

CyberBytes

Straight Talk about Data Forensics Effectiveness in Civil Cases- October 2004

Recent Court Decisions

Requesting Party Must Bear E-Discovery Costs; Court Appoints Special Referee to Manage E-Discovery Process

Lipco Elec. Corp. v. ASG Consulting Corp., 2004 WL 1949062 (N.Y. Sup. Ct. Aug. 18, 2004). The plaintiffs sought to compel discovery of relevant electronic files, data and backup tapes from the defendants, despite the fact the defendants had already produced hard copies of the electronic documents at issue. The plaintiff asserted that the only way it could confirm the accuracy of the hard copy data was by obtaining the raw data in computerized form. In response, the defendants argued that extraction of the electronic data would be difficult, costly, and time-consuming, even if the requested data was "material and necessary" to the action. The defendants claimed they would need to hire an expert to retrieve the documents because they could not extract the data from hard drives or backup tapes without assistance. The court noted that, under New York state law, the party seeking discovery must bear the costs of production. Concluding that the electronic data was discoverable, the court noted it "need only determine whether the material is discoverable and whether the party seeking discovery is willing to bear the cost of production." The court declared it was unable to order production of the electronic data until the plaintiffs established they would bear production costs. The court ordered the parties to supply a detailed breakdown of the electronic data's location, procedures used to extract it, and the costs involved. Noting that "[d]iscovery has been proceeding at a snails pace, if at all," the court also appointed a special referee to manage, arrange, and monitor the e-discovery progress.

Court Refuses to Issue Sanctions for Spoliation of Electronic Evidence

Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004). In a patent infringement and trade secret theft suit, the plaintiffs requested direct access to all of the defendants' hard drives, servers and databases. The defendants argued the discovery request was overbroad because it included more than the products at issue in the suit. Refusing to grant the plaintiffs' request for direct access to all of the defendants' computer systems, the court stated such a request "would require an expenditure of time and resources far out of proportion to the marginal value of the materials to this litigation." Alleging discovery misconduct by the defendants, the plaintiffs also moved for spoliation sanctions against the defendants for failing to preserve emails and other electronic data relating to the product in dispute. However, the court declined to award spoliation sanctions because no evidence of intentional destruction of the emails existed, the plaintiffs did not attempt to establish the circumstances under which the emails were deleted, and a preservation order was not in place for the other electronic data.

Sanctions Upheld in Metropolitan Opera Case

Metropolitan Opera Ass'n, Inc. v. Local 100, 2004 WL 1943099 (S.D.N.Y. Aug. 27, 2004). In a case involving a labor dispute, the defendants moved for reconsideration of an earlier decision in which the court issued severe sanctions for mishandling and deleting electronic data during discovery. See Metropolitan Opera Assoc., Inc. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003). Among other things, the defendants argued sanctions were unwarranted because they had initially produced all relevant documents despite the plaintiff's contrary arguments. The defendants also contended that the court could not impose sanctions unless proof existed

that the deleted documents were actually relevant. In response, the court declared it was unknown whether they actually produced all relevant documents since the defendants had deleted documents. The court further stated the decision to impose sanctions was not based upon whether the documents were relevant but, rather, based upon the "vexatious manner" in which the defendants failed to comply with discovery. In upholding the sanctions award, the court noted the "defendants and their counsel may not engage in parallel know-nothing, do-nothing, head-in-the-sand behavior in an effort consciously to avoid knowledge of or responsibility for their discovery obligations and to obstruct plaintiff's wholly appropriate efforts to prepare its case." See also Metropolitan Opera Ass'n, Inc. v. Local 100, 2004 WL 1923760 (S.D.N.Y. Aug. 27, 2004.) (In another decision issued in the case on the same day, the judge refused to recuse herself for remarks about the case made during a continuing legal education seminar.)

Citing Zubulake, Court Shifts 75 Percent of E-Discovery Costs to Plaintiff

Wiginton. CB Richard Ellis, Inc., 2004 WL 1895122 (N.D.Ill. Aug. 10, 2004). In a class action sexual harassment lawsuit, the plaintiff requested the defendant bear the costs of searching 94 backup tapes for relevant emails. The plaintiff based its argument on a sample search of three backup tapes, purportedly containing a large number of relevant documents. The defendant disputed the volume of relevant documents recovered and asserted it should not be responsible for the costs since only a small number of the recovered documents contained relevant data. In conducting its sampling analysis, the plaintiff retained an EDD firm to retrieve relevant emails from three tapes, conduct keyword searches, and load the results into an online review tool. The search resulted in the discovery of 8,660 documents

relating to eight search terms provided by the plaintiff. In analyzing who should bear the costs, the court adopted the seven-factor Zubulake test and added an eighth factor, which required the court to weigh "the importance of the requested discovery in resolving the issues at stake in the litigation."

Balancing these eight factors, the court determined cost-shifting was appropriate and ordered the plaintiff to pay 75 percent of the costs of restoring the backup tapes, searching the data, and transferring it to the online review tool.

CyberControls' Tips

Metadata-Who Cares?

Requesting documents in paper form or in TIFF or PDF formats may not turn out to be as useful to attorneys as one might assume. And while some attorneys have learned to stipulate in their production requests that "...an electronic copy" of specified documents be produced, in most instances, the electronic metadata is vacant.

The importance of metadata depends on the needs of the case. If questions arising from suspicions as to the authenticity of a document, the original authorship, the date of creation, whether multiple revisions were created, or on what computer or external media device was the document saved on are important, then your discovery request needs to be much more definitive.

When a user writes a document with the majority of word processing applications (Microsoft Word® or Word Perfect®) an extensive amount of background information is generated and tagged to the document file called metadata. Most users do not utilize this 'data about data' and so, it remains dormant on the author's original version which is stored on their computer hard drive. REPEAT—the **original** metadata you may be in pursuit of for documents, presentations, spreadsheets, and other compilations are only retrievable from the originator's computer.

Once a responding party makes a copy of the original document from the author's computer onto a CD or floppy diskette for production a new clean slate of metadata accompanies the copy. None of the original metadata is transferred with the production copy.

So, don't be duped by utilizing ineffective definitions in your production

requests. Insist upon the stipulation that all electronic documents and files must be forensically acquired to ensure that all original metadata is preserved in the discovery process. Anything less is less.

Active Data vs. Inactive Data

By now, most attorneys have heard the phrase, "deleted doesn't always mean deleted". So what does that really mean to a litigator?

First, it has no value whatsoever to litigators who conduct their discovery based upon the benevolence factor of their opponent. Active documents and e-mails are those data files that are still alive and easily accessible to those in search of them.

By the mere omission of the term 'inactive' data in a discovery request, the responsive side is off the hook in searching for any relevant documents, e-mails and other data that was deleted sometime in the past.

Even though inactive data is not readily accessible to the producing side, its existence cannot be disputed. In the normal course of everyday business and communications, computer users elect to delete data on their computers on a regular basis.

Once deleted, the data file or e-mail is re-assigned to the un-used hard drive space of the user's computer. These inactive files continue to exist until some time in the future when they are arbitrarily overwritten by newly saved data files.

Experience has shown that inactive files are forensically recoverable even after years of being in a dormant state. This is even true in situations where subject computers have been re-formatted and deployed to new users.

Conclusion: by stipulating that all relevant electronic data including active, inactive, and replicate states in your production request, you will be assured of not overlooking critical elements of evidence that might exist.

E-Mail Secrets

There is little doubt that e-mail has continued to play a leading role in evidentiary support for a multitude of civil cases.

Observers attribute the increased numbers of e-mail with revealing content that turns out to be damaging is a result of the casual attitude that

prevails amongst e-mail authors and recipients. Soon to eclipse conventional e-mail in corporate America is Instant Messaging (IM).

When it comes to e-mail production, in a response to an e-discovery request, the majority of responses are provided in either a TIFF or PDF electronic format. These production efforts are carried out by EDD vendors that specialize in the automated process of extracting active, relevant e-mails that are then converted to the TIFF or PDF format for the requesting party.

The reviewing stage just before the production results are delivered to the requesting party include:

- Attorney/client privilege review
- Work doctrine privilege review
- Privacy review
- Trade Secret review
- Duplicate review and removal

What is the definition by which the producing party and their EDD vendor go by when it relates to duplicates and de-duping the response list of e-mails in production?

In Jack Seward's recent article in American Bankruptcy Institute, "Protecting Yourself Against E-illiteracy: Avoid Being Duped", he asks some challenging questions:

- "Do you understand that the producing party and the EDD vendor may plan to remove from production e-mail and electronic communications they claim are duplicates?"
- Do you understand that if the claimed duplicates are removed, you may not be able to discover "who, what, where and when" about those deduplicated (a.k.a. "de-duped") e-mail and electronic communications?"
- Do you understand that when the claimed duplicates are allowed to be de-duped, only one instance of the e-mail and electronic communications is produced?
- Do you understand that when the claimed duplicates are allowed to be de-duped, all e-mail saved by corporate officers, directors, current employees, past and dismissed employees, workout and turnaround consultants, and those who may have identified the existence of fraud, or made a complaint as a whistleblower on corporate desktop

computers, laptops and removable media, will not be included?

- Do you understand that when the de-dupe is allowed to take place, the possibility of reviewing that e-mail document in the complete context of the e-mail thread is difficult, if not impossible, to interpret?
- Do you understand that the producing party and EDD vendor will claim that providing duplicates and not allowing the EDD vendor to remove them will increase costs of production?
- Do you understand that the producing party claim of increased cost is true, but the reason for the concern by the producing party and the EDD vendor is the inherent risk of having multiple e-mails, including attached files, one coded responsive and the other privileged?
- Do you understand if the producing party and the EDD vendor was allowed to remove the claimed duplicate e-mail, including attached files, the identity of the individual who sent or received the communications will affect the claim of privilege?
- Do you understand that the producing party and EDD vendor does not want to provide e-mail duplicates, including attached files, and electronic files that may be stored on corporate desktop computers, laptops and removable

media used by employees in the ordinary course and that may have been deleted from the corporate back-up media after 90 days under the document retention policy?

- Do you understand that the producing party may have used a 90-day document retention policy improperly and deleted e-mail, including attached files, that would contain important and necessary corporate records, and financial statements, that may not be found on the back-up media may be stored on corporate desktop computers, laptops and removable media used by employees in the ordinary course?
- Do you understand that if the producing party and EDD vendor were allowed to remove claimed duplicate e-mail, including attached files, for electronic communications sent from the same person on the same date and with the same description in the subject line and the same name used for the attached file, that the content may often be dissimilar?"

Jack continues with this approach at scrutinizing all of the permutations of accepted practices employed by the producing party and many EDD vendors, often unbeknownst to the requesting party.

Yes, peeling back the multitude of layers and practices in forensic discovery

requires experience, technical knowledge, and a skeptical disposition. This is reason enough to retain the support services of a computer forensics firm before you accept the approach to production practiced by unknown EDD vendors and your opponents.

Jack's complete article can be downloaded from www.cybercontrols.net in the White Papers section.

Final Words

As autumn surrounds us all with its vibrant colors, our diminished light of day is difficult to adjust to. When it comes to integrating data forensics into your litigation strategy for the first time, it too can seem difficult to adjust to. But, the payoff can be huge and long term. Data forensic discovery is both a strategy and a Following the process that works best for you will eventually become as natural as other processes you've employed. Just be careful not to exclude a consistent persistence in the pursuit of **all** relevant electronic data that your case is entitled to.

Editor.....Robert B. Guinaugh

Technical Editor.....Wolfgang Wilke

Contributing Writers....Jack Seward