



NEW TECHNOLOGIES INC.

The Digital Discoverer

Trends in computer forensics & e-discovery for civil litigators

Who Should Pay for Digital Discovery?



The general rule in civil discovery is that each party pays its own document production costs. Recently, however, legal commentators and burdened parties have attempted to dislodge this rule,

complaining that the enormous growth of digital communications has increased the amount of discoverable information to such a degree that civil discovery is no longer affordable.

Digital discovery can indeed be enormously expensive. In some cases it costs millions of dollars to satisfy document production requests. In a case that formed an early benchmark for assigning electronic discovery costs (*Rowe Entertainment, Inc. v. The William Morris Agency, Inc.* 205 F.R.D. 421 (S.D.N.Y. 2002)), a litigant estimated it would take \$9.75 million to satisfy a single document request. In such cases there may be millions of e-mails, backup tapes, and other responsive material to locate, sort, review and produce. Moreover, high costs are compounded by the fact that in some cases litigants must search offices located across the country or across the world in order to satisfy discovery requests.

Opposing the Old Rule

There has been a movement afoot to topple the old “each party pays its own document production costs” rule, and those

opposing the rule have put forth several cogent arguments in favor of relieving producing parties of the financial burden of production. One argument goes that the exorbitant costs of digital discovery can threaten the financial base of a company even before a determination of liability has been made. Proponents of this stance assert that forcing the producing party to pay is too burdensome given that, in addition to paying the costs to produce documents in readable format, producing parties must also bear the costs to screen producible documents for confidential information. In addition, proponents complain that the ability to request large amounts of information at the expense of the producer is improperly used in some cases to “blackmail” information-rich producing parties into unnaturally early settlements because it is simply cheaper to settle than to produce. Further, in cases where both parties have large amounts of digital information, each party may inflict high costs on the other by issuing burdensome production requests. Some parties may drop out of litigation early because they cannot afford to see the case through. These “wars of attrition” can force some litigants to abandon suits based simply on a cost-benefit analysis, rather than based on merit. Finally, for defendants whose information technology systems are extensive and complex, opponents of the old system argue that it permits unscrupulous litigants to engage in “fishing expeditions” at the expense of their opponent.

Another group of commentators argue that document requesters should bear more of the cost burdens associated with their document requests, based on economic principles. In *Electronic Media Discovery*:

Inside The Digital Discoverer

Inside NTI Pg. 2
Featured Software: NTA Stealth

Ask The Experts Pg. 3
What are some key issues to consider when trying to extract emails for discovery purposes?

Data Reduction: The New Buzz in E-Discovery

The old adage “Be careful what you ask for, because you just might get it” rings especially true for electronic discovery. Clients responding to discovery requests have learned that sending terabytes of information can be a far better evasive maneuver than attempting to resist requests. Conversely, many representing a requesting party in a lawsuit have become gun shy to electronic discovery due to its perceived cost and cumbersome nature.

This is not surprising. A terabyte of electronic data corresponds to approximately 375,000,000 documents. A great deal of that data is unresponsive, to say the least. But how can a firm manually review this much data in a timely or reliable way to winnow out the junk? How can a firm circumvent the need to convert and/or review all this data to ensure compliance with regulations such as HIPPA and Sarbanes Oxley not to mention issues of privilege?

Put simply, it can't.

Some litigation teams have be-

Continued on page 3

The Economic Benefit of Pay-Per-View (Cardozo Law Review), Marnie H. Pulver calls for an amendment to PPPR. He argues for a new rule that requires requesting parties to “pay the [entire] cost for the production of discovery because it will internalize costs.” To understand Pulver’s reasoning, it is necessary to understand the Law and Economics tradition (“LE”) from which it is derived. LE theories tend to favor rules of law that “internalize” costs on decision-makers in order to achieve economic efficiency. The rationale is as follows: Persons are presumed to act or make choices that are always in their self-interest. “Cost-internalization” means that the actor or chooser bears the costs of his actions or choices. “Cost-externalization” means costs of actions or choices are borne by other persons or society as a whole, rather than the chooser. Rational actors/choosers will make more “expensive” choices when they do not have to foot the bill, whereas they will make less expensive choices when they do. Therefore, LE theories generally

hold that costs tend to rise under rules that allow choosers to externalize, while costs tend to fall under rules that force choosers to internalize. Since the goal of LE is to conserve costs (no matter who expends them), it generally supports rules that internalize costs on those who are in a position to control them...those who are responsible for *causing* the costs. If requesting parties are forced to bear the costs of their choice to request documents, they will have incentive to limit discovery requests.

The New Paradigm: Rowe Entertainment

Rules 26 (b) & (c) already give courts the authority to shift costs, and recent cases demonstrate that courts are capable of dealing with the cost burdens of digital discovery in practical, judicious ways. *Rowe Entertainment Inc., v. William Morris Agency Inc.* provides an excellent example. Instead of relying on ideology or inflexible rules, the *Rowe* court took a common sense, mul-

tifactor balancing approach in order to determine whether production costs should be shifted. The court’s approach required that costs be shifted depending on the following considerations:

1. *Specificity Of Discovery Requests:* Are the requests too broad?
2. *Likelihood Of Finding “Critical” Information:* Is there a low probability of a successful search?
3. *Availability From Other Sources:* Is the requested material available from another source at less expense?
4. *Purpose Of Retention:* Was the requested data retained for purposes of ongoing activities?
5. *Benefit To Requesting Party:* Is the requesting party the only party to benefit from the requested production?
6. *Total Costs:* Are the production costs substantial?
7. *Ability And Incentive To Control Costs:* Is the requesting party in a position to control the costs of production?

Continued on page 4

Inside NTI:

In each issue, we feature a key NTI employee or an important NTI technology development. This issue we feature:

NTA Stealth Internet Lead ID Software

NTI has developed Net Threat Analyzer (NTA) Stealth, a powerful new weapon in the fight against dangerous Internet content. The magnitude of unsavory content traveling over the web each day is staggering: 372 million web pages contain pornography are readily accessible, and 2.5 billion pornographic e-mails are sent each day. Over 100,000 websites offer illegal child pornography. Surveys indicate that 20% of men and 13% of women admit to accessing pornography at work. NTA Stealth allows IT administrators to quickly identify what websites a computer user has accessed and what e-mail addresses a computer user has e-mailed. The software relies upon artificial intelligence and processes that are

so unique they are protected by a U.S. patent.

NTA Stealth works like this: computer systems administrators or police officers simply place a floppy disc in the computer’s floppy drive (or a flash memory device into the computer’s USB port), turn the computer on and NTA Stealth will fill the floppy (or flash memory) with a database of 20,000 or more web URLs the computer has accessed. NTA Stealth will add URLs to the floppy or flash memory until the investigator stops the program’s operation or the memory device is full. If the floppy or flash memory fills with URLs, NTA Stealth asks the investigator to place another floppy in the drive or connect a second flash memory device to the USB port so NTA Stealth can continue the investigation. NTA Viewer is companion software to NTA Stealth. This software utility displays and analyzes the results generated by NTA Stealth, giving investigators a statistical frequency of Internet web browsing and e-mail activity. NTA Viewer also creates custom reports and allows investigators to click on URLs of interest. If the investigator’s com-

puter is connected to the Internet and the investigator clicks on a URL revealed by NTA Stealth, NTA Viewer launches the investigator’s Internet browser and directs the browser to the URL of interest.

Details on NTA Stealth are listed on NTI’s website at <http://www.forensics-intl.com/nta.html> and information about NTA Viewer is at <http://www.forensics-intl.com.ntaview.html>.



Continued from page 1

come so frustrated with the burden of reviewing so much electronic data — and so angry at the exorbitant fees they have been charged for file conversion and electronic document database design — that they’ve given up on pursuing electronic discovery altogether. Understandable, but not very practical, as over 90% of business correspondence resides in an electronic format. Instead of throwing the baby out with the proverbial bath water, litigation specialists are finding that there’s a better way to deal with the preponderance of e-discovery: reduce it.

The philosophy behind data reduction is simple and based upon two assumptions:

1) the great majority of electronic discovery is drudge and need not be reviewed at all, and

2) involved parties have some inkling about the nature of material that’s potentially responsive, e.g., they know what individuals might be involved or what sort of file they might be seeking or needing to produce. (email, word processing document).

The challenge, of course, is how to isolate data that might be responsive so it can be easily reviewed without potentially overlooking significant data.

The protocols that computer forensics consultants have developed to locate “hidden” or unknown data can be likewise applied to reducing the universe of discovery data to a more manageable subset. Using forensics software tools, all data can be reviewed in its native file format, obviating the need for costly file conversion prior to review. All data that falls outside the desired parameters, such as duplicate files, machine-created files, and files outside the pertinent date range of the case can be immediately eliminated. Once the original, broad discoverable universe is culled down to only that data which may likely be responsive, basic review and key word searches using any number of litigation support software programs can further isolate potentially responsive material from the megabytes of junk.

Ask The Experts

Addressing frequently asked questions from clients.

In each issue of *The Digital Discoverer*, we address a common question our clients have about computer forensics and digital discovery strategies.

Q: What are some key issues to consider when trying to extract emails for discovery purposes?

A: There are a number of questions that should be answered before you begin to attempt to extract email from a local hard drive or central server. The first and perhaps most obvious question is: What format does the email reside in? Is it Microsoft Outlook, Microsoft Exchange, Lotus Notes, or some customized format? Different programs store data in different configurations, hence different protocols must be used to search data while maintaining its admissibility as evidence. For instance, all email in an Exchange environment is stored in one large file. If you have a

finite list of users whose email correspondence is of interest, you would begin by extracting their email, then search it in its native format for responsiveness, and then produce a PST file containing just the relevant emails, as determined by the presence of key words. This PST file can then be reviewed by your client. Another question that should be addressed up front is ‘where is the email stored?’ Is it stored on a central server, on tape, or locally on individual’s machines. Depending on the timeframe, responsive email may no longer exist on the server/pc in question, and may only exist on tape backups. This will impact the scope of your discovery request.

A third question of significance is ‘how many email users are of interest?’ Many times, an enterprise’s email will be stored on one server or even in one large file. There are certainly ways to extract email by user, but it can be time-intensive. Knowing exactly how many users are of interest can greatly affect the scope and cost of the extraction project.

To give a sense of scope, consider the electronic data on three computers tied to a theft of trade secrets case. This data might total 120 gigabytes of drive space. In the initial data reduction phase, all but 15 gigabytes of user-created files are eliminated from the mix, as outlined above. However, 15 gigabytes is still too much data to be processed manually, and would still be quite expensive to convert and load into a traditional litigation support program, so more forensics methodologies will be used to cull out unresponsive data. Data might first be purged by date range—for example, all emails and other files created outside of the responsive timeframe would be eliminated. Next, data might be purged by file type. In this case example, we have good reason to believe that evidence of theft of trade secrets would reside in either word processing documents or Adobe Acrobat PDF files, so we isolate those files for closer consideration. This short-list of potentially responsive files might then be searched fo-

rensicly by key words, such as product names associated with the case. This phase of data analysis will generally reduce the data universe to several hundred megabytes — not a small amount of data, but much more manageable than the 120 gigabytes you began with. This is the data that might be loaded into a litigation support program for closer review by the litigation team.

By deploying data reduction strategies—using timeline analysis, selective sampling, and similar techniques — a litigation team takes an intelligent approach to coping with large amounts of electronic discovery. By reducing the universe of electronic data to a manageable magnitude through an informed culling process, the litigation team achieves two important objectives: 1) they harness the power of potentially responsive information, and 2) they do so for a fraction of the cost of processing the data through conventional scanning/conversion methods.

Continued from page 2

8. *Resources Of Each Party*: Do the resources of each party suggest that the requesting party should pay?

The more these questions have answers in the affirmative, the more appropriate it is to shift production costs to the requesting party.

The New New Paradigm: Zubulake

But wait! Just when it seemed that the 8-factor test established in *Rowe* was beginning to gain traction, a new case materialized on the horizon. In *Zubulake v UBS Warburg* (S.D.N.Y.), Laura Zubulake sued UBS Warburg LLC, UBS Warburg, and UBS AG, alleging gender discrimination and illegal retaliation. The plaintiff contended that key evidence was contained in various emails exchanged among UBS employees which subsequently existed only on backup tapes and perhaps other archived media. She requested that the defendant produce “[a]ll documents concerning any communication by or between UBS employees concerning plaintiff.” When the defendant produced only 350 pages of documents, the plaintiff, having already produced 450 pages of emails alone, requested that the defendants produce the email from archival media. The defendant, citing *Rowe*, asked the court to shift the cost of production – estimated at \$175,000 – to the plaintiff. Zubulake filed a motion to compel UBS to provide these emails. Noting that the 8 factors cited in *Rowe* might result in disproportionate cost shifting away from large defendants, Judge Shira A. Scheindlin set forth a new 7-factor test for cost analysis, drawing from *Rowe* and *McPeck v.*

Ashcroft. Judge Scheindlin is explicit that the factors should be weighted according to 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.

“Just when it seemed that the 8-factor test established in *Rowe* was beginning to gain traction, a new case materialized on the horizon.”

6. The importance of the issues at stake in the litigation.
7. The relative benefits to the parties of obtaining the information.

In the order handed down, Judge Scheindlin emphasized the need for parties to be fully informed of the technology and cost issues and confirmed that the test employed is a qualitative one in which all relevant factors must be considered in resolving issues on allocating costs and determining whether and how the presumption that the producing party pays should be altered. The presumption is still that the producer pays, especially in situations where data is considered accessible.

Zubulake...Again

Before the dust had settled on what’s come to be called *Zubulake I*, an order was handed down that casts new light on the cost-shifting argument. On July 24th, in what’s termed “*Zubulake III*,” Judge Scheindlin ordered that the plaintiff share in the costs of the restoration of back-up tapes. This order was handed down in response to a motion that the defendant had filed requesting the court to shift these costs to Zubulake if restoration of additional backup tapes was ordered. The motion advised the court that it had processed a sampling of five back-up tapes (from a total of 94) for responsive emails at a cost of \$19,003.43, and that it estimated the cost of processing remaining back-up tapes would be \$273,649.39 (\$165,954.67 in restoration costs and \$107,694.72 in review costs). In considering the motion, the court applied the 7-factor test it had established in *Zubulake I*. The court felt that factors 1, 2 and 3 weighed slightly against cost-shifting, that factors 5 and 6 had no bearing, and that application of factor 4 would not rule out cost-shifting. However, the court felt that factor 7 was in favor of cost-shifting, as it was clear that the plaintiff would stand to gain much more from discovery of the backup information than the defendant.

With the case still in progress, it’s quite possible that further precedents could be established (in October, *Zubulake IV* had implications for spoliation). In the short run, it seems that the impact of *Zubulake III* will be that defendants will still be required to assume the costs of review of information, once it is deemed to be in “accessible” format.

New Technologies, Inc., a wholly-owned subsidiary of Armor Holdings, Inc. (NYSE:AH), provides digital document discovery services, primarily through computer forensics, to civil litigators. Working with litigation team members as partners we:

- Use forensic processes to cost-effectively manage electronic discovery efforts.
- Consult with you to determine what electronic information is valuable to a case, and how to get it in admissible format.
- Use various forensics procedures (with software tools we’ve developed) to find evidence on computer hard drives and other storage media.

Contact Us At:

Tel: 503-661-6912

E-mail: info@dataforensics.com

Web: www.dataforensics.com



NEW TECHNOLOGIES INC.