Remote Forensics May Bring the Next Sea Change in E-discovery: Are All Networked Computers Now Readily Accessible Under the Revised Federal Rules of Civil Procedure?[1]

Joseph J. Schwerha IV, M.S., J.D.
California University of Pennsylvania
TraceEvidence, LLC
schwerhaiv@yahoo.com

Scott Inch, Ph.D
Bloomsburg University
sinch@bloomu.edu

Abstract

The recent amendments to Rule 26 of the Federal Rules of Civil Procedure created a two-tiered approach to discovery of electronically stored information ("ESI").[2] Responding parties must produce ESI that is relevant, not subject to privilege, and reasonably accessible.[3] However, because some methods of storing ESI, such as on magnetic backup tapes and within enormous databases, require substantial cost to access and search their contents, the rules permit parties to designate those repositories as "not reasonably accessible" because of undue burden or cost.[4] But even despite the difficulty in searching for ESI, the party's duty to preserve potentially responsive evidence remains; it simply gains the option to forgo poring over the material.[5] Further, the court might nevertheless compel production if the requesting party demonstrates good cause.[6]

Regardless of whether the responding party believes certain documents to be reasonably accessible or not, courts may still require their production. In such cases, the court may then choose to order production, but shift the costs of doing so to the requesting party. Throughout this process, the burden and cost of production are central themes. Their determination is fluid, varying from

[1] We must give special thanks to Mr. Schwerha's research assistant, Mr. Christopher Kovach. He helped with research and initially drafted parts of our article. His efforts and expertise were invaluable.

[2] FED. R. CIV. P. 26(b)(2)(B).

[3] *Id*.

[4] *Id*.

[5] FED. R. CIV. P. 26(b)(2)(B), Advisory Committee Note of 2006.

[6] FED. R. CIV. P. 26(b)(2)(B).

case to case and even over time in the same situation. Nowhere is this more evident than where a responding party has numerous, geographically dispersed computers under its control that may contain responsive ESI to a request for production of documents. Traditionally, a responding party would be forced to make a decision of whether or not to send out computer forensic experts to all of these locations to make forensically sound copies of all of those computers and then analyze each. This process is time consuming and costly. Recently, several companies have put forth substantial solutions that facially allow a responding party to capture and analyze data on geographically dispersed computers remotely. That process, in general, is often defined as remote forensics.

The question is now whether newly available remote forensic solution indicate that all networked computers are readily accessible under the current state of the law. This article attempts to define remote forensics, examines a selection of applicable court decisions, and then analyzes the currently available commercial software packages that allow remote forensics.

1. REMOTE FORENSICS

In small companies, where all hardware and software is local, evidence acquisition is a relatively simple process. IT staff arrives on scene, removes the physical hard disk and images it in any number of ways. In mission critical situations, the hard disk could be cloned and the duplicate hard disk could be put back into the machine (often without the employee's knowledge) while the original disk is taken for examination.

In a large corporation with offices in many locations, the acquisition model is much different. Decisions are impacted by budget and personnel. A company may not be able to afford to send a seasoned IT person to a remote location to do the acquisition. While gone, the centrally located IT staff is short handed and the company has to pay for travel expenses which can be substantial depending on the location and duration of the acquisition. If repeated, this process can be quite troublesome.

The idea of remote forensics is to allow the IT personnel to forensically examine any computer in the company network without being physically present at its location. The challenge is to do this in a forensically sound manner so the evidence collected could be submitted in court.[7] In general, remote forensic processes are less sound as they typically involve a running machine, sometimes being used by the employee at the time the evidence is being collected. Typical capabilities are previewing the target computer (see files and processes), performing keyword searches, capturing a physical

[7] In order to be submitted in court, the evidence must be authentic – that is – exactly what the proponent claims it is. If the evidence has been significantly altered, then it generally would not be authentic and in many cases would not be allowed in court.

memory dump, and acquiring a forensic copy of the remote hard disk.

Very large companies may purchase and deploy a large scale enterprise-wide solution with the expectation that they will repeatedly have to perform such investigations. These solutions can be very expensive but often save the company money in the long term. Solutions such as these often have other benefits in addition to their forensics capabilities such as security and compliance auditing. However, the cost and installation process has put them well beyond the reach of many small to mid-sized companies. Smaller companies likely do not have the need or budget to invest in an enterprise-wide software solution. They are more likely to choose a smaller tool that would allow installation after an incident has occurred.

The need for a viable remote forensic solution is not new; but, the increase in networking of geographically dispersed computers has greatly increased this need in recent years.[8] In December, 2006, the Federal Rules of Civil Procedure were modified with regard to electronic discovery, forcing judges and attorneys to address the issue.

2. DEFINING "REASONABLY ACCESSIBLE"

Anticipating the changing nature of technology and the disparity in resources among different parties, the rules only define "not reasonably accessible" in terms of burden and cost.[9] Hence the rules ignore technological issues and focus instead on only economic concerns. Because of this, parties may identify for themselves what they consider to be not reasonably accessible, given their own means and opportunity. Preliminary discovery may be needed to determine whether a party's claim is justifiable.

Despite the seemingly wide-open definition of reasonably accessible, some guidelines exist, based primarily on the manner in which data is stored.[10] Explicit examples offered by the advisory committee include "back-up tapes intended for disaster recovery purposes," "legacy data that was 'deleted' but remains in fragmented form, requiring a modern version of forensics to restore and retrieve," and "databases that were designed to create certain information in certain ways and cannot readily create very different kinds or forms of information."[11] In the seminal case of Zubulake v. UBS Warburg LLC, Judge Scheindlin identified five categories of data:

[8] Pencock, Smith & Wilson, *Design and Implementation of a Remote Forensics System, Information Networking Institute,* Carnegie Mellon University (May, 2005) (http://www.foundstone.com/us/resources/whitepapers/remote_forensics_systems.pdf)

[9] J.M. Moore, Moore's Federal Practice § 26.53[1] (3d ed. 2005).

[10] *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

[11] Memorandum from Hon. Lee H. Rosenthal, Chair, Advisory Committee on the Federal Rules of Civil Procedure to Hon. David F. Levi, Chair, Standing Committee on Rules of Practice and Procedure 34 (May 27, 2005), *available at* http://www.uscourts.gov/rules/supct1105/Excerpt_CV_Report.pdf.

1. Active, online data: "On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life . . . Examples of online data include hard drives.
2. Near-line data: "This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. . . . Examples include optical disks.
3. Offline storage/archives: "This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speed may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility. . .”
4. Backup tapes: "A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably. . . The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks." . . . Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.
5. Erased, fragmented or damaged data: "When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters. . . As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk." Such broken-up files are said to be "fragmented," and along with damaged and erased data can only be accessed after significant processing.

Judge Scheindlin categorized the first three types as accessible and the final two as inaccessible, noting that accessible data is “stored in a readily usable format . . . [and] does not need to be restored or otherwise manipulated to be usable."[12] On the other hand, inaccessible data is not readily usable: backup tapes, fragmented data, and deleted files need to be restored, defragmented, and undeleted.[13] The key difference is the amount of effort needed to access raw data and reconstruct relevant information. The more burdensome and time consuming it is to retrieve information, the more likely courts would characterize the data as not reasonably accessible.

These hurdles can exist in the form of "acquiring or creating software to retrieve potentially responsive electronic data or otherwise require the responding party to render inaccessible electronic information accessible."[14] This seems to suggest that parties must rely upon software programs and other tools within their control, or usable at little to no additional cost, but notably refrains from imposing any sort of state of the art standard. However, it also hints at a minimum level of compliance, intimating that *some* standards exist, and *not* meeting them would never render data inaccessible.[15]

3. RECENT COURT CASES

But no explicit rule exists.[16] Since the amendments to the Federal Rules, magistrate and district justices have looked to the circumstances of each individual case in determining whether information is not reasonably accessible. Precedent currently remains relatively sparse.

The following cases, nevertheless help shed light on the current workable definition of Rule 26(b)(2)(B). In these cases, the measure of accessibility was primarily calculated based upon the cost of producing the data in question, and the courts allocation of the costs would generally encourage organizations to store data in reasonably accessible formats. Remote forensic tools make it cheaper and easier to access a broad range of information on computer networks, reducing the burden on producing parties.

[12] Zubulake, 217 F.R.D. at 320.

[13] *Id*.

[14] American Bar Association Civil Discovery Standards § IV.10 at 59-60 (August 2004), http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf.

[15] *See* Static Control Components, Inc. v. Lexmark Int'l, Inc., No. A. 04-84, 2006 U.S. Dist. LEXIS 16662, *19-20 (E.D. Ky. Apr. 5, 2006) (noting that a "peculiar computer system" is no excuse for non-production); CP Solutions PTE, Ltd. v. Gen. Elec. Co., No. 04-2150, 2006 U.S. Dist. LEXIS 27053, *14 (D. Conn. Feb. 6, 2006) (stating that, despite the fact that email attachments were "created with different software programs," there is no excuse for producing "emails and attachments in a jumbled, disorganized fashion.").

[16] *See, e.g.*, Best Buy Stores, L.P. v. Developers Diversified Realty Corp., No. 05-2310, 2007 U.S. Dist. LEXIS 7580, *2-3 (D. Minn. Feb. 1, 2007) (holding that defendants had failed to prove that information stored on backup tapes was not reasonably accessible).

3.1 Quinby v. WestLB AG[17]

In this sexual harassment suit, plaintiff moved for sanctions against defendant arising out of a dispute concerning discovery of emails in defendant's possession. Plaintiff requested that seventeen current and former WestLB employees' email accounts be searched for "certain terms alleged to refer to plaintiff in particular or that are sexist in general."[18] Defendant claimed the request was overly broad and amounted to an undue burden. The magistrate judge referred both parties to Zubulake v. UBS Warburg LLC[19] and ordered affidavits addressing its cost-shifting factors.[20] Defendant was also ordered to "restore, as a sample, the back-up tape or tapes that contain emails from February 2003 into a readable, searchable format."[21] Defendant created "daily back-up tapes, consisting of about twenty to forty tapes . . . [and] stores daily back-up tapes for fifteen weeks and then recycles the tapes. Similarly, monthly tapes are stored for thirteen months before they are recycled and annual tapes for two years."[22]

Although the case predates the amendments, it is nevertheless notable because of its references to *Zubulake* and the conclusion that backup tapes were the "most complete source for the emails and retrieving the emails from any other source would have resulted in either an incomplete production or duplication of effort."[23] Additionally, the judge declared that archiving data onto back-up tapes makes that data inaccessible.[24] Further, defendants could not be sanctioned for choosing to preserve data on backup tapes; that practice satisfies the preservation obligation, even if it renders data inaccessible.[25]

In later proceedings, the judge stated the position that "cost-shifting is only appropriate where electronic discovery imposes an undue burden or expense," but also added that "if a party creates its own burden or expense by converting into an inaccessible format data that it should have reasonably foreseen would be discoverable material at a time when it should have anticipated litigation,

[17] Quinby v. WestLB AG, No. 04-7406, 2005 U.S. Dist. LEXIS 35583 (S.D.N.Y. Dec. 15, 2005).

[18] *Id*. at *2.

[19] 217 F.R.D. 309 (S.D.N.Y. 2003).

[20] *Id*. at 322 (creating a new seven-factor test to determine whether cost-shifting is appropriate; the seven factors are: (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.)

[21] Quinby, 2005 U.S. Dist. LEXIS 35583, at *4.

[22] *Id*. at *23.

[23] *Id*. at *18.

[24] *Id*. at *26.

[25] *Id*. at *27 n. 10.

then it should not be entitled to shift the costs of restoring and searching the data."[26] He reiterated, however, that backup tapes, at least in this situation, are *not* reasonably accessible – and noted that cost-shifting is a useful tool to encourage parties to store data in readily accessible formats.[27]

3.2 Static Control Components, Inc. v. Lexmark Int'l, Inc.[28]

SCC filed a declaratory judgment action against Lexmark, seeking a judgment that its off-brand ink cartridges did not violate the Digital Millennium Copyright Act. Lexmark disagreed and filed numerous counterclaims. SCC moved for an order compelling Lexmark to respond to a series of Requests for Production of Documents, including records comprising Lexmark's "pre-sale customer inquiry database."[29] Prior to June 30, 2004, Lexmark allegedly told SCC that as many as 60,000 records in that database could be responsive to its document requests; however, Lexmark refused to produce the database, citing an undue burden.[30]

Lexmark explained that it "maintained its pre-sale customer inquiry database: (a) in a form that is not text-searchable; (b) using software that is no longer commercially available; and (c) software which it modified for its own use."[31] Therefore, according to Lexmark, the information was not reasonably accessible, even though it offered on three separate occasions to make its database available to SCC under limited conditions – namely, at Lexmark's facilities. SCC replied that Lexmark's terms are unacceptable, "chiefly because Lexmark represents that the only way to retrieve information from this database is by inputting a specific caller's name, phone number, or call reference number (which is an internal designation created by Lexmark.)"[32] In other words, SCC thought the process would be pointless.

The magistrate judge agreed, holding that Lexmark must produce its database in a "reasonably usable form," and that it cannot "hide behind its peculiar computer system as an excuse" for non-production.[33] Because of the proprietary nature of Lexmark's database, the judge categorized the information as "Outside Counsel Only," to be produced under a protective order governing discovery in the case.[34]

[26] Quinby v. WestLB AG, No. 04-7406, 2006 U.S. Dist. LEXIS 64531, *29 (S.D.N.Y. Sep. 5. 2006).

[27] *Id*.

[28] Static Control Components, Inc. v. Lexmark Int'l, Inc., No. 04-84-KSF, 2006 U.S. Dist. LEXIS 16662 (E.D. Ky. Apr. 5, 2006).

[29] *Id*. at *15.

[30] *Id*. at *16-17.

[31] *Id*. at *18.

[32] *Id*. at *19 (internal quotations omitted).

[33] *Id*.

[34] *Id*.

3.3 Semsroth v. City of Wichita[35]

Plaintiffs, former police officers, sued the defendant city and police department and alleged sexual and gender discrimination. They requested copies of emails from supervisors; the emails existed in current active user files and on a backup tape.[36] Because the active files would not show deleted emails, the officers requested production of the backup tape, which the city would need to restore to an email server, since it keeps backups for disaster recovery purposes only.[37] No dispute exists to the relevance of the material; the crux of the dispute is who will bear the costs.

Plaintiffs argued that the cost should be borne by the producing party, and that the expenditure of these costs cannot constitute an "undue burden." The city responded that plaintiffs should cover some of the costs, because "it would not buy [search] software absent an order of the Court, there is no evidence that the search of the back-up tape will even find any of the words identified by Plaintiffs for use in a search, and the burden of compliance with Plaintiffs' requested discovery would be . . . undue."[38] The magistrate judge noted that, under amended rule 26(b)(2)(B), the burden of establishing that information is not reasonably accessible falls on the city; and that plaintiffs can, despite that undue burden, obtain discovery by showing good cause.[39]

Plaintiffs alleged that the city's choice of backup tapes should warrant denying its motion out of hand. The judge disagreed, finding that the tapes were a reasonable storage method, and distinguished it from *Quinby*, where defendant converted data into an inaccessible format when it should have reasonably expected litigation.[40]

Importantly, the judge distinguished *mediums* that might be considered "inaccessible" under the definition of the rule and whether an undue burden or cost exists. The amendment made clear that "any inaccessibility" *must* be due to an undue burden or cost; he rejected the idea of blanket exceptions into the rule, even for traditionally inaccessible mediums like backup tapes.[41] Here, the cost to the city would amount to $3,374.95.[42] Ultimately, the judge held that the cost to the city was of restoring the single backup tape at issue did not amount to an undue burden or cost.[43] And because the emails were reasonably accessible, the cost-shifting factors outlined in Rule 26(b)(2)(C) were not

[35] Semsroth v. City of Wichita, 239 F.R.D. 630 (D. Kan. 2006).
[36] *Id*. at 632.
[37] *Id*.
[38] *Id*. at 633.
[39] *Id*. at 634.
[40] *Id*. at 635 n.5.
[41] *Id*. at 637.
[42] *Id*. at 638.
[43] *Id*. at 640.

implicated.[44] But had the cost of restoring the tape been greater, the court noted that cost-shifting "would easily have supported a shifting of some of the costs to the Plaintiffs."[45]

3.4 Ameriwood Indus., Inc. v. Liberman[46]

Plaintiff alleged that defendants, while employed by plaintiffs, used confidential information to sabotage plaintiff's business relationships and steal clients. Defendants cited poor business management on the part of plaintiff. Plaintiff moved to compel defendants' compliance with its document requests and interrogatories. Included was a request for production of "a mirror image of all computers used by any defendant to conduct business on his own behalf or on behalf of plaintiff . . . including defendants' personal home computers . . ."[47] Plaintiff asserted that defendants forwarded customer information, trade secrets, and account information to their personal email accounts; it also guessed that defendants concealed their actions. Plaintiff filed with the court an email sent from defendant, while still employed by plaintiff, to an employee at Samsung. Because of this, the court found that other relevant emails may still exist on defendants' computers.[48]

However, because defendants submitted affidavits describing the "significant costs of copying the hard drives, recovering deleted information, and translating the recovered data into searchable and reviewable formats," the court concluded that the information was not readily accessible because of undue burden or cost.[49] Despite this, the court nevertheless found that plaintiff had shown good cause to obtain mirror images; it crafted a three-step "imaging, recovery, and disclosure process [that] provides the requesting party sufficient access to information that is not reasonably accessible and ensures the process does not place an undue burden or cost on the responding party."[50]

In a later proceeding, defendant requested all internal emails pertaining to plaintiff's business and its management from October 2005 through March 2006. The request identified six people that may possess responsive documents – who plaintiff identified as having 52,124 potentially responsive emails and 4,413 document files. The court found the information not reasonably accessible because of undue burden or cost, and further held that defendants failed to show good cause to order disclosure.[51]

[44] *Id*.

[45] *Id*.

[46] Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524-DJS, 2006 U.S. Dist. LEXIS 93380 (E.D. Mo. Dec. 27, 2006).

[47] *Id*. at *4-5.

[48] *Id*. at *10-11.

[49] *Id*. at *12-13.

[50] *Id*. at *15.

[51] Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524-DJS, 2007 U.S. Dist. LEXIS 10791

3.5 Cenveo Corp. v. Slater[52]

In a case similar to *Ameriwood*, plaintiff alleged that its former employees misappropriated trade secrets and confidential information. Plaintiff sought to use a mirror imaging method to access defendants' hard drives, whereby the image would be turned over to a third-party forensics expert for analysis; it asked defendants for a privilege log as well. On the other hand, defendants offered to produce the image themselves and use plaintiff's search terms.[53]

Because of the interplay between plaintiff's claims and defendants' computers, the court granted plaintiff's request to select an expert to oversee the imaging process.[54] The court found that plaintiff's interest in obtaining the information outweighed defendants' burden in producing it, obviating the need to show good cause to compel production.[55] Notably, the court found *Ameriwood* instructive and created a three-part imaging, recovery and disclosure process.[56]

3.6 Hedenburg v. Aramark American Food Services.[57]

In this run of the mill employment discrimination and wrongful termination case, defendant employer sought a "mirror image" of plaintiff's home computer hard drive, arguing that access to such computers is common and normal in employment cases; defendant offered to have the hard drive sent to a "special master" to avoid recovery of non-discoverable information.

The court rejected defendant's motion to compel discovery, calling it a "fishing expedition," noting that a "thorough search of an adversary's computer is sometimes permitted where the contents of the computer go to the heart of the case."[58] Here, plaintiff claims that she went through her files and found nothing, so defendant lacks the good cause necessary under 26(b)(2)(b) to investigate. The gist of cases like this is that, in some cases, parties from whom discovery is being sought may *not* have to prove their information is not readily accessible – provided that the request is obviously a fishing expedition. In other words, some courts seem comfortable requiring that the requesting party establish good cause before turning to the question of accessibility. (Or perhaps the "undue burden" and "good cause" inquiries are sometimes conflated.)

(E.D. Mo. Feb. 12, 2007).

[52] Cenveo Corp. v. Slater, No. 06-CV-2632, 2007 U.S. Dist. LEXIS 8281 (E.D. Pa. Jan. 31, 2007).

[53] *Id*. at *2.

[54] *Id*. at *4.

[55] *Id*.

[56] *Id*. at *5.

[57] Hedenburg v. Aramark Am. Food Services, No. C06-5267 RBL, 2007 U.S. Dist. LEXIS 3343 (W.D. Wash. Jan. 17, 2007).

[58] *Id*. at *3.

3.7 Best Buy Stores, L.P. v. Developers Diversified Realty Corp.[59]

Defendants objected to the magistrate judge's granting of plaintiff's motion to compel defendants to produce documents. The magistrate judge "rejected defendants' conclusory statements that compliance with their electronic discovery obligations . . . is cost prohibitive," even though the documents were stored on backup tapes.[60] Nor had defendants "met their burden to establish that the information sought 'is not reasonably accessible because of undue burden or cost.'"[61]

In the case before the district court, defendants' expert provided cost estimates for recovering the information stored on backup tapes and requested a deadline for those files that were not readily available. Plaintiff opposed the modification. The court found that "a modification of the deadline might be warranted if compliance with the deadline is in fact technologically impossible," but affirmed the magistrate judge's order in all respects, including her refusal to automatically define backup tapes as not readily accessible.[62]

3.8 Peskoff v. Faber[63]

Plaintiff sought to recover damages from defendant's venture capital fund, alleging fraud in the inducement, breach of fiduciary duty, and other related causes of action. Pursuant to an earlier order to compel, defendant searched computer systems and produced relevant emails; however, at issue is plaintiff's contention that more emails exist and have not been produced.[64] The magistrate judge found the search inadequate:

> All of the unopened emails in the Inbox--a total of fourteen--are dated the same day, a date following plaintiff's departure . . . The 10,436 emails in the "Old Mail" subfolder are all unopened. The emails in the "Old Mail" subfolder are for the period June 25, 2003, to April 14, 2004, but the emails in the 65 other subfolders are all dated for the period June 2000 to June 2001. Thus, there are gaps of several years among the various subfolders with no emails whatsoever during these time periods. While there may be reasons why this is so, on this record all one can say is that this phenomenon is inexplicable.[65]

The judge stated that parties are relieved of producing information not reasonably accessible, and if good cause is shown, discovery may be ordered and cost-shifting taken into consideration; however, he noted the negative

[59] Best Buy Stores, L.P. v. Developers Diversified Realty Corp., No. 05-2310, 2007 U.S. Dist. LEXIS 7580 (D. Minn. Feb. 1, 2007).

[60] *Id*. at *2.

[61] *Id.* (quoting FED. R. CIV. P. 26(b)(2)(B)).

[62] *Id*. at *3-4.

[63] Peskoff v. Faber, 240 F.R.D. 26 (D.D.C. 2007).

[64] *Id*. at 28.

[65] *Id*. at 30.

corollary: "*accessible* data must be produced at the cost of the producing party."[66] Because of this, the judge ordered defendant to conduct an additional search at his own expense.[67]

3.9 EEOC v. Boeing Co.[68]

Defendant designated prior testimony instead of live witnesses as responsive to topics in plaintiff's Rule 30(b)(6) deposition. Plaintiff moved for an order to compel live witness testimony. Through one of the topics at issue, plaintiff sought to discover all bases for defendant's claim that the retrieval of emails responsive to plaintiff's request for production of documents would cost at least $55,000.[69]

The court noted that, in its earlier opinion, it had "no reason to doubt" defendant's cost estimate, and that plaintiff had not shown good cause to justify the discovery. Here, plaintiff did not claim that defendant's cost estimate is relevant to its case; it simply wanted to know how the number was calculated. The court held that plaintiff cannot raise an issue that "it should have raised in its earlier motions to compel," and denied that portion of its motion.[70]

3.10 Wells v. Xpedx[71]

Plaintiff moved to compel discovery of emails of seven of defendant's employees during various time periods in the years 2002 and 2003. Plaintiff further contended that defendant implemented a new email deletion policy in 2003, with emails being deleted after 90 days unless marked for retention. However, under this policy, automatically deleted emails could not be restored without the consent of defendant's legal department. Moreover, plaintiff argued that defendant's archives, "legal hold" folders, and backup systems might contain the emails in question – and that corporate representatives could help him determine whether the emails still exist.

Defendant stated it produced all relevant emails and that, because of the policy, any emails not marked for retention were deleted after 90 days.

However, the court noted that "[d]eleted emails are, in most cases, not irretrievably lost."[72] And the producing party has the *obligation* to "search available electronic systems for deleted emails and files."[73] The court stated

[66] *Id*. at 31.
[67] *Id*.
[68] EEOC v. Boeing Co., No. CV-05-03034-PHX-FJM, 2007 U.S. Dist. LEXIS 29107 (D. Ariz. Apr. 17, 2007).
[69] *Id*. at *7.
[70] *Id*. at *8.
[71] Wells v. Xpedx, No. 8:05-CV-2193-T-EAJ, 2007 U.S. Dist. LEXIS 29610 (M.D. Fla. Apr. 23, 2007).
[72] *Id*. at *3 (internal quotations omitted).
[73] *Id*. (quoting Peskoff v. Faber, 20 F.R.D. 26 (D.D.C. 2007)).

that it lacked sufficient information to determine whether defendant produced all responsive emails; it ordered the parties to confer in good faith concerning the matter and deferred ruling on the motion to compel discovery.

No subsequent history concerned ESI, so presumably the parties agreed – however, this case is notable because email retention policies do not, in and of themselves, trump electronic discovery rules, because even deleted emails might still exist. Thus, a policy that truly did delete emails after a specified amount of time (for example, by not retaining them in backup servers) might serve a party best, for otherwise, the information could be deemed reasonably accessible.

3.11 Columbia Pictures, Inc. v. Bunnell [74]

In this case, one relevant question was at issue: is a computer's random access memory (RAM) subject to discovery under Rule 34? The court, despite acknowledging that RAM is temporary at best, holds that RAM is ESI under the circumstances of the case. Much of their argument rests on the definition of the word "stored" – noting that RAM, by definition, stores data and that Rule 34 is, by definition, a broad rule meant to encompass all kinds of data.

After the litany of semantic arguments, the court cited a Ninth Circuit case from 1993 dealing with copyright infringement which held that information stored in RAM satisfies the Copyright Act's statutory prerequisites," namely that "the medium store information with a degree of permanence and for 'more than a transitory duration'."[75]

The importance of the trend to find information stored in RAM discoverable cannot be overstated – although one could make a solid argument that anything stored in RAM is not reasonably accessible, courts can still compel production of inaccessible records (regardless of how costly production may be) upon a showing of good cause. In some cases, these costs can be relatively astronomical.[76]

3.12 Garcia v. Berkshire Life Ins. Co. of America [77]

In this disability claim case, plaintiff sued defendant insurance company, claiming that she was totally disabled. The insurance company learned that plaintiff actually attended college, law school, and graduate school and wanted to determine whether she was actually disabled. It requested plaintiff's emails from her university, and the university in turn sent the emails to plaintiff's

[74] Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007).

[75] *Id.* at 447-48 (quoting Mai Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 517-18 (9th Cir. 1993)).

[76] *See, e.g.*, Kentucky Speedway, LLC v. NASCAR, 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. Dec. 18, 2006) (discovery costs amounted to $3M USD in five months).

[77] Garcia v. Berkshire Life Ins. Co. of Am., 2007 U.S. Dist. LEXIS 86639 (D. Colo. Nov. 13, 2007).

counsel, who reviewed the documents. But there was a large discrepancy between what the university sent to plaintiff's lawyer and what the lawyer produced to the insurance company – plaintiff submitted 10 emails and a privilege log with 135 other emails; the DVD on which the emails were burned contained 4,000 emails with 1,500 attachments.

Plaintiff's counsel persisted; the insurance company moved to compel discovery. In response to that motion, plaintiff's counsel (still persisting) doubted that other emails existed and cited computer illiteracy as his reason. In essence, this fell under a 26(b)(2)(B) claim, since the emails were presumably not reasonably accessible to plaintiff or her lawyer. The court summarily rejected that argument and compelled discovery, noting that plaintiff was "on notice" when defense counsel notified her of the problems with the DVD. However, the court *does* suggest that good faith technical ignorance might excuse the attorney's initial dealings – but good faith mistakes can only go so far.

3.13 Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority[78]

This suit involved a claim that the Defendant failed to provide adequate transportation services to disabled persons.[79] In section III of the opinion, the Court addressed the Defendant's failure to preserve electronically stored information, as well as the Defendant's claim that certain ESI in its possession was not readily accessible.

Plaintiff had moved the court to compel the Defendant to produce backup tapes of certain electronic documents that the Defendant had produced since the litigation had started. Though the Complaint had been filed on March 25, 2004, the Defendant allegedly did nothing to implement a litigation hold until June, 2006. In the meantime the Defendants had failed to implement a litigation hold and allowed routine deletion of emails after 60 days, despite the fact that litigation had actually commenced. The court chastised the Defendants and then considered the Plaintiff's request to force the Defendant to search its backup tapes for any information that had been deleted. [80] The Plaintiff argued that the Defendant should restore the monthly backup tapes to a searchable database. The Defendants resisted on the principles of burden and expense.[81] The court noted that it was hesitant to permit a party who obviously failed to preserve evidence argue that the remaining evidence is inaccessible.[82] Nevertheless, the court skipped the analysis of accessibility, and merely ruled

[78] Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority, 2007 U.S. Dist. LEXIS 39605 (D.D.C., June 1, 2007)

[79] Disability Rights, 2007 U.S. Dist. LEXIS 39605 *1 (D.D.C., June 1, 2007)

[80] Id. at *24.

[81] Id. at *25.

[82] Id. at *26.

that that there was good cause to order production under Federal Rule of Civil Procedure 26(b)(2)(C).[83]

3.14 Petcou v. C.H. Robinson Worldwide, Inc.[84]

This was an employment discrimination case where the Plaintiff was requesting emails from 1998 through 2006, including deleted emails. To comply with same, the Defendant was going to have to restore and search backup tapes. The Plaintiff wanted 5,300 employees' email searched. However, the respondent argued that those tapes were not reasonably accessible due to burden and cost.[85]

The Defendant argued that in order to comply with the Plaintiff's request it would have to restore numerous backup tapes at a cost of $325 - $365 per tape. [86] The total for each employee was going to be $79,300.[87] The court then found that the producer met its burden of proving that the emails were not reasonably accessible.

The court then undertook determination of whether good cause was demonstrated in consideration of rule 26(b)(2)(B). Upon considering the arguments from both sides, the court ruled that there was not good cause, reasoning that "the costs of searching the tapes would outweigh the benefits."[88]

Defining the words "reasonably accessible" remains unclear; the legal landscape is still chaotic, although some courts, like the Southern District of New York, seem more likely than others to rule on certain forms of information. But despite this uncertainty, common themes have emerged: whenever a party objects to discovery on the basis of information being not reasonably accessible, it must support that argument with sufficient evidence.[89] Boilerplate language and conclusory statements, like the kind used by defendants in *Best Buy*, who likely assumed that backup tapes were always inaccessible, are rarely accepted. Courts, becoming increasingly technically savvy (or at least economically conversant) want cost-benefit analyses; this means that parties without the benefit of experts to conduct these analyses, like individual plaintiffs, may face difficulty.

[83] The reader might also want to consider Benton v. Dlorah, Inc. 2007 U.S. Dist. LEXIS 80503 (D. Kan. Oct. 30, 2007). In that case, upon consideration of a motion to compel production of deleted emails, the court ordered same, stating: "Deleted documents should be retrievable from her computer system and [thereby] remain within her control." Id. at 7. It is important because the court essentially decided that deleted emails were reasonably accessible.

[84] Petcou v. C.H. Robinson Worldwide, Inc., 2008 U.S. Dist. LEXIS 13723 (N.D. Ga. Feb, 2008)

[85] Petcou, 2008 U.S. Dist. LEXIS 13723 *2.

[86] Id.

[87] Id.

[88] Id. at * 3.

[89] *See* O'Bar v. Lowe's Home Ctrs., Inc., No. 5:04-CV-00019-W, 2007 U.S. Dist. LEXIS 32497, *23 n.6 (W.D.N.C. May 2, 2007).

Producing parties should have solid numbers ready – and must be able to argue effectively that such numbers pose an undue burden. However, the argument must be kept in context, taking into consideration not only the amount in controversy but also the parties' assets – $55,000 is minimal to a multinational corporation like Boeing. Hence while the court might impose a duty to investigate upon individual plaintiffs, it would be easier for them to prove that discovery amounted to an undue burden. In sum, the "undue burden or cost" relates not only to the responding party's financial ability, but also to the information's potential relevance in the ongoing litigation, and the party needs to articulate just *why* the information is both unnecessary and costly to produce. This naturally implicates preliminary discovery, which has its own related costs.

As for what files need to be retained and for how long, cases like *Wells v. Xpedx* shed some light on that question but also raise new ones. The *Wells* court held that the producing party had the obligation to search through its archives to find deleted emails, notwithstanding its document retention policy, which held emails for only a specified period of days. The party never argued that the files were not reasonably accessible? One commentator believed that the question hinged on whether the emails were "double deleted," or where, for example, the trash folder is emptied and document recovery necessarily requires some sort of forensics examination:

> In my opinion, and that of most commentators and courts that have squarely faced the issue, the obligation to search for "double deleted" files should not arise <u>in all circumstances.</u> This duty should only arise in certain special circumstances, where, for instance, there is evidence that highly relevant emails have been double-deleted, and therefore that there is good cause to go to the extra time and expense inherent in a forensic examination for such files. Most courts do not require an extraordinary search for deleted files, unless and until special circumstances are shown to warrant such extraordinary efforts.[90]

Ultimately, for some time, cases like *Zubulake* encouraged a Luddite-like approach to technology, where shredding everything and not knowing the

[90] Ralph Losey, *When Should You Search for Deleted Files?*, http://ralphlosey.wordpress.com/2007/06/02/when-should-you-search-for-deleted-files/ (last accessed Dec. 15, 2007).

contents of one's ESI excused conduct[91]. But courts are moving toward a trend of equating technical incompetence with ESI being not reasonably accessible. In essence, they have created a sort of fiduciary duty of care between parties and the tribunal itself: parties must in good faith keep themselves (and the court) informed. And, because objecting to discovery is often decided on economic terms, parties must additionally be honest about the costs of production.

4. REMOTE FORENSICS SOFTWARE COMPARISON

The law in this area seems not only to depend upon certain courts' prior legal analyses; but, also upon changing technologies. Up until recently, the performance of remote forensics was somewhat limited, very expensive, or both. By and large, such endeavors were limited to super specialists and large corporations up to this point in time.

Courts have been reticent to require forensic preservation of any computer within a litigant's control due to the cost and effort involved in forensic preservation of entire systems where there systems are numerous and geographically disparate. A good recent example is *John B. v. Goetz,* 2008 U.S. App. LEXIS 13459 (6th Cir. Jun. 26, 2008). In that case, the appellate court overturned a lower court's ruling that 50 key custodian's computers had to be forensically preserved as a sanction for failure to comply with the District Court's earlier order on a motion to compel. Judge Rogers ruled that ""[t]he provisions in the orders that require the forensic imaging of all computers containing responsive ESI constitute an abuse of discretion. *Id*. at *26. While this case could be distinguishable from other cases on the basis that the court considered the privacy concerns of public officials who were the respondents, it certainly makes the point that forensic preservation of every machine containing relevant ESI will at least be questioned by courts due to the effort in effecting such preservation. Or you could efficiently search many disparate systems for responsive data without creating forensic duplicates.

With the advent of several companies entering the remote forensics market, the availability and price of the base software packages have now begun to include options that may be considered affordable by future courts. The feature sets seem also to be expansive. If so, this begs the question: Does remote forensics now allow for economic and efficient ediscovery of all networked computers, thereby deeming the data found thereon to be "readily accessible" under the Federal Rules

[91] "Zubulake thus creates a perverse disincentive that prevents companies from investing in more efficient data storage technologies, because parties with efficient storage systems are generally forced to produce more digital documents than parties using legacy storage systems. Although companies eventually may determine that the need for a newer storage system exceeds the risks posed by broad electronic discovery, litigants should not be forced to weigh potential adverse legal consequences against the benefits that could be realized by investing in appropriate systems for their business needs." Daniel B. Garrie & Matthew J. Armstrong, *Electronic Discovery and the Challenge Posed by the Sarbanes-Oxley Act*, 2005 U.C.L.A. J.L. & TECH. 2 (2005).

of Civil Procedure? To delve into this question, it was necessary to at least do a preliminary investigation of the tools available and their feature sets.[92]

It is also imperative to state that preservation with remote forensic tools would not likely take place in the same manner as in-person forensics. For instance, in most circumstances, it is still technically very difficult to take a full image of a computer over a network connection. These tools are much more likely to be utilized to perform word searches remotely and return files that satisfy those queries, or to capture specific files from numerous remote machines. Both of these functions are the strong suit of remote forensic utilities, generally.

4.1 Analysis of the Current Commercially Available Tools

The tools under consideration can be categorized in several ways. One way is to categorize them according to when they are installed. One group has to be installed before the incident or situation to be investigated (Proactive or Preventative), while another group can be installed after the incident or situation to be investigated (Reactive or Investigatory). Most reactive solutions require installation of an executable file or servelet on the target computer(s). Examples of packages we consider proactive include: Guidance Software EnCase Enterprise / EDiscovery, AccessData Enterprise / Ediscovery, Paraben P2 Enterprise, Wetstone Livewire. Examples of packages that we consider to be reactive include: Tech Pathways ProDiscover IR, Paraben P2 Shuttle, and F-Response Consultant Edition.

A second possible categorization is by price. For our purposes, we will consider three price levels, expensive (high five figure to six figure price), moderate (high four figure to low five figure price), and inexpensive (low four figure price). We considered the following to be relatively more expensive: EnCase Enterprise / EDiscovery, AccessData Enterprise / Ediscovery. We considered the following to be realatively moderately priced: Paraben P2 Enterprise, Wetstone Livewire, Tech Pathways Prodiscover IR, Paraben P2 Shuttle. Finally, we considered F-Response Consultant Edition to be the least expensive, though it is really a conduit for other computer forensic tools and not a standalone remote forensic solution.

With regard to E-Discovery, we believe the following features should be available: ability to image a computer over the network, multiple image formats, disk preview over the network, searching over the network, live analysis (including physical memory dump) over the network, and encryption of transmitted data. Also considered were: price, ease of use (does the new

[92] Please note that we did not deliberately leave out any solution commercially available in the United States. One may also argue that there are several free-ware solutions available, such as Helix. They are powerful and inexpensive (i.e. free). However, due to the fact that there is not a product being sold, marketed and supported in the United States utilizing Helix as a remote forensics tool, we did exclude it from consideration. Perhaps, discussion of same will be covered in future article.

software require training) and additional equipment needs (does the solution require the user to buy a server).

Below is a brief discussion of each software solution. We have tried to address each of the features above and have made every attempt to present the most current information available. Many of the products listed have other desirable features such as Incident Response capabilities, but these are beyond the scope of this article.

EnCase Enterprise

Guidance Software's EnCase Enterprise was one of the first remote forensics tools. Originally released around 2001, it is the most widely used enterprise solution and is the product that all others are compared to. This product must be installed across the entire network before the analysis can begin.

Given its high price, Enterprise includes a rich feature set. Additional functionality can be added by purchasing the E-Discovery module. Using this combination, it is possible to image a workstation across the network, though the type of image will be limited to EnCase's proprietary .e01 format. Remote disk previewing and searching are supported and all transmitted data can be encrypted. Using the E-Discovery module allows searching across the entire network simultaneously. Live analysis is listed as a feature, including a remote physical memory dump. Because of its size and complexity, Enterprise / EDiscovery does have steep hardware requirements (it requires its own server) and does require training (though a year-long training pass in included). The price tag is high (even small installations can be six figures), but it is intended to provide a complete internal E-Discovery solution.

EnCase claims the product is installed in half of the Fortune 50 companies, 100 of the Fortune 500 and has been cited in over 50 court cases. It has garnered acclaim from Socha-Gelbmann and the Gartner Report. For more information, visit www.encase.com.

Access Data

Access Data Enterprise / EDiscovery is most a more recently developed solution. It was released in early 2008 and at this point has limited adoptions. Designed to compete head to head with EnCase Enterprise / EDiscovery, this product must also be installed across the entire network before an analysis can begin.

Like EnCase's products, the AccessData Enterprise installation performs many of the needed tasks, but can be supplemented with the E-Discovery module for advanced functionality. Remote disk imaging and preview, and remote searching across the entire network are possible with transmitted data encrypted for security. Many output formats are possible (dd, e01, smart) as with the stand-alone FTK Imager product. AccessData also boasts the ability to image multiple nodes simultaneously. Similar to EnCase, purchasing a separate server is recommended. AccessData provides training at installation, with no further training recommendations other than familiarity with their FTK forensic products. The Enterprise and E-Discovery interfaces correspond to the new FTK 2.0 GUI that has been recently released. Pricing is in the same tier with EnCase Enterprise and E-Discovery.[93]

Although too new to have a long client list, AccessData will likely be competitive with companies that have already chosen FTK as their primary forensics tool. For more information, visit www.accessdata.com.

Paraben's P2 Enterprise

Paraben's P2 Enterprise is a full featured product designed to compete with the products from AccessData and Guidance Software, but at a more moderate price point. In addition, it appears to provide E-Discovery functionality with no additional module required. This may make a full enterprise and ediscovery solution available to small and medium sized businesses who could never justify the expense of the "big two". The product is relatively new, originally released in early 2007.

Paraben's product has the ability to image over the network, preview disks, remotely search and do live analysis including physical memory dumps, all while sending the data in encrypted format. It can image in a logical or physical form that is output to a raw format that Paraben calls PFR (named for Paraben's imaging software: Paraben Forensic Replicator). It also has some unique proactive monitoring functions such as tracking intellectual property and logging chat activity even when the user's logging features are turned off. One of the unique functions of Paraben's product is that it is designed to scale to the full size of the network and can work with as many machines as desired at once. Paraben's product requires a separate server like the other vendors in this area. Training is included in the costs associated with the onsite installation of this product. For more information, visit www.paraben.com.

[93] A significant number of practitioners have had difficulty getting FTK 2.0 to operate properly. This may cause practitioners to be wary of Access Data's enterprise solutions. It should be noted that at the time we wrote this article, Access Data was devoting serious resources to revising FTK 2.0.

Wetstone's Livewire

Wetstone's Livewire is also a full featured product with a smaller price tag. Although Livewire has been around since about 2004, a recent update with a brand new GUI interface makes it seem new. Several features from the older version are not yet available on the update, but according to company representatives these capabilities should be available again soon. The product can preview disks, image a disk, create a physical memory dump and perform keyword searches across the network though the output is limited to raw or dd format. No additional hardware is needed and training requirements are minimal due to the new GUI interface and company webinars. Livewire is priced at about $10,000 and claims users from both law enforcement and Fortune 500 companies. For more information, visit www.wetstonetech.com.

TechPathway's ProDiscover

TechPathway's ProDiscover IR has been around since 2004. The network capabilities were a natural extension of the existing ProDiscover forensic products. As this is a reactive solution, deployment is not necessary before the incident occurs. The software can image a disk, preview a disk, perform a physical memory dump, and perform keyword searches on a single computer connected to the network. Scripting allows the processing of multiple computers in serial fashion. Output format is limited to a raw type format with a header and footer and sessions are encrypted for security. Although no additional hardware is required, the vendor does recommend a three day training session to familiarize the new user with the software. The product enjoys relatively wide adoption with many high profile government agencies and Fortune 500 companies. ProDiscover IR boasts an easy to use interface, relatively high acquisition speeds across network connections and the ability to easily and quickly push and pull the remote agent to and from the target machine. In addition, the software has been vetted in both civil and criminal court. For more information, visit www.techpathways.com.

Paraben's P2 Shuttle

Paraben's reactive solution is P2 Shuttle. Like all reactive software, it does not have to be deployed before the incident occurs. Shuttle can image a disk, preview a disk, search systems, and perform a physical memory dump from any computer on the network using an encrypted session. Like P2 Enterprise the image output is limited to the PFR format. A few unique features are Shuttle's ability to search up to 25 computers simultaneously and the ability to do screen captures. Although no additional hardware is required, the software does require access to a MySQL database. Although Paraben offers a four day class, the company also offers web demos and contends the software is very easy to use. Shuttle, like Paraben's Enterprise product, was released in early 2007. At its price point, there are few, if any other products that can compare. For more information, visit www.paraben.com.

F-Response

F-Response Consultant Edition is a unique solution to the enterprise forensics problem. Released in 2008 (though tested for years), F-Response creates a read only connection between the analysis machine and any other computer on the network. This allows the investigator the ability to use any forensic tool to do imaging or analysis. The connection allows the forensic software to act on the remote disk as if it was physically connected to the analysis machine. Because F-Response is tool independent it is a versatile solution due to the fact that it allows most forensic practitioners to continue to use the software that they currently utilize. Remote imaging, previewing and searching are all possible. Image formats are endless; limited only by tool choices. Searches across the entire network are limited by the number of disks that can simultaneously be mounted and searched in the chosen forensic software. Although F-Response does not offer an internal ability to encrypt transmitted data, it does support Microsoft IPSEC encryption. Although physical memory dumping is not currently possible, the company believes it will be able to provide this functionality by early 2009. No additional hardware is required, though obviously the user will need to provide the forensics software to image or analyze a computer disk. The company provides videos showing the use of the product and claims that no further training is needed. All three versions of the software are inexpensive, which is one of the big selling points of this solution. If the user already owns forensics software, F-Response extends the capabilities of that software greatly. The idea is to give the client with an existing copy of FTK (or other software) enterprise level capabilities for very little money. For more information, visit www.f-response.com.

Although the basic functionality of many of these products is similar, each one is unique. Different interfaces, ease of use, price and hardware requirements might make one a much better choice for a particular user. Many of these products have a demo version so a potential buyer can test the product for a short time. In order to make a basic comparison easier to digest, we have prepared a table outlining some of the basic feature sets of these products:

	EnCase Enterprise/ Ediscovery	**AccessData Enterprise/ Ediscovery**	**P2 Enterprise**	**Wetstone Livewire**	**ProDiscover IR**	**P2 Shuttle**	**F-Response**
Image over network	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Output format	e01	dd, e01, smart	Pfr (dd)	dd	dd with header/footer	Pfr (dd)	Any format possible
Disk Preview	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Keyword Searches	Yes	Yes	Yes	Yes	Yes, single machine	Yes	Yes
Physical Memory Dump	Yes	Yes	Yes	Yes	Yes	Yes	No, expected 2009
Encryption of session	Yes	Yes	Yes	?	Yes	Yes	Supports MS IPSEC
Price	Expensive	Expensive	Moderate	Moderate	Moderate	Moderate	Inexpensive
Additional Equipment	Server	Server	Server	None	None	None	Forensic Software
Training Required	Yes	Yes	Yes	Webinars	Yes	Yes	Online demos

It is important to note that we have included a rather small comparison feature set. We really only included items that we believed were necessary elements at this time. Naturally, all of the products met virtually all of criteria. Nevertheless, we don't mean to convey that these are all similar products in all ways. Each one of these products is different in various ways. Just because they meet the base criteria set forth herein does not mean that they are equivalent. Similarly, just because one or more of these products is more expensive does not mean that they will add any features absolutely necessary for ediscovery.

It is equally important to note that the above comparison is based upon the company's own publications of their product's feature set. We have not done any independent testing to confirm or repudiate those claims. Certainly, we have all experienced products that don't perform as advertised. Thus, please do not assume that we have endorsed any of these products, nor have we tested their advertised feature sets.

5. WHAT CAN BE DERIVED?

Under Federal Rule of Civil Procedure 26(b)(2)(B), litigants need only produce ESI that is "readily accessible."[94] The applicable rule defines "readily accessible" in terms of burden and cost.[95] Nevertheless, they still have a duty to preserve – not produce - all relevant evidence within their possession and control, regardless of burden and cost.[96]

Courts have looked at many different factors to determine whether the burden

[94] Fed. R. Civ. P. 26(b)(2)(B).

[95] Id.

[96] Fed. R. Civ. P. 26(b)(2)(B), Advisory Committee Note of 2006.

and cost of producing certain ESI renders it not “readily accessible”, both before and after the Federal Rules of Civil Procedure were modified. Much of the discussions about whether documents were readily accessible concentrated in the form that the ESI was held.[97] Other courts refused to make strict delineations along those lines, rather concentrating on analysis of burden and cost of that particular production.[98] One thing remains clear, the lesser the cost, the lesser the burden, the more likely to be deemed readily accessible.

This certainly begs the question of whether smaller firms may get an advantage. This derives from what we call the Mercedes-to-moped analogy. If you can imagine you require two of your vendors to pick up packages at 5 geographically dispersed locations on a very tight schedule. If it’s too hard, you might give them a break. But, you initially want them both to try. To get there you’d have to travel at a high rate of speed. The vendor with the Mercedes doesn’t have as much of a problem. They just travel at a high rate of speed and get the job done. If the job proves too much, then they just go out and rent a few average cars and make separate trips. Not a problem. The vendor with the moped has a harder time. They don’t have the capabilities to make the trip with just their moped. They would have to go out and find another solution, such as rent average cars. However, this is a bigger burden to the moped vendor since they have a moped budget. Thus, like the moped vendor who might get excused from picking up all 5 packages, smaller firms might get excused from producing geographically dispersed electronically stored information. It might be a little strange; but, smaller firms may get an advantage under the current law.

It naturally follows that any products that would tend to make production of ESI cheaper and easier could have a definite effect on what courts’ deem readily accessible in any particular case. Certainly, if we could just wish the data out of our computer systems, courts would be likely to hold that all relevant data must be produced no matter where it may be found. Technology has not advanced that far, however, and the remote forensics discipline, including the tools necessary to own and to conduct it, is still advancing forward. The present software set advertises that it is capable of forensically acquiring relevant data across large distances. The financial costs involved therein vary, however, from the hundreds to the hundreds of thousands dollars to implement. In some cases, however, they do appear low enough that one could speculate judges will begin ruling that data sets residing in geographically disparate computers are readily accessible using remote forensics. However, until that actually happens, we will have to wait and see. We do think, however, that it is a question of when, not if, that will occur.

[97] See e.g. Quinby v. WestLBAG (S.D.N.Y. Dec 15, 2005)(archiving data onto back-up tapes makes that data inaccessible).

[98] See e.g. Semsroth v. City of Wichita (D. Kan. Nov. 15, 2006)(rejecting making blanket exceptions to accessibility, like back-up tapes).