

Bill Dean

From: Bill Dean [bill.dean@forensicdiscoveries.com]

Sent: Wednesday, October 10, 2007 9:32 PM

Subject: Knoxville's EDiscovery Newsletter - October 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

- Upcoming Speaking Engagement
- Preparing Your Clients for EDiscovery (part 2)
- Case Law Demonstrating what *not* to do in Discovery
- Spoliation Case Law
- Computer Forensics Protocol Case Law
- Onsite Presentations and Obligation Free Consulting
- Next Month's Topics

Upcoming Speaking Engagement

On Tuesday, October 16th, I will be speaking at the annual CyberSecurity Summit at the University of Tennessee. I will be speaking on the topic of "Presenting Digital Evidence in Court". For more information on the conference, speakers, etc., go to <http://cybersecurity.utk.edu/>. After the conference, a download of all presentations will be available.

Preparing Your Clients for EDiscovery (part 2)

Last week I was reading *Information Week* that contained an article related to EDiscovery which was based on a survey of their readers. Of the respondents of the survey, 53% stated that they have produced ESI in discovery. This statistic further suggests that ESI discovery is becoming as common as paper discovery. Picking up where we left off from last month's newsletter, the data map is essential to the success of any discovery project. Once that is in place, the remaining steps of preservation, collection, processing, and production can become a standard, repeatable process for your clients. This month we will briefly discuss the steps to preserve, collect, process, and produce data in the EDiscovery process.

Prior to the implementation of the updated Federal Rules of Civil procedure last December, many companies felt that "the sky was falling". The thought was that these updated rules would require companies to keep ESI perpetually. Being unable to destroy data would add significant operational costs to store the information long term. Rule 37(f), also known as the "Safe Harbor" rule, addressed this concern. This rule states that "*absent exceptional circumstances a court may not impose sanctions on a party for failing to provide ESI lost as a result of routine, good-faith operation of an electronic information system.*" This rule recognizes that some computer systems routinely alter and delete information without specific direction from an operator. This is where data retention policies become so important to your clients. A data retention policy classifies electronic information and states how long the company will retain the information before destroying it. For example, companies typically prefer not to store e-mail forever. Therefore, companies implement a data retention policy that is specific to e-mail stating that e-mail will only be retained for 365 days and it will then be purged from the system. There are two key points to make about retention policies. The first is that companies must be following their retention policy and not decide to start following it when they sense litigation (that didn't work out well for Arthur Anderson and Enron). This is further reason to ensure that your clients properly dispose of old computers and storage media as it can also be discoverable. The second point about retention policies is that companies must suspend applicable portions (if not all) of their retention policies once a litigation hold is in place (many feel even before the preservation letter). To elaborate more on the suspension of retention rates, parties cannot exploit the routine operation of an information system to thwart discovery by allowing a system to continue to destroy information that it is required to preserve.

With courts quickly becoming less tolerant for spoliation of ESI after the adoption of the updated rules last year, preservation is an essential part of EDiscovery. The change in mindset needed to handle ESI in comparison to paper is that paper does not automatically destroy itself, electronic often does. That is why preservation of ESI must be handled differently than paper. The essential aspect of a litigation hold relevant to ESI is to communicate the data to be preserved and the custodians of that data. Be certain that your client understands what the litigation hold means to their operation. It is essential that the details such as the specific data of interest (office files, e-mail, databases, etc) and who the custodians are to be clearly communicated. Hopefully these details would have been determined in the conferences per Rule 26(f) and 16(b). With the data map already created, it should be relatively simple to determine the location of the agreed upon data in question. Below are some standard steps in implementing a preservation hold:

- Clearly communicate to the IT department the details of the litigation hold.
- Have the existing backup tapes removed from the backup rotation to preserve them and replace with new media. Backup media can be expensive and not all EDiscovery requires restoring data from backup, but this simple step can prevent lots of heartache later if your client is asked to restore data.
- Create forensic images of the custodians' computers. Like backup tapes, this may not be needed. However, better to have it and not need it than need it and not have it.
- Stop the automatic purging of data from systems. Be certain to communicate to the IT department that any purging of data must be suspended while the litigation is in place.

Even relatively small cases can involve millions of files and email messages. Much of the data may ultimately be irrelevant, but all of it must be properly preserved at the outset in its original form in order to ensure its evidentiary integrity should it be required later in court. Courts are increasingly requiring strict adherence to accepted forensic procedures to ensure evidentiary integrity for court submission.

The collection phase of EDiscovery will vary from case to case but some rules of thumb apply to all instances. The custodians of the data should not be in charge of the collection. Either an IT person or an EDiscovery expert should be in charge of collecting the data. Allowing the custodian to collect could raise the suspicion that not all relevant data has been produced and custodians typically do not know where all of the data is stored. Below are some basic steps for collection:

- Gather the backup tapes removed from the backup rotation.
- If applicable, gather the forensic images of the hard drives.
- Make verifiable copies of all relevant data (office documents, e-mail, databases, etc).
- Store all of this information in a safe location outside of the IT environment to avoid mishandling.

The EDiscovery phase of processing will vary greatly depending on the data outlined in the discovery requested. In some instances, the requested data may only be office documents and e-mail. In other instances the data could be stored in a proprietary system that will require data conversions. One clear point that I want to make is that the majority of IT departments typically do not have the tools in house to properly process and cull the data for relevant information. Using specialized EDiscovery and forensic tools, millions of pages of documents can be indexed and keyword searched quickly. If your IT department indicates that they plan to process the information themselves, ask some questions about what tools they will be using and do some research to determine if the tools are adequate to produce the information that was agreed upon with opposing counsel per Rule 34(b). You can also call me and I will tell you

whether or not the tool is adequate. What can make the production a sticky topic is that unlike paper, ESI can be in many formats. As an example, a simple e-mail can be produced in up to 10 different formats. In addition, you will likely be reviewing the data and will also need to ensure you have the proper tools to review the data quickly and efficiently.

The process to prepare for EDiscovery can be perceived as a burden to your clients, especially those with large IT operations. However, this process will save much time and confusion if your client does receive a discovery request that includes ESI. While this process is designed for EDiscovery, it provides other aspects of value. This model can also be used during audits and conducting internal investigations. One goal of the EDiscovery process is to make every effort to avoid having to restore data from backup tapes. The costs of restoring and processing data from backup tapes can quickly increase the costs to your clients. The end goal is to demonstrate due diligence by having a plan and process that is repeatable.

I truly did not intend for this article to be this long and promise future articles will be shorter. I do hope that it has provided some value to you. I wanted to complete the "Preparing your clients" this month so I can write the next article on how to prepare you for your clients' EDiscovery. Whether your clients agree to prepare for discovery or not, I want to help you prepare for their discovery by collecting the needed information about their environment and tips for making the EDiscovery process as smooth as possible.

Case Law Demonstrating what *not* to do in Discovery

We have spent the last two newsletters discussing ways to prepare and respond to electronic discovery requests. Below is a textbook case law example of how not to respond to a discovery request.

[Metropolitan Opera Association, Inc. v. Local 100, 212 F.R.D. 178 \(S.D.N.Y. 2003\)](#)

Similar to *Danis v. USN Communications, Inc.*, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000), this case chronicles the myriad failings and misrepresentations of defense counsel regarding discovery obligations.

Ultimately, the court granted the plaintiff's motion for judgment as to liability against defendants and for additional sanctions in the form of attorneys' fees necessitated by the discovery abuse. Like the *Danis* case, this case provides a checklist of what not to do in discovery. The court found that defendants committed a number of abuses, including the following:

- In response to plaintiff's counsel's continuing assertions of lack of an adequate document search and demonstrations of non-production, defense counsel repeatedly represented to the court that all responsive documents had been produced when, in fact, a thorough search had never been made and counsel had no basis for so representing.
- Defense counsel knew the defendant's files were in disarray and that it had no document retention policy, but failed to cause a retention policy to be adopted to prevent destruction of responsive documents, both paper and electronic.
- Shortly after plaintiff's counsel announced they might seek permission to have a forensic computer

expert examine defendant's computers in an attempt to retrieve deleted emails, defendant replaced those computers without notice.

- Counsel failed to explain to the non-lawyer in charge of the document production, inter alia, that a document included a draft or other non-identical copy and included documents in electronic form.
- The non-lawyer defendant put in charge of document production failed to speak to all persons who might have relevant documents, never followed up with people he did speak to and failed to contact all of defendant's ISP's to attempt to retrieve deleted emails, as counsel represented to the court that he would.
- No lawyer ever doubled back to inquire of the employee in charge of document production whether he conducted a search and what steps he took to assure complete production.
- In the face of plaintiff's counsel's constant assertions that no adequate document search had been conducted and responsive documents had not been produced, defense counsel failed to inquire of several important witnesses until the night before their depositions.
- Defense counsel lied to the court about a witness' vacation schedule in order to delay the witness' court-ordered deposition.

Spoliation Case Law

[Appellate Court Finds Preliminary Injunction Warranted Based on Computer Forensic Expert's Findings](#)

***Liebert Corp. v. Mazur*, 827 N.E.2d 909 (Ill. Ct. App. 2005).** The plaintiffs sought to enjoin several of its former employees from allegedly using electronic "e-commerce" Web sites - containing confidential customer lists, quotations and price books - in a new, competing business. One of the defendants admitted that he downloaded price books from the company's server to his laptop on the day he resigned. The plaintiffs hired a computer forensic expert to examine the laptop, and the expert discovered confidential files were accessed, downloaded and placed in a Zip file. The expert also determined a new Zip folder - containing quote histories and budgets - was created and subsequently copied from the hard drive to a CD-Rom on the same day the defendant was served with the plaintiffs' complaint and preliminary injunction motion. During the copy, the computer automatically placed the files in a "CD burning folder", a folder most computer users are not aware exists. During the next few days, in a "mass wave of deletion," over 12,000 files were deleted from the defendant's computer. The laptop's application log, which tracks programs like the CD-Rom burning program, was also deleted four days after the complaint was served. Despite this evidence, the trial court denied the plaintiff's motion for a preliminary injunction, finding insufficient evidence existed to prove any of the defendants used the price books before they were destroyed. On appeal, the court reversed the decision, determining the trial court abused its discretion, and ordered the trial court to grant a reasonable preliminary injunction. The appellate court noted, "[b]ecause [the defendant] destroyed this crucial piece of evidence [the application log], we presume it would have showed he successfully copied the price books on a CD."

[Computer Expert Investigation Leads to Finding of Electronic Document Trade Secret Theft](#)

***Four Seasons Hotels and Resorts v. Consorcio Barr*, 267 F. Supp.2d 1268 (S.D.Fla. 2003).** The plaintiff brought an action against the defendant licensee alleging, among other things, violations of the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and Uniform Trade Secrets Act. A computer forensic investigation revealed that the defendant accessed the plaintiff's computer network, downloaded confidential data onto backup tapes, fabricated electronic evidence, and deleted files and overwrote data prior to his computer being turned over for inspection to the plaintiff. The court held that the defendant acquired the plaintiff's confidential customer information through improper means, namely,

by theft and by espionage through electronic means. The court issued a judgment for the plaintiff and ordered monetary damages, among other relief.

[Computer Forensics Expert Uncovers Employee's Attempt to Download Company Confidential Documents](#)

***LeJeune v. Coin Acceptors, Inc.*, 2004 849 A.2d 451 (Md. 2004).** In a case involving the violation of a state trade secrets act, an employer alleged that a former employee copied proprietary electronic documents from his work laptop to a compact disc (CD), shortly before he went to work for a competitor. The employee stated that, for the sake of simplicity and because he did not know how to save individual files onto a CD, he had transferred his entire "My Documents" folder, which contained personal files such as his wedding photographs, and inadvertently captured some of his former employer's confidential business documents. The employer's computer forensics expert refuted the employee's claims, testifying that a file, which was not contained in the "My Documents" folder, was also copied to the CD. The expert also determined that the employee had attempted to hide the document transfer by deleting information about the downloads from the laptop. Based on this evidence, the appellate court affirmed the lower court's finding that the evidence supported a finding of trade secret misappropriation.

[Adverse Inference Instruction Issued for Spoliation of Computer Files](#)

***Minnesota Mining & Mfg. v. Pribyl*, 259 F.3d 587 (7th Cir. 2001).** The plaintiff brought suit against three former employees for misappropriation of trade secrets. The appellate court affirmed the trial court's negative inference instruction to the jury where the one defendant committed spoliation of evidence by downloading six gigabytes of music onto his laptop, which destroyed many files sought by the plaintiff, the night before the defendant was to turn over his computer pursuant to the discovery request. However, the fact that hard drive space was destroyed on one defendant's computer did not relieve the plaintiff from proving the elements of its claims.

[Parties Agree to Discovery Management Plan, Including Computer Forensic Examinations and Active Data](#)

***In re Celexa and Lexapro Prods. Liab. Litig.*, 2006 WL 3497757 (E.D. Mo. Nov. 13, 2006)** In this multi-district litigation regarding two prescription drugs, the parties agreed to a document management plan which the court incorporated into its order. The parties established that the plaintiffs would preserve the hard drives of computers used by the plaintiffs and the plaintiffs' decedents, and such hard drives would be imaged and analyzed pursuant to an agreed forensic examination protocol. The parties also decided the defendants would not be required to restore any of their backup tapes at this time, and instead, responsive electronically stored information would be collected from the defendants' active IT environment. They must preserve the thirty-five backup tapes set aside for this litigation, but may otherwise resume backup tape recycling. The plaintiffs deferred the production format decision to the defendants and allowed them to produce data in any format that is generally searchable and manageable. The parties were unable to agree on how costs should be apportioned, the scope of discovery into electronic databases, and who should perform the forensic examination of the computer hard drives. The court determined it would decide these issues after more briefing by the parties.

[Magistrate Recommends Spoliation Sanctions for Failure to Stop Automated E-mail Deletion](#)

***DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005).** In a breach of contract claim relating to the defendant's NASCAR team, the plaintiff sought sanctions against the defendant for destroying relevant e-mails. In defending its actions, the defendant claimed its computer system was set up to delete both internal and external e-mails automatically, unless affirmative efforts were taken to preserve them. As a result of the automated deletion, internal e-mails from key custodians were

“irretrievably lost.” One key individual testified he was never instructed to preserve relevant communications, even after the lawsuit commenced. In considering whether sanctions were justified, a magistrate judge declared “[s]uch normal procedures for destruction of documents must...be suspended when a party is on notice that they may be relevant to litigation, and the failure to make an adequate search of such documents before their destruction may be evidence of bad faith.” Although ultimately finding the defendant’s actions amounted to negligent spoliation and did not show evidence of bad faith, the magistrate found sanctions would be appropriate and recommended the trial court issue an adverse inference instruction and an order allowing the plaintiff to present evidence of the spoliation

[Court Finds Defendants Acted in Bad Faith by Failing to Halt Email Destruction Policy](#)

***Broccoli v. Echostar Communications Corp.*, 2005 WL 1863176 (D. Md. Aug. 4, 2005).** In an employment discrimination case, the plaintiff filed a motion for sanctions against the defendants for failing to preserve electronic documents and for spoliating email evidence. Citing *Zubulake*, the court addressed the defendants’ duty to preserve emails and other relevant documents. The evidence showed the defendants were on notice of the lawsuit long before they halted their data destruction policy. In fact, the defendants admitted they never issued a company-wide instruction regarding suspension of their data destruction policy and they did not save the plaintiff’s emails relating to the harassment incidents or his termination. Based on this evidence, the court granted the plaintiff’s motion for sanctions and issued an adverse inference jury instruction relating to spoliation of the emails. The court declared the defendants acted in bad faith by failing to suspend their email and data destruction policy and by failing to preserve essential personnel documents in order to comply with their preservation obligations. The court further stated, “Given [the defendants’] status as a large public corporation with ample financial resources and personnel management know-how, the court finds it indefensible that such basic personnel procedures and related documentation were lacking.”

Computer Forensics Case Law

[Parties Agree to Discovery Management Plan, Including Computer Forensic Examinations and Active Data Collection](#)

In re *Celexa and Lexapro Prods. Liab. Litig.*, 2006 WL 3497757 (E.D. Mo. Nov. 13, 2006). In this multi-district litigation regarding two prescription drugs, the parties agreed to a document management plan which the court incorporated into its order. The parties established that the plaintiffs would preserve the hard drives of computers used by the plaintiffs and the plaintiffs’ decedents, and those hard drives would be imaged and analyzed pursuant to an agreed forensic examination protocol. The parties also decided the defendants would not be required to restore any of their backup tapes at this time, and instead, responsive electronically stored information would be collected from the defendants’ active IT environment. They must preserve the 35 backup tapes set aside for this litigation, but may otherwise resume backup tape recycling. The plaintiffs deferred the production format decision to the defendants and allowed them to produce data in any format that is generally searchable and manageable. The parties were unable to agree on how costs should be apportioned, the scope of discovery into electronic databases, and who should perform the forensic examination of the computer hard drives. The court determined it would decide these issues after more briefing by the parties.

[Court Orders Mirror Imaging of Computer Hard Drives, Citing New Federal Rules of Civil Procedure](#)

Ameriwood Industries, Inc. v. Liberman, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006). In a suit alleging misappropriation of trade secrets inter alia, the plaintiff motioned the court for an order compelling the defendants to produce computer hard drives for imaging. The plaintiff sought e-mails from the defendants related to dissemination of trade secrets. The plaintiff not only requested all work-related computers, but any home computers that may have been used to transmit the trade secrets. The plaintiff argued it was entitled to the hard drives even if information was deleted since the computers may contain evidence that goes to the heart of the claims. Furthermore, the defendants failed to produce a later discovered e-mail which the plaintiff eventually discovered, thereby creating an argument to search for other undisclosed discovery material. The defendants argued the costs involved would be substantial and imaging should not be completed. The court determined the data requested was not reasonably accessible because of undue burden and cost. However, the court closely examined the newly implemented Federal Rules of Civil Procedure and determined that there was good cause for the plaintiffs to search the defendants' hard drives since "allegations that a defendant downloaded trade secrets onto a computer provide a sufficient nexus between plaintiff's claims and the need to obtain a mirror image of the computer's hard drive." The court then provided detailed guidance for the mirror-imaging process and discovery of documents on the defendants' hard drives. It held that the plaintiff would choose a qualified computer forensics expert and the defendants were required to produce all hard drives, including those from their homes. A disclosure process was also ordered which outlined the process regarding production of documents and privilege issues.

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 you for your clients' EDiscovery
- ESI 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

This document does not provide legal or other professional advice and should not be relied upon as anything other than a starting point for research and information on the subject of electronic evidence.