ALM
LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

Special Report
e-Discovery

Defensible Legal Hold Process

Beyond Notifications

By Deborah A. Johnson

If the road to hell is paved with good intentions, then the road to legal sanctions can be paved with intentions to show good faith. That's particularly true when it comes to implementing a legal hold process. Companies with lawsuits on the horizon must be extremely careful with the technology they use and the processes they follow regarding e-discovery in order to avoid sanctions and maintain defensibility.

Some in-house counsel may comfort themselves with the idea that they can issue a legal hold notification and present it to a judge with as a showing of good faith. As companies are finding, however, these actions alone merely establish an intention to have custodians preserve potentially relevant information. Unfortunately, intentions are irrelevant.

Establishing good-faith compliance with a duty to preserve requires constant vigilance on the part of the in-house legal team, a vigilance that goes beyond notification. In the recent case *Cache La Poudre Feeds, LLC v. Land O'Lakes*

continued on page 5

The Revised Federal Rules of Civil Procedure

Where We Are One Year Later

By Adam I. Cohen

The 2006 amendments to the Federal Rules of Civil Procedure ("FRCP") were anticipated by some corporate counsel with Y2K-like gloom and doom predictions. In particular, many wondered aloud whether the rules would have the effect of placing reasonable limits on electronic discovery, or whether instead they would open the floodgates and drown us all in a sea of electronic document production. However, the past year has shown that, like the Y2K hysteria that went out with a whimper, the fretting over the negative impact of the amendments may have been overblown. Although there were a couple of notable surprises, most federal courts addressing e-discovery disputes under the new rules issued opinions consistent with prior case law. This article identifies some of these opinions from the period post-dating the rules amendments to draw some lessons that are emerging.

Preservation and Spoliation

Despite the flood of e-discovery articles and courses, many litigants continue straying from preservation compliance. However, the predominating trend continues to show that, notwithstanding the negligence standard for culpable spoliation conduct in some jurisdictions, severe sanctions are reserved for spoliation that is not mere oversight, but at least serious bumbling, if not bad faith. As is universally true when it comes to dealing with courts, credibility is critical in e-discovery disputes. For example, in *Cache La Poudre Feed, LLC v. Land O'Lakes Inc.*, 244 F.R.D. 614 (D. Colo. 2007), the defendant incurred monetary sanctions for neglecting to follow up with key witness-custodians as well as failing to supervise IT in preserving electronically stored information ("ESI"). The defendant tried to defend the sanctions motion by claiming that these custodians were not likely to have relevant information — despite having identified them as witnesses on its initial disclosure.

The Washington, DC, MTA found itself under fire from Magistrate Judge John Facciola after admitting its failure to suspend its "auto-delete" routine for e-mails two years into the case, then having the "chutzpah" to argue that although relevant e-mails might be found on backup tapes, such e-mails were "not reasonably accessible" under new Rule 26(b)(2)(B). *Disability Rights Council of Greater Washington, et al. v. Washington Metropolitan Transit Authority, et al.,* 242 F.R.D. 139 (D.D.C. 2007). *See also Citizens for Responsibility & Ethics in Washington v. Executive Office of the President*, No. 1:07-cv-01707-HHK (D.D.C. Nov. 12, 2007) (White House ordered to preserve backup tapes of deleted e-mails). Given prior cases sanctioning parties for similar "auto-delete" failures, the court's ire and requirement to produce backup tapes of deleted e-mails was predictable. *See In re Kmart Corporation*,

continued on page 2

Revised Federal Rules

continued from page 1

371 B.R. 823 (N.D. Ill. 2007) (automatic deletion of e-mail not suspended two years into litigation, but sanctions imposed for failure to properly institute a litigation hold).

The cases following the Rule 37(f) "safe harbor" firmly reassert the prior case law: Using document retention policies as an excuse for the destruction of evidence subject to preservation duties is a losing tactic. Unfortunately, some parties are still learning this lesson the hard way. *See Doe v. Norwalk Community College*, 2007 U.S. Dist. LEXIS 51084 (D. Conn. 2007) (school had no routine retention policy and wiped hard drives of key witnesses, adverse inference and other sanctions ordered); *Doctor John's, Inc. v. City of Sioux City*, 486 F. Supp. 2d 953 (N.D. Iowa 2007) (argument that retention regulations required destruction of evidence deemed frivolous, no sanctions ordered based on public interest).

Parties are also on notice that disingenuousness regarding whether ESI is in their "possession, custody or control" will bring harsh consequences. In *In re NTL, Inc. Securities Litigation*, 244 F.R.D. 179 (S.D.N.Y. 2007), Magistrate Judge Andrew Peck lambasted the defendant, when it claimed it could not provide documents held by certain non-party entities and e-mail held by those entities was destroyed. It was eventually revealed that all along the defendant had a written agreement with these entities allowing access to the ESI. This chicanery brought an adverse inference and monetary sanctions.

Adam I. Cohen is a senior managing director in FTI's Technology practice, where he leads the e-discovery readiness practice. Prior to joining FTI, Cohen was a litigation partner at Weil Gotshal. He is the co-author of the annually updated treatise Electronic Discovery: Law and Practice (Aspen Publishers 2003), which has been cited as authority in several federal court opinions.

One decision on preservation sparked a firestorm of controversy. A federal judge in California ordered that defendant Web site operators, accused of facilitating infringing movie downloads, preserve a "server data log" showing IP addresses of users of the service, and recording their requests. *Columbia Pictures Inc., et al. v. Bunnell*, 2007 U.S. Dist. LEXIS 63620 (C.D. Cal. 2007). Defendant objected that this data was stored only in RAM, not normally retained, and that such "ephemeral data" is not subject to preservation and discovery. The court disagreed, albeit issuing caveats about the relevance of this particular data to this particular case. Given the nature of the case and the apparent absence of any burden in providing the logs, this opinion may not be as radical as it has been characterized. However, it indicates the prudence of considering "ephemeral" ESI in evaluating e-discovery compliance steps.

Other Assorted Discovery Mishaps and Sanctions Issues

A more recent case that has been making legal headlines is *Qualcomm Inc. v. Broadcom Corp.*, 2007 U.S. Dist. LEXIS 57136 (S.D. Cal. 2007), in which the court found that plaintiff and its counsel had obstructed discovery with "gross litigation misconduct" that included "constant stonewalling, concealment, and repeated misrepresentations." While it is difficult to discern the whole story based on published materials, normally courts do not issue such remarks for minor technical errors or small oversights. It is clear from the evolving Qualcomm scenario that the consequences of non-compliance with e-discovery obligations will be visited on counsel, including outside lawyers. *See also School-Link Technologies, Inc. v. Applied Res., Inc.*, 2007 U.S. Dist. LEXIS 14723 (D. Kan. 2007) (lawyers need to supervise discovery to ensure compliance). This is not a new concept, as classic e-discovery cases, notably *Zubulake v. UBS Warburg* and *Coleman v. Morgan Stanley* (the Florida state court case of $1.4 billion verdict fame) demonstrated before the FRCP were revised.

An earlier opinion issued on the heels of the FRCP amendments also sparked derision from the bench, and more importantly, severe sanctions. In *Wachtel v. Health Net, Inc.*, 239 F.R.D. 81 (D.N.J. 2006), the court described "a lengthy pattern of repeated and gross non-compliance with discovery." The pattern involved e-mail discovery, specifically the failure to preserve e-mails, the failure to search for it before it was destroyed, the failure to tell counsel that it existed when it wasn't destroyed, and the failure to comply with orders to produce it. The punishment was devastating, including the striking of filings and pleadings, imposition of costs, and sanctions directed personally at one of the attorneys. *Cf. Malletier v. Dooney & Bourke*, 2006 U.S. Dist. LEXIS 96796 (S.D.N.Y. 2006) (no sanctions for alleged deficiencies in discovery responses where factual allegations lacked specificity and no evidence of prejudice was presented).

Electronic Search Protocols

Several of the decisions from the past year are instructive in providing protocols guiding the identification of responsive information. Parties prepared to propose such protocols early in the case will have the upper hand in steering discovery. *See Williams v. Taser International, Inc.*, 2007 U.S. Dist. LEXIS 40280 (N.D. Ga. 2007). Courts will order hearings on search protocols where the disputed issues are complex and the costs potentially significant. *See Apsley v. Boeing_Co.*, 2007 U.S. Dist. LEXIS 5144 (D. Kan. 2007) (hearing ordered to evaluate defendant's claims of burden where plaintiff sought extensive keyword searches of e-mail across multiple storage platforms).

A failure to plan and execute a reasonable search is not likely to pass unnoticed. In *Peskoff v. Faber*, 244 F.R.D. 54 (D.D.C. 2007), Judge Facciola identified several sources of ESI that had not been addressed by the defendant, which claimed that the information sought did not exist.

continued on page 7

Making e-Discovery Cost-Effective for Smaller Companies

By Richard B. Friedman

In the days of only paper documents, smaller companies could afford to wait until they became involved in a lawsuit to worry about pre-trial discovery, but today's reliance on digital information makes that a risky and unnecessarily expensive strategy. To meet the requirements of the amendments to the Federal Rules of Civil Procedure concerning electronic discovery that went into effect on Dec. 1, 2006, companies need to plan and prepare ahead of time. Although these rules present a new set of challenges for small companies, the good news is that developing and implementing an e-discovery strategy does not always have to be an expensive project. By taking a handful of cost-effective steps, companies can save both time and money in litigation costs in the long run.

Meeting the Legal Obligations Of New Technology

As is widely known, technology has become a great equalizer. Even the smallest companies have the same powerful communication tools at their disposal as the largest enterprises. From e-mail to instant messaging, voice mail, electronic documents, databases, and spreadsheets, information technology is readily available at a reasonable cost to businesses of every size. In fact, the availability of such powerful technology has allowed even small companies to reach and serve customers around the world and, in some cases, to become extraordinarily successful.

Richard B. Friedman (rfriedman@dreierllp.com) is a partner in the Litigation Department at Dreier LLP with extensive experience in commercial litigation and arbitration. He is co-chair of the Corporate Litigation Counsel Committee of the Commercial and Federal Litigation Section of the New York State Bar Association.

While technology has given even small companies access to global communications capabilities, it also has laden them with new legal obligations. No matter what their size, all companies involved in federal court cases have an equal duty to abide by the Federal Rules. Further, given the ubiquity of digital information in commerce today, state legislatures and courts will almost certainly eventually follow suit.

At the heart of the Federal Rules for e-discovery are the obligations to be able to locate, preserve, and produce in a timely manner digital information that is relevant to the subject matter of a lawsuit. While the amended Federal rules do allow the courts to consider the relative abilities of both parties to bear the costs of electronic discovery and to shift the costs in some circumstances, smaller companies still have to take reasonable pre-litigation measures to comply with the law. Those companies that fail to make a reasonable effort to meet the e-discovery standards risk not only incurring higher than necessary e-discovery costs, they also expose themselves to damaging court sanctions.

These measures do not necessarily have to involve large investments. A common sense approach to managing digital information combined with the establishment of proper policies and procedures can go a very long way to meeting companies' e-discovery obligations. In addition, by taking reasonable measures ahead of time, smaller companies increase their chances of being able to successfully argue that the costs of e-discovery should be shifted to the requesting party in certain cases. That argument is likely to be most persuasive when such party is much larger than the prospective producing party.

Although some executives in smaller companies may believe that their companies' exposure to e-discovery is minimal, it is worth noting that one of the most highly contested areas of federal court litigation today involves intellectual property, particularly patents, trademarks, and copyrights. A company's ability to protect its intellectual property, which is often its most valuable property, may depend on its ability to successfully navigate e-discovery issues in federal court. In an intellectual property action involving a smaller company and a much larger company, the bigger company will almost certainly seek to take advantage of every opportunity, including exploiting the e-discovery deficiencies of the smaller organization.

Keeping e-Discovery Costs Manageable

When it comes to e-discovery, preparation is key, and much of this advance work should really be a regular part of business operations. A failure to plan and prepare is one of the largest drivers of e-discovery costs as companies waste money and time to come up with ad hoc solutions that often disrupt their IT operations, their management team, and their business. Among the key issues in planning are simply knowing what kind of information the company collects and keeps, how it is stored, where it is stored, and how it is backed up. This kind of information inventory should be a standard part of all companies' overall corporate risk management strategy.

The next step is to develop, implement, and adhere to a regular document retention plan that sets out a schedule for the routine destruction of unneeded digital information. Companies then need to put in place the capabilities to preserve information when litigation ensues and a litigation hold is implemented. Litigation hold policies and procedures must be effective in preserving electronic information as well as the associated "meta-data" that tracks when the information was created, edited and/or deleted and by whom. All employees, whether executives or hourly workers, need to be strongly advised not to attempt to destroy electronic or other information when a litigation hold is in place.

All of these steps are essential to taking advantage of the "safe harbor" afforded by the Federal Rules for e-discovery. This safe harbor provision, contained in Rule 37(f) and

continued on page 4

Smaller Companies

continued from page 3

derived from a ruling by the U.S. Supreme Court in a case involving accounting firm Arthur Andersen, recognizes that not every bit of data created can or should be saved. The rule thus provides an exemption for material that is lost as a result of the "routine, good-faith operation of an electronic information system." A company that does not have an established document retention plan or suddenly reinstitutes a lapsed plan when litigation is threatened will have a hard time reaching this safe harbor.

Another critical reason for small companies to take these steps ahead of time is to better position the company for e-discovery disputes involving information that is difficult and expensive to retrieve, for instance, copies of e-mails that exist only on disaster recovery back-up tapes. Federal Rule 26(b)(2)(B) provides an exemption for electronic information that is "not reasonably accessible because of undue burden or cost." In addition, the Federal Rules allow courts to provide for the shifting of discovery costs to the requesting party when certain requirements are met.

A small company seeking to shift the cost to its larger adversary, however, will need a more effective argument than mere size. Given their size disparities, it will be expected that the smaller company is dealing with a smaller quantity of digital information in a more limited number of locations, both physical and virtual, than its larger adversary. The smaller company will have to be able to demonstrate that the data is not reasonably accessible and that the cost or burden in man-hours would be excessive in the context of the litigation. The smaller company's in-house and outside counsel will need to have a detailed knowledge of the company's IT system to do this effectively. If a smaller company is successful in shifting costs, however, and it later emerges that it did not take reasonable care to properly preserve information, potentially significant negative ramifications are likely to ensue.

Shrinking the Document Universe

When it comes to producing requested documents, companies should be aware that one of the largest drivers of unnecessary costs is duplication. While limited numbers of paper documents typically exist, there may be dozens if not hundreds of copies of electronic documents. A prime example is an e-mail sent from a manager to a large group of employees, who may all retain copies. There is no need for a company to produce more than one copy of that e-mail provided it is unaltered. To control costs, companies may consider limiting the kinds of electronic information they create, for example, by prohibiting or curtailing text and instant messaging and thus avoiding the expense of having to archive and possibly retrieve that information.

Considering the hundreds of thousands or millions of pages that may be involved in a commercial litigation, a key means of reducing the cost of e-discovery is to simply reduce the universe of documents that must be preserved and reviewed. There are a variety of off-the-shelf software tools that eliminate duplicate documents and quickly pay for themselves in cost savings.

Once duplicate documents have been weeded out, companies can also seek to save costs by eliminating duplicate layers of review for documents, whether it be by legal assistants, junior associates, senior associates, or senior partners. Having the review performed by the person with the right level of expertise to make an appropriate judgment will save the potential costs of having to do the review over again pursuant to a court order.

Communicating with Opposing Counsel

Another critical, cost-effective and too-often-overlooked means of limiting e-discovery costs is open communication with opposing counsel from the earliest stages of the case. Often, two relatively small companies will find it to their mutual advantage to reach amicable discovery agreements in order to avoid costly battles. Absent some overriding strategy consideration to the contrary, opportunities to resolve discovery disputes should be embraced as early as possible. Being prepared ahead of time should also strengthen a company's position in early discussions because it lessens the opportunity for opposing counsel to try to exploit deficiencies in document retention procedures.

Among the issues to be negotiated in pre-trial conferences is the form in which the information is to be produced. Companies are bound only to produce information in one format, typically the format in which it is ordinarily maintained. Counsel will want to take into consideration cost factors when deciding how material is to be produced. Agreeing to accept material such as e-mails in printed form may add to costs later on if those printed e-mails must be collated with their printed attachments. Typically, the courts will require parties to a litigation to live by the electronic discovery agreements they reach in pre-trial conferences. Preparation plays a key role in another significant means of keeping costs under control — avoiding having to do things all over again, such as having to pay for a forensic expert to examine the company's computer servers under a court order during a search for information.

Litigation is by its very nature unpredictable and may strike a company, regardless of its size, at the most inconvenient time. A lack of preparation that leaves a company unable to produce crucial documents during discovery can lead to significant adverse judgments as well as lasting damage to the company's reputation and business. While, at present, the electronic discovery rules are principally limited to federal courts, state legislatures and courts can be expected to adopt similar rules in time. Preparing now enables companies to make electronic discovery a more manageable and predictable part of their legal expense and to limit their exposure to adverse court rulings and judgments.

—❖—

Legal Hold Process

continued from page 1

Farmland Feed, LLC 2007 WL 684001 (D. Colo. Mar. 2, 2007), the court held that simply notifying custodians of a duty to preserve is not sufficient proof that a company has engaged in a defensible preservation effort. Companies cannot assume that employees have the knowledge, ability or intention to locate, preserve and produce all potentially relevant electronically stored data after receiving a litigation hold notice. Counsel has a continuing obligation to ensure that employees have followed the instructions contained within the hold notice and properly preserved the responsive information in their possession, as the defendant in *Cache La Poudre Feeds* learned. In that case, the judge lambasted the defendant for its counsel's incomplete preservation efforts subsequent to issuing a legal hold notice.

Part of that ruling focused on Land O' Lakes' mishandling of Federal Rule of Civil Procedure 26(g), which requires that every disclosure be signed by an attorney or other party, and that the "signature of the attorney or party constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the disclosure is complete and correct as of the time it is made."

According to the court, in-house and outside counsel at Land O' Lakes failed to properly preserve and collect electronically stored information and to follow up appropriately to the hold notice. When custodians found 50,000 pages of documents that were potentially relevant to the trademark dispute at hand, only 415 of which were e-mails, counsel inside and outside the company simply accepted those findings. No attempts were made to verify the completeness of the collection.

This did not represent an acceptable effort, Magistrate Judge Craig B. Shaffer found. "Land O' Lakes General Counsel and retained counsel failed in many respects to discharge their obligations to coordinate and oversee discovery," Shaffer's ruling read. "While instituting a 'litigation hold' may be an important first step in the discovery process, the obligation to conduct a reasonable search for responsive documents continues throughout the litigation." The court also was disturbed by the company's failure to prevent routine "wiping" of computers for employees who had left the company. This, the court found, constituted spoliation.

… simply notifying custodians of a duty to preserve is not sufficient proof that a company has engaged in a defensible preservation effort.

To show a good-faith effort has been made, it's not enough for companies to issue a litigation hold notice and give employees the burden and sole discretion of tracking down potentially responsive materials. Following are 10 steps in-house counsel can take when issuing a legal hold notice that is defensible.

Make It Policy

The moment a company becomes aware of or reasonably anticipates litigation is not the time to create from scratch a policy for hold notices. Crafting a thorough, well-reasoned policy ahead of time is one way to show that the company handles its electronic data in good faith.

Depending on the industry and size of the company, in-house counsel may want to conduct regular training on litigation hold notices and data preservation. However, this may not make sense for every company or for employees at every level, and it may serve to confuse or distract many workers. The more heavily regulated and litigious the industry, the more it may be worthwhile to introduce the concept to employees who are likely to receive a litigation hold notice in the future.

Consider What Is Reasonable

In theory, the rule for whether a company should issue a litigation hold notice is fairly straightforward: is there a "reasonable" anticipation of litigation that would trigger a duty to preserve information. In practice, however, determining whether litigation is reasonably likely can be far more complicated.

In-house counsel should develop policies regarding the circumstances that would trigger a litigation hold. When considering whether a situation could lead to a lawsuit, in-house counsel should take into account several factors, including: 1) the nature of the potential lawsuit; 2) who the adversary is and how likely that adversary is to file a lawsuit; 3) the legitimacy of the claims; and 4) the likelihood that potentially responsive data may be lost or destroyed.

Don't Leave It to Employees

Even if a company establishes a formal training program to teach employees how to respond to a litigation hold notice, in-house counsel must follow up with custodians regularly and be prepared to offer constant guidance. They also should remember that some custodians may decide it's not in their best interest to preserve all potentially relevant materials and take appropriate actions. A hold notification is only part of the preservation process. A hold notice is expected and required, but it's the actions a defendant takes afterward that are key to showing a good faith effort.

Know Where the Data Lives

Litigation has a continual presence at many companies and can be the

continued on page 6

Deborah A. Johnson is VP Discovery and Litigation Solutions at Orchestria. She is a contributing author to The Sedona Principles: Best Practice Recommendations and Principles for Addressing Electronic Document Review and Production.

Legal Hold Process

continued from page 5

source of great stress for in-house counsel. When in-house counsel find themselves dealing with multiple large-scale discovery efforts, they often have limited time to respond and too often have no clear understanding of where all potentially responsive data is located. Before long, that situation can turn into a nightmare.

With recent case law and the newly amended Federal Rules, courts have limited tolerance for companies that do not know where their data is stored, in what formats the data exists, and how accessible that data is. Judges will not be sympathetic to litigants who cannot produce ESI or can't produce it in the appropriate formats.

Work with HR and IT

To get a complete understanding about where and how ESI is stored, the legal department should work closely with IT on an ongoing basis. This will help ensure that those who manage the computer systems, e-mails and all data stores are properly adhering to the document retention policy.

When a litigation hold notice is issued, in-house counsel also must work with the human resources department to ensure that all potential custodians are identified. If a key custodian leaves the company in the midst of or prior to discovery, in-house counsel need to know that. They also need to make sure the employee does not destroy relevant information, and the hard drive of the former employee's computer is not wiped clean for the next person to use.

Stop Automatic Document Destruction

As soon as a litigation hold notice is issued, companies must ensure that potentially relevant data is not destroyed by the automatic document destruction processes that are in place. The data subject to preservation must be segregated from data stores that otherwise have an automatic deletion schedule. Allowing the routine deletion of files to destroy potentially relevant data will not create goodwill with the court.

Understand the Technology

When evaluating a good-faith effort, the court will carefully consider the technology that parties used in the discovery process. The key consideration for the defensibility of technology is whether it was appropriate for the task at hand and

… courts have limited

tolerance for companies

that do not know where

their data is stored …

whether it was used properly under the circumstances. In-house counsel must not only inquire as to whether the technology works, but also whether and how it is transparent.

In addition, control of data and easy access to it are critical. Consider technology that can be utilized as soon as the litigation hold is issued. In-house counsel should look for technology that will automatically track, manage and monitor all legal holds in one place, making it easier to determine the status of each hold and which potential custodians have responded. The use of proven, thorough, transparent technology will be extremely valuable when establishing that a good-faith effort has been made.

Document Everything

If companies do not track their actions during discovery, it becomes difficult, if not impossible to argue that all relevant data has been turned over without spoliation. In-house counsel should document every step of the process, from preservation to production. This is where proper technology can help. Without accurate, reliable documentation, discovery can get very messy, very quickly.

Don't Rely on a Safe Harbor

When the amended Federal Rules were issued late last year, many in-house counsel took comfort from Rule 37(f), which offers a safe harbor in case the routine operations of a company's computer systems leads to the inadvertent destruction of potentially relevant data. Safe harbor may offer some protection, but it does not equal a get-out-of-jail-free card. Litigants must understand their actions will be scrutinized very carefully, and it is extremely dangerous to rely on safe harbor if the company knew or should have known that computer operations were likely to destroy potentially relevant data.

Review and Repeat

A litigation hold notice is a living document, not something that can be issued and then filed away. As litigation proceeds and discovery evolves, in-house counsel periodically should review the litigation hold to ensure the original notification still properly covers the scope of the matter at hand. In-house counsel also should send periodic reminders to new and existing custodians to ensure continued compliance with their preservation obligations.

Aside from timelines and other mechanical requirements of the FRCP, there are few bright-line rules in litigation. This is especially true of collection, preservation and discovery of ESI, where the volumes of data increase exponentially and the locations of that data is strewn across multi-faceted systems throughout complex organizations. With the appropriate transparent procedures and technologies, companies involved in litigation can execute a defensible legal hold process and support a good-faith preservation effort.

—❖—

Revised Federal Rules

continued from page 2

The court ordered the defendant to provide affidavits describing its search process and to work with plaintiff to develop a protocol for independent examiners to search for the ESI. Clearly, lawyers need to pay attention to search methods even if implemented by their clients if they want to be able to defend their discovery efforts.

Accessibility and Claims of Burden

Decisions addressing disputes over e-discovery burdens are multiplying rapidly. Parties that have difficulty producing relevant information because they employ systems that hinder search and extraction may find little sympathy from courts. *See Zurich American Insurance Co. v. Ace American Reinsurance Co.,* 2006 U.S. Dist. LEXIS 92958 (S.D.N.Y. 2006) ("opaque data system" will not sustain objection to production of claim denial data). In contrast, one court found that scanned images indexed only by name of claim administrator were "not reasonably accessible" where the requested search would have to be manual and cost $80,000. *W.E. Aubuchon Co. v. Benefirst, LLC*, 2007 U.S. Dist. LEXIS 44574 (D. Mass. 2007); *see also Christian v. Central Record Service*, 2007 U.S. Dist. LEXIS 80027 (W.D. Ark. 2007) (production of the hard copies of deleted e-mails, requiring the search of several hundred thousand boxes, found to be unduly burdensome). However, where ESI is available solely through less accessible sources because a party failed to preserve more accessible sources, there will be no free pass on production. *See Disability Rights Council of Greater Washington, et al., supra.*

Courts continue to consider shifting costs for backup tape restoration, but shifting is far from preordained. *See In re Veeco Instruments Inc. Securities Litigation*, 2007 U.S. Dist. LEXIS 23926 (S.D.N.Y. 2007) (defendant initially to pay for backup tape restoration and prepare affidavit detailing costs and preliminary search results as to predicate cost-shifting analysis); *see also In re Veeco Instruments Inc. Securities Litigation*, 2007 U.S. Dist. LEXIS 85629 (S.D.N.Y. 2007) (approving settlement and recognizing potential cost of backup tape discovery).

Requesting parties continue to test the scope of e-discovery. In *Philips v. NetBlue, Inc.*, 2008 U.S. Dist. LEXIS 67404 (N.D. Cal. 2007), a CAN-SPAM Act case, the defendant sought dismissal based on the allegation that plaintiff was obligated to preserve hyperlinked images, hosted by non-parties, from links appearing in e-mails. Denying the motion, the court called this argument "absurd." *Cf. Smith v. Café Asia*, 2007 U.S. Dist. LEXIS 73071 (D.D.C. 2007) (Court required preservation and inspection of ESI on plaintiff's cell phone). In one opinion likely to cause consternation, a Florida district court held that a party has the obligation to search for and produce relevant deleted e-mails and ordered depositions of IT personnel. *Wells v. XPEDX*, 2007 WL 1200955 (M.D. Fla. 2007). While in the past courts have ordered such production where there is a special showing of need or good cause, asserting this as a general proposition is dubious.

Decisions addressing disputes over e-discovery burdens are multiplying rapidly.

Computer Inspections/ Forensic Imaging

The pace of requests for forensic imaging is quickening following the amendment to the FRCP explicitly recognizing the right to such ESI inspections. The results have been consistent with prior case law — inspections are not granted as a matter of course, but only where a basis has been established in terms of the importance of the information sought to the issues at play in the litigation and the likelihood of finding relevant information, a showing that the party possessing the storage media in question has not been forthcoming with respect to relevant information from that source, and the deployment of protocols and technology that protect the integrity of the target data and the confidentiality of privileged or irrelevant personal information.

See John B. v. Goetz, No. 3:98-cv-00168 (6th Cir. Nov. 26, 2007) (staying District Court order permitting imaging and inspection of Tennessee State Agencies' computers by plaintiffs' computer expert); *Butler v. Kmart Corp.*, 2007 WL 2406982 (N.D. Miss. 2007) (denying request to directly access databases without evidence of improprieties); *Scotts Co. LLC v. Liberty Mutual Insurance Co.*, 2007 U.S. Dist. LEXIS 43005 (S.D. Ohio 2007) (mere suspicion does not support request for forensic inspection); *Balfour Beatty Rail, Inc. v. Vaccarello*, 2007 U.S. Dist. LEXIS 3581 (M.D. Fla. 2007) (no justification offered to support "fishing expedition" request for hard drives); *Hedenburg v. Aramark American Food Services*, 2007 U.S. Dist. LEXIS 3443 (W.D. Wash.) (speculation of impeaching evidence does not warrant inspection). *Cf., Frees, Inc. v. McMillian*, 2007 U.S. Dist. LEXIS 4343 (W.D. La. 2007) (inspection of hard drive ordered, subject to protective measures, where hard drive was most likely repository of relevant ESI); *Andarko Petroleum Corp. v. Davis*, 2006 U.S. Dist. LEXIS 93594 (S.D. Tex. 2006) (inspection ordered to assist in determining sanctions motion).

Format of Production

The new rule governing format of production was crying out for interpretation of the criteria of "ordinarily maintained" and "reasonably usable." A related subject of anticipated case law was and is whether and what

continued on page 8

Revised Federal Rules

continued from page 7

production of metadata will be required. In a continuation of landmark production format case, Magistrate Judge David Waxse denied a request for production of e-mails in native format, where the requesting party failed to demonstrate a need for that format. *Williams v. Sprint*, 2006 WL 3691604 (D. Kan. 2006). This accords with other decisions rebuffing requests for native format and metadata productions. *See Michigan First Credit Union v. Cumis Insurance Society*, 2007 U.S. Dist. LEXIS 84842 (E.D. Mich. 2007) (denying request for production of metadata and citing "general presumption against metadata production"). Such requests require a rationale related to the specific case. *See Pace v. International Mill Ser., Inc.*, 2007 U.S. Dist. LEXIS 34104 (N.D. Ind. 2007) (request for native format production case-specific determination); *Kentucky Speedway, LLC v. NASCAR, Inc.*, 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. 2006) (showing of relevance or need required to obtain metadata production). Preservation, as opposed to production, may be another story. *In re National Security Agency Telecommunications Records Litigation*, 2007 WL 3306579 (N.D. Cal. 2007) (order prohibiting the alteration or destruction of, *inter alia*, metadata during pendency of action). *See also, In re Payment Card Interchange Fee & Merchant Discount Antitrust Litigation*, 2007 U.S. Dist. LEXIS 2650 (E.D.N.Y. 2007) (where stipulated protocol eliminated metadata from production, defendant was stopped from objecting to productions made under that protocol, but going forward plaintiffs were to preserve and produce metadata).

ADMISSIBILITY

We sometimes forget that there is a point to all of this discovery other than the desire to inflict pain on an adversary. Presumably someday someone may want to use some portion of what was produced as means of proving or disproving a claim or defense. In *Lorraine v. Markel*, 2007 WL 1300739 (D. Md. 2007), Magistrate Judge Paul Grimm took the opportunity to expound on this subject, as presented by e-mails attached to summary judgment briefs without any supporting evidence as to their admissibility. In an opinion that is required reading for lawyers aspiring to use ESI to win a case, Judge Grimm delivered a sweeping review of prior case law and analysis of the Federal Rules of Evidence with respect to admissibility issues associated all manner of electronic evidence. What courts will require going forward in order to admit ESI as evidence remains to be seen, but lawyers should be thinking about this issue in pursuing and conducting discovery (and indeed clients should be thinking about it in managing their electronic information during the ordinary course of business).

NON-PARTIES

The recent amendments to Rule 45 presage that non-parties should expect to participate in e-discovery. *Auto Club Family Ins. Co. v. Ahner*, 2007 U.S. Dist. LEXIS 63809 (E.D. La. 2007) (ESI must be produced in response to a subpoena where burden of showing that ESI is "not reasonably accessible" not met); *see also United States v. Premera Blue Cross*, 2007 U.S. Dist. LEXIS 23213 (S.D. Ohio 2007) (non-party audit firm ordered to produce e-mails, plaintiff to pay cost of production). However, the parameters of e-discovery from non-parties are evolving, with courts showing sensitivity to non-party status in evaluating costs of compliance. *See Guy Chemical Co. v. Romaco AG, et al.*, 243 F.R.D. 310 (N.D. Ind. 2007) (requesting party pays cost of production from backup tapes deemed "not reasonably accessible" due to cost of $7,200).

CONCLUSION

Perhaps one of the most notable aspects of the past year in e-discovery cases is the lack of resolution to questions that have been haunting corporate counsel for years: What are the boundaries of the preservation obligation with respect to instant messaging? Voice mails? What does good faith require in implementing litigation holds (*see* page 1) and arresting routine destruction of ESI? Will attorney document review fees be subject to cost shifting under the right circumstances? What about shifting costs associated with ESI that is voluminous but accessible? These and other questions remain unanswered, and the fact is that even as opinions issue addressing these issue directly or indirectly, they are likely to be district court opinions, addressing particular factual circumstances, with no real precedential value.

However, certain core e-discovery truths become more firmly established with every new opinion: that corporations must have litigation hold procedures, that both inside and outside counsel will be held accountable for their clients' compliance at the risk of professional liability in the form of sanctions, and that the costs of electronic discovery to a large extent will be viewed by courts as part of the cost of doing business for large corporations. Whatever may be said about the uniformity or lack thereof in the federal court opinions in the year following the new FRCP, it is a certainty that the next year will see more flesh on the procedural rules bones as electronic discovery accounts for an ever-increasing proportion of all discovery.

—❖—