscourts.gov/>) to

perform online research. PACER, along with most other research sites, are fee based. Recently a new (free) legal research site has emerged, [Altlaw.org](http://www.altlaw.org). Read more about its origins at InformationWeek (<http://www.informationweek.com/news/showArticle.jhtml?articleID=201802106>) or give it a try.

Onsite Presentations and Obligation Free Consultation

Forensic Discoveries is available to provide onsite presentations or Q&A sessions on topics such as Electronic Discovery, Technical Implications of the updated Federal Rules of Civil Procedure, or Computer Forensics. Forensic Discoveries is also available to you, obligation free, to answer any specific questions pertaining to these topics. Simply give us a call and we will be glad to answer any questions pertaining to Electronic Discovery and Computer Forensics.

Next Months Topics

I hope that this newsletter has provided value to you. I am already working on the topics for next month's newsletter:

- Preparing your client for EDiscovery (part 2)
- ESI Spoliation Case Law
- Computer Forensic Protocols Case Law

If you have a topic that you would like addressed in the newsletter, please let us know. Either visit <http://www.forensicdiscoveries.com/newsletter.html> and submit your suggestion there or reply to this e-mail with your suggestion.

For previous versions of Forensic Discoveries EDiscovery newsletters, visit <http://www.forensicdiscoveries.com/pastnewsletters.html>

Sincerely,

Bill Dean

Owner/President

Forensic Discoveries

<http://www.forensicdiscoveries.com>

(865) - 809-7590