



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 7, NO. 2 PAGES 21-38

REPORT

FEBRUARY 1, 2007

HIGHLIGHTS**Records Retention Policies Must Evolve as E-Documents Become Norm**

In an interview with BNA, three partners from the Discovery Technology group at Jeffer, Mangels, Butler & Marmaro LLP, Los Angeles, discuss the impact of the new federal discovery rules on records retention policies. One effect is already clear: companies that fail to retain records that are relevant to litigation face sanctions, including the limitation of expert evidence on matters relevant to the undisclosed records. **Page 24**

Court Orders Defendants to Produce Original Documents in Options Case

Defendants charged with backdating stock option grants are ordered to produce a selection of original documents from a CD they originally proffered that contained more than 10,000 TIF-tagged image file documents. The lack of any readily apparent irregularities in the grants, however, saves them from having to make the majority of their production in original form. **Page 27**

Complaint Was Timely Filed, Even Though Computer Rejected It

A suit filed online within the applicable deadline is not time-barred just because it was rejected by a computer for bearing the wrong docket number. In some interesting dicta, the court equates a software system with a human being, at least for purposes of electronic filing. **Page 28**

NASD Charges Morgan Stanley With Failing To Provide, Destroying E-Mails

Morgan Stanley DW's problems with electronically stored information continue, as it is charged with rule violations for routinely failing to provide e-mails to claimants in arbitration proceedings and regulatory investigations, as well as for hiding and destroying e-mails. Morgan Stanley is also charged with having falsely claimed that millions of e-mails it possessed had been lost in the Sept. 11, 2001, terrorist attacks on the World Trade Center in New York, where its e-mail servers were housed. **Page 32**

Failure to Second-Guess Client's Evidence Results in Attorney's Suspension

A Wisconsin lawyer who continued to press a lawsuit without first making any meaningful inquiry into the authenticity of some fishy documents that his client supplied—including e-mails—receives a harsh reprimand. In finding that the lawyer violated Wisconsin's rule on competence, the court points out that the competency requirement is intended to protect the system of justice as well as the individual client. **Page 33**

Minding the Gap: Information Management Compliance Gap Analysis

Many organizations facing the challenges of information management and e-discovery struggle with the right way to get started. There is no shortage of books and articles that clearly identify the issues and challenges, but few that provide practical guidance on how to address them. Barclay T. Blair, of Kahn Consulting, Inc., describes a simple 10-step gap analysis methodology that organizations can implement immediately. **Page 34**

BNA CONFERENCES

UPCOMING EVENTS: BNA announces e-discovery conference dates for 2007. Six federal magistrate judges will participate in three programs moderated by Magistrate Judge Ronald J. Hedges of the U.S. District Court for the District of New Jersey. **Page 36**

ALSO IN THE NEWS

EMPLOYMENT ISSUES: Norway is considering a legal proposal that will redefine employers' right of access to employee work-related e-mail. **Page 37**

SCOPE: In a case involving workers' use of their employer's e-mail system, the National Labor Relations Board denies a motion to eliminate some of the questions the board had invited interested parties to discuss in amicus briefs, some of which deal with technology issues and retention policies. **Page 32**

FOURTH AMENDMENT: Federal agents with a search warrant authorizing the seizure of the drug testing records related to 10 named professional baseball players did not violate the Fourth Amendment by seizing an entire computer directory that contained the drug testing records of all major leaguers, as well as other professional athletes. **Page 29**



BNA, INC.

DIGITAL DISCOVERY & E-EVIDENCE REPORT

THE BUREAU OF NATIONAL AFFAIRS, INC., 1231 25TH STREET, N.W. WASHINGTON, D.C. 20037 (202) 452-4200

Paul N. Wojcik
PRESIDENT AND
CHIEF EXECUTIVE OFFICER

Gregory C. McCaffery
PUBLISHER AND
EDITOR-IN-CHIEF

Richard H. Cornfield
EXECUTIVE DIRECTOR

Robert A. Robbins
EXECUTIVE EDITOR

Carol L. Eoannou, MANAGING EDITOR (ceoannou@bna.com)

CORRESPONDENTS

Paul F. Albergo, *Chief of Correspondents*; Paul Connolly, *Assistant Chief of Correspondents*; Albany, N.Y., Gerald Silverman; Atlanta, Barney Tumey; Austin, Texas, Kurt Fernandez; Boston, Martha W. Kessler, Rick Valliere; Chicago, Michael J. Bologna, Thomas D. Wilder; Cincinnati, Bebe Raupé; Denver, Tripp Baltz; Houston, Susanne Pagano; Los Angeles, Tom Gilroy, Carolyn Whetzel; New York, Kip Betz, John Herzfeld; Norwalk, Conn., Steve Burkholder, Denise Lugo; Philadelphia, Lorraine McCarthy; Phoenix, William Carlile; Portland, Ore., Tom Alkire; Raleigh, N.C., Andrew Ballard; Sacramento, Calif., Laura Mahoney; San Francisco, Joyce E. Cutler; Seattle, Nancy Netherton; St. Louis, Christopher Brown; St. Paul, Minn., Mark Wolski; Tampa, Fla., Drew Douglas; Washington, Jeff Day; Williamston, Mich., Nora Macaluso

Correspondence concerning editorial content should be directed to the managing editor.

ABOUT BNA

For more than 70 years, BNA has been meeting the information needs of professionals and businesses across a wide range of fields, including:

- Business and Finance • Corporate Law • Employment and Labor Law • Environment and Safety • Health Care • Human Resources • Intellectual Property • International Law and Business • Litigation • Taxation

BNA also publishes books, software, and other online services, and offers product training and custom research, as part of BNA's mission to provide comprehensive solutions to customers' information needs.

SUBSCRIPTION INFORMATION

To subscribe to this or any BNA publication:

Call Customer Relations at 800-372-1033 or e-mail customercare@bna.com.

Visit <http://www.bna.com> for free trial information.

BNA PLUS

For custom service, documents, or research, call (800) 372-1033 or (202) 452-4994, or e-mail bnaplus@bna.com.

BNA BOOKS

BNA Books publishes some of the most respected titles and authors in their legal specialties. Editorial offices are located at 1231 25th St. N.W., Washington, D.C. 20037; telephone: (202) 452-4343; fax: (202) 452-4997, or e-mail books@bna.com. Contact BNA Books customer service offices by telephone at 800-960-1220 or by fax at (732) 346-1624.

TAX MANAGEMENT AND BNA SOFTWARE

BNA Software is a division of Tax Management, Inc., a premier provider of authoritative tax analysis, reference, and notification. Tax Management's services are available in print, on CD-ROM, and on the Web.

Copyright policy: Authorization to photocopy selected pages for internal or personal use is granted provided that appropriate fees are paid to Copyright Clearance Center (978) 750-8400, <http://www.copyright.com>. Or send written requests to BNA Permissions Manager: (202) 452-4084 (fax) or permissions@bna.com (e-mail). For more information, see <http://www.bna.com/corp/copyright> or call (202) 452-4471. For Customer Service call 800-372-1033 or fax 800-253-0332, or e-mail customercare@bna.com.

DIGITAL DISCOVERY & E-EVIDENCE REPORT (ISSN 1537-5099) is published monthly by The Bureau of National Affairs, Inc., 1231 25th St., N.W., Washington, D.C. 20037-1197. POSTMASTER: Send address changes to Digital Discovery and e-Evidence, BNA, P.O. Box 40949, Washington, D.C. 20016-0949

In This Issue

Leading the News / Page 24

Court News / Page 27

Regulatory News / Page 32

Legal Ethics / Page 33

Records Management / Page 34

Conference Report / Page 36

International News / Page 37

Journal / Page 38

TOPICAL INDEX

BEST PRACTICES Records retention policies must evolve as electronic documents become the norm and procedural rules on production change, according to a group of attorneys interviewed by BNA 24

FORM OF PRODUCTION Defendants are ordered to produce original documents in an options case 27

FORENSIC TESTIMONY The Supreme Court declines to review a Texas rule authorizing a judge to take judicial notice of the reliability of expert testimony 27

E-FILING A complaint is timely filed, even though a computer rejected it 28

FOURTH AMENDMENT The United States has broad authority to seize e-files mixed with evidence taken from the warrant's target 29

ADMISSIBILITY A computer expert's opinion on the scope of a search is an inadmissible legal conclusion 29

MOTION TO QUASH A subpoena to a Web host seeking a poster's identity will be quashed if the claim cannot survive summary judgment 27

BEST PRACTICES A 10-step process for conducting an information management compliance gap analysis is described 34

AUTHENTICITY Failure to second-guess a client's 'evidence' results in attorney's two-month suspension 33

EMPLOYMENT ISSUES Revision of employer right to access employee e-mail is debated in Norway 37

SECURITIES REGULATION NASD charges Morgan Stanley with failing to provide, and destruction of e-mails 32

SCOPE National Labor Relations Board will hear questions regarding technology and policy in e-mail case 32

SAVE THE DATES BNA 2007 conference series finalized 36

CONFERENCES & MEETINGS 38

TABLE OF CASES

Novellus Systems Inc. Derivative Litigation, In re (N.D. Cal.) 27

Sanders v. U.S. (U.S.) 27

Farzana K. v. Indiana Department of Education (7th Cir.) 28

U.S. v. Shaffer (10th Cir.) 29

McMann v. Doe (Ariz. Super. Ct.) 27

Nunnery, In re (Wis.) 33

Guard Pblng. Co. (NLRB) 32

Leading the News

BNA recently interviewed Stanley M. Gibson, Michael A. Gold, and Dan P. Sedor, partners in the Discovery Technology group at Jeffer, Mangels, Butler & Marmaro LLP, Los Angeles. They answered questions about records retention policies and the impact of the new federal discovery rule.

Companies that fail to retain records that are relevant to litigation face sanctions, the interviewees caution. One sanction, they say, is the limitation of expert evidence on matters relevant to the undisclosed records.

Records Retention Policies Must Evolve as Electronic Documents Become the Norm and Procedural Rules on Production Change

*INTERVIEW WITH STANLEY M. GIBSON, MICHAEL A. GOLD,
AND DAN P. SEDOR, PARTNERS IN THE DISCOVERY
TECHNOLOGY GROUP AT JEFFER, MANGELS, BUTLER &
MARMARO LLP, LOS ANGELES*

BNA: Which people or department(s) in a company typically have primary responsibility for establishing and then periodically reviewing and updating a records retention plan?

Sedor: Prior to the prevalence in litigation of electronically stored information—ESI—the task of preparing and revising records retention plans usually fell to a records manager, office administrator, or human resources manager, who would often work together with company counsel to figure out the various periods that specific records would have to be retained to comply with the law. With the advent of ESI in litigation, IT personnel started taking on duties in connection with records retention, and the focus of the design, implementation, and enforcement of retention policies has been shifting to a combination of legal and IT personnel.

Interestingly, IT personnel are often put in the uncomfortable position of having to enforce unpopular retention policies on which the actual users of the ESI have had little or no input. Not surprisingly, they often meet resistance. The best retention plan is one that accommodates the needs of the business—and its employees—while helping to ensure compliance with regulatory and litigation requirements. That sort of policy cannot be drafted or updated in a vacuum. It needs the participation of key department heads as well as the IT, legal, and records management functions, and the sponsorship of senior management.

BNA: You have written that having too many records is something that a company should avoid. Why would that be a problem?

“The attorney review for relevance to a particular case and privilege is frequently the most time consuming and expensive part of e-discovery. Proper records management will significantly reduce these costs and increase business efficiency.”

JEFFER, MANGELS,
BUTLER & MARMARO LLP

Gibson: Maintaining too many records decreases business efficiency and dramatically increases the costs of e-discovery. A company should focus on the reasons it maintains records, for business reasons, regulatory requirements, and legal holds. Records that do not fall within these categories should not be retained. Retaining unnecessary records makes it much more difficult to locate what records are needed by the company. It also increases the cost of e-discovery significantly by forcing the company and its attorneys to review records that should not have been retained in the first place. The attorney review for relevance to a particular case and privilege is frequently the most time consuming and expensive part of e-discovery. Proper records management will significantly reduce these costs and increase business efficiency.

BNA: Are there any federal or state laws that mandate the destruction of records (as opposed to the retention of records)?

Sedor: Yes. One area of focus of such laws is the destruction of employee and consumer information. The

Federal Fair and Accurate Credit Transactions Act requires the actual destruction of personal information of former employees and consumers before it is discarded. On the state side, Michigan, among others, requires employers to protect employee Social Security numbers and other personal information. Among other things, Michigan employers must adopt document destruction protocols.

BNA: Are there any states that impose unusual or noteworthy records retention requirements on companies that do business in those states?

Gold: Every state has some form of document retention regime, driven in varying measures by the state's corporations, tax, employment, environmental, and procedural litigation laws and regulations. Almost half of the states have enacted a personal information security law of some kind, with California having taken the lead in 2003 with the enactment of its law. While not strictly 'unusual' or 'noteworthy,' these laws do bear, at least in some measure, on company records retention policies. That is because all companies operating in jurisdictions with such laws must be cognizant of the need to make sure that information covered by these laws is appropriately and effectively accounted for in their retention policies and is properly safeguarded from hackers or unauthorized insiders.

BNA: If a corporation does business in a number of foreign countries, how should it determine to what extent the laws of those countries affect the way it designs its records retention policy?

Gold: There is no substitute for employing the service of knowledgeable legal counsel in the foreign jurisdiction in question. In the U.S., applicable document retention laws and regulations are more or less accessible through routine research. This is also the case in many, but not nearly all, foreign jurisdictions. Many countries have overlapping regulations at the national or local levels. In Milan, Italy, for example, the city-state's laws will bear upon document retention, along with the laws of the local Italian province, the Italian national government, and the Maastricht Treaty of the European Union. In China, for another example, certain elements of the retention regime are more or less anecdotal and are not set forth in any written law.

A U.S. multinational company must also be cognizant of foreign privacy laws in designing its retention policies. A U.S. company with purely domestic operations has more latitude on privacy issues in the context of its retention policy. But the European Union's Privacy Directive, for instance, seriously limits a company's flexibility in dealing with stored documents that are governed by that law. Finally, as in the U.S., the foreign retention policy must take account of litigation imperatives and the need to know the location of stored information and how to access it without violating privacy laws in the event of litigation, regulatory enforcement action, or investigation.

BNA: You have written that "an essential component of any records retention plan is a litigation hold procedure designed to ensure that relevant records are not lost or destroyed when litigation has commenced or is reasonably anticipated." When should a company treat litigation as "reasonably anticipated" and what procedures should the company follow in implementing a "litigation hold"?

Gibson: Litigation hold procedures are frequently the least well understood aspects of e-discovery. Compa-

nies should implement a litigation hold when they reasonably anticipate litigation. Although there is no definitive guideline for exactly when a company reasonably anticipates litigation, it will generally occur before a company is served with a lawsuit, and a company should put a litigation hold in place when it believes that it is likely to be sued either because of the particular circumstances at issue or because it is routinely sued in similar circumstances.

To institute the litigation hold, the company should issue concise directives to the appropriate employees and suspend the routine destruction of documents as appropriate. All directives should be in writing and should require a confirmation from the employee receiving the directive that he or she will comply. In addition, the litigation hold should be reviewed and updated on a regular basis.

**The amended federal discovery makes it
"imperative for corporate counsel to interact
closely with IT and understand where and how
e-data is stored within the company."**

JEFFER, MANGELS,
BUTLER & MARMARO LLP

BNA: What sanctions can a court impose if a company fails to retain records that are relevant to litigation?

Sedor: To begin with, it's important to keep in mind the relatively low culpability threshold required for the imposition of sanctions. Willful intent to destroy or conceal evidence is not required. To the contrary, harsh sanctions can issue against litigants who have merely failed to suspend existing automatic deletion programs.

There are a variety of sanctions available, running the gamut of harshness from simple monetary sanctions, to limitations on evidence and testimony, to adverse inference instructions, and even to default judgments. Monetary sanctions can range from tens of thousands to hundreds of thousands of dollars, and may include the award of attorneys' fees. Evidentiary sanctions can take the form of orders limiting the sanctioned party's evidence or testimony or restricting the sanctioned party's ability to object to the other side's evidence. Courts have focused on evidence that was not timely or properly produced, but may also limit expert testimony on pertinent subjects.

An adverse inference instruction is a charge to the jury that they are to draw an adverse inference from the sanctioned party's conduct, such as by assuming that missing evidence would have been damaging to that party's case. The adverse inference instruction can be and often is case-determinative. Default judgments are at the far end of the sanction spectrum—the most serious sanction possible. In a few cases, the sanctioned party's conduct has been found to be so improper that this most serious of terminating sanctions was warranted.

BNA: Amendments to the Federal Rules of Civil Procedure became effective on Dec. 1, 2006, that specifically address e-discovery and electronically stored in-

formation. How do the new rules affect what corporate counsel should be doing concerning corporate records?

Gibson: Corporate counsel have a new obligation to ensure that the company properly manages e-data. It will be imperative for corporate counsel to interact closely with IT and understand where and how e-data is stored within the company. In addition, corporate counsel must also ensure that the company's outside counsel understand the company's e-data. Outside counsel will be called upon to make regular statements to opposing counsel and the court regarding the company's e-data and whether it is reasonably accessible or not reasonably accessible because of undue burden or expense. Corporate counsel have a new role to play to coordinate between the business units, IT, and the outside counsel.

BNA: What is spoliation and what are some of the problems that can inadvertently arise for a company concerning this if the company is not careful with its records?

Sedor: The Sedona Conference, an influential group of commentators in the areas of electronic document retention and discovery, defines spoliation very simply as the destruction of records which may be relevant to ongoing or anticipated litigation, government investigation, or audit. The problem with ESI is that it is easier to delete or modify than hard copy records. In fact, aspects of an electronic file such as its metadata—i.e., data about the electronic file such as who created it and when it was last accessed or modified—can be altered simply by accessing or copying the file. If that sort of information is important, its alteration conceivably could constitute spoliation.

However, under new Federal Rule of Civil Procedure 37(f), the loss of potentially relevant ESI is not subject to sanction under the rule if it was lost as a consequence of the routine, good-faith operation of a computer system. In each instance where a litigant loses potentially relevant ESI, it will need to show that steps were taken to preserve that ESI in order to meet the good-faith requirement and that the loss occurred as a consequence of routine procedures notwithstanding those preservation steps. One key element of any good-faith showing will be the implementation of the sort of litigation hold procedure that we discussed earlier. Such a procedure should help to prevent the deletion of potentially relevant e-mails by users and from servers and the overwriting of backup media that may be the sole source of potentially relevant ESI. Litigants who fail to design, implement, and monitor compliance with a litigation hold when it is required are courting disaster in the form of sanctions if any potentially relevant ESI is lost as a result.

BNA: How does a company's need to maintain the privacy of certain records affect how it designs its records retention plan?

Gold: In a few different ways. First, federal and state privacy laws may limit or restrict access to certain records, even internally within the company that has created or maintains the records. Thus, a sound retention plan must assign appropriate 'privacy values' to certain classes of records and ensure that its enforcement protocols impose appropriate measures to limit or

restrict access to the records in a manner consistent with the applicable privacy laws.

Second, the company's enforcement protocols must specify appropriate sanctions for breaches of the privacy rules and those sanctions must be uniformly enforced. A failure to provide for appropriate sanctions or to enforce the sanctions in the event of lapses may directly constitute a violation of the privacy law itself. And in some cases, such a failure may at a minimum give rise to an inference that the company has breached a privacy law.

“Litigants who fail to design, implement, and monitor compliance with a litigation hold when it is required are courting disaster”

JEFFER, MANGELS,
BUTLER & MARMARO LLP

Either way, the result could be a regulatory enforcement action or a consumer class action lawsuit or a derivative shareholders lawsuit. Privacy considerations are at least equally important for the retention policies of multinational corporations. This is because certain foreign jurisdictions have laws that provide greater protection for personal consumer information (such as the European Union's Privacy Directive).

BNA: Should a records retention plan have any specific procedures concerning personal records, as opposed to business records?

Gibson: A records retention plan should specify that personal records should not be stored on company computers. If this is impractical for a particular company, then personal records should be stored in a designated location only. Employees should be reminded that personal records on company computers are company property and are not private. The company should also advise employees that the company may be called upon to disclose personal records stored on company computers in certain situations, such as regulatory investigations or lawsuits.

BNA: Are there any specific procedures that a company should employ in order to minimize the likelihood that it may be unable to assert the attorney-client or work-product privilege concerning the appropriate records retention plan?

Gibson: A company should have its records retention plan audited and reviewed under the direction of legal counsel (and in certain cases outside counsel) to make sure that any audit and recommendations from the audit remain protected by the attorney-client privilege. There will be many recommendations that will come from a review and an audit of the records retention plan, some of which the company may decline to implement. In order to avoid having the audit and recommendations disclosed in legal proceedings, the audit and recommendations should be supervised and driven by counsel, which will best ensure that the attorney-client privilege applies.

Court News

Motion to Quash

No Subpoena to Web Host for Poster Identity If Lawsuit Cannot Survive Summary Judgment

A defamation plaintiff seeking the identity of an anonymous online speaker must assert a claim detailed enough to survive a motion for summary judgment before a court will compel disclosure of the speaker's identity, the Arizona Superior Court held Jan. 18 (*McMann v. Doe*, Ariz. Super. Ct., No. cv2006-092226, 1/18/07).

The court granted a defendant's motion to quash subpoena requests based on a finding that the plaintiff failed to meet the standard set out in *Doe v. Cahill*, 884 A.2d 451 (Del. 2005) (*DDEE*, November 2005, p. 7). The *Cahill* court held that, for a court to compel disclosure of an anonymous speaker's identity through discovery, the plaintiff must plead facts sufficient to survive summary judgment, and must afford the speaker an opportunity to file an opposition.

After business transactions with plaintiff Paul McMann went sour, the anonymous defendant in the case before the court set up the defamatory Web site www.paulmcmann.com, which included an interactive message board where visitors were encouraged to share their dislike of the plaintiff.

The plaintiff first sought to identify the defendant by subpoenaing the defamatory site's hosts, Domains by Proxy and GoDaddy, in Massachusetts, where the plaintiff's business was located. That effort was rejected for lack of jurisdiction. The Arizona court did not evaluate jurisdiction, but again denied the request because the plaintiff's substantive allegations were too insubstantial to compel discovery of the defendant's identity.

"The Court believes that the correct standard to be applied in this situation is that announced in *Doe v. Cahill*," Judge Christopher Whitten wrote. Because the plaintiff's complaint did not set out accusations with the specificity and definiteness required to survive summary judgment, and because the notice to the defendant was defective, the court ruled that the plaintiff failed to meet the *Doe v. Cahill* standard.

Full text of the court's opinion is available at <http://ddee.bna.com>.

Forensic Testimony

Supreme Court Declines to Review Texas Rule Judge Can Take Judicial Notice of Reliability

The U.S. Supreme Court denied review Jan. 12 a case in which a criminal defendant said a state trial court should not have admitted expert testimony of state forensic computer examiner who recovered child

pornography from computer media found in the defendant's apartment using EnCase computer program (*Sanders v. U.S.*, U.S., 06-761, review denied 1/12/07).

The defendant asked the Supreme Court to overturn the decision by the Texas Court of Appeals. The state court reasoned that use of EnCase under these circumstances has previously ruled to satisfy the *Daubert/Kelly* criteria for reliability by another Texas court of appeals. And, the appeals court said, under *Hernandez v. State*, 116 S.W.3d 26 (Tex. Crim. App. 2003), once some courts have determined scientific reliability and validity of specific methodology to implement or test particular scientific theory, other courts may take judicial notice of reliability of that particular methodology.

The petitioner presented the following questions: (1) Does the Texas rule of *Hernandez v. State*, allowing taking of judicial notice of reliability of expert or scientific methodology in a criminal case, violate a criminal defendant's rights to equal protection or due process? (2) Why should the State of Texas be allowed a lower burden for admission of expert testimony in a criminal proceeding than a similarly situated proponent in a civil proceeding when the prosecution in a criminal proceeding must carry a substantially higher burden of proof than a civil litigant to prevail? (3) Why should a litigant be deprived of his right to notice of and to challenge the taking of judicial notice?

The petition for certiorari was filed by Leigh W. Davis, of Fort Worth, Tex.

Form of Production

Court Orders Defendants to Produce Original Documents in Options Case

The U.S. District Court for the Northern District of California Jan. 5 ordered defendants charged with backdating stock option grants to produce, as part of their initial disclosures, the original documents referenced in a CD containing more than 10,000 TIF—tagged image file—documents (*In re Novellus Systems Inc. Derivative Litigation*, N.D. Cal., Master File No. C06-03514 RMW (HRL), 1/5/07).

However, in an unpublished opinion by Magistrate Judge Howard R. Lloyd, the court said the defendants need not produce, as part of their initial disclosures, all documents they reviewed in concluding that there were "no irregularities" in the granting of the challenged stock options.

Alleged Backdating. The court recounted that this lawsuit is a shareholder derivative action based on charges that Novellus Systems Inc. and others improperly backdated Novellus stock-option grants. As part of their initial disclosures under Fed.R.Civ.P. 26(a), the defendants produced a CD containing documents that, the defendants "apparently contend, show that the stock

option grants mentioned in the complaint were authorized.”

However, the plaintiffs rejoined, the CD contains more than 10,000 TIF documents, “some of which bear illegible fax lines or show irregularities in Novellus’ stock option grants (e.g., as to the dates of signature pages on the purported authorizations.” They moved the court to compel an inspection of the original documents and for an order compelling the defendants to produce, as part of their initial disclosures, “ ‘all documents reviewed in the course of their determination that there were no irregularities.’ ”

Fairness. Granting the motion in part, the court acknowledged that the relevant portion of Rule 26(a)(1) “does not expressly provide for the inspection of the disclosed documents. Nonetheless, it said it “sees no reason why plaintiffs should not be allowed to inspect the originals of an apparent handful of documents which they claim are illegible or show facial irregularities as to signature dates and the like.”

“Fairness would seem to require it,” the court reasoned, adding that permitting an inspection would not violate a stay of further discovery pending resolution of the defendants’ “anticipated” dismissal motion. “At any rate, defendants do not show, or even argue, that an inspection would impose an undue burden.”

No Grounds. However, the court declined to order the defendants to produce as part of their initial disclosures all documents they reviewed in the course of deciding that the option grants were proper. It explained that Rule 26 requires a party to disclose only such documents it may use to support its claims or defenses.

“In essence,” the court reasoned, “plaintiffs’ motion is based upon their contention that defendants will be unable to successfully defend this lawsuit with the documents provided in their initial disclosures. Suffice to say that each side will have an opportunity to present its arguments as to the evidence at the appropriate time; and, the decision as to what is to be disclosed under [Rule] 26(a) is not without risk.” As such, the court found “no grounds to compel defendants to produce any further documents in connection with their initial disclosures.”

Full text of the court’s opinion is available at <http://ddee.bna.com>.

E-Filing

Complaint Was Timely Filed, Even Though Computer Rejected It

A suit filed online within the applicable deadline is not time-barred just because it had the wrong docket number and was rejected by a computer, the U.S. Court of Appeals for the Seventh Circuit decided Jan. 4 (*Farzana K. v. Indiana Department of Education*, 7th Cir., No. 06-1632, 1/4/07).

A court clerk would have to accept such a complaint despite its defective number, and an e-filing system “cannot reject any paper that the clerk must accept,” Chief Judge Frank H. Easterbrook said.

A mother dissatisfied with services the local public school was offering for her autistic teenager filed an In-

dividuals with Disabilities Education Act suit. A federal district court, noting that administrative remedies were available, dismissed the suit in December 2004. Six months later, on June 6, 2005, a final administrative ruling issued. The plaintiff’s attorney electronically filed a complaint for judicial review in federal district court in Indiana on July 6, 2005, just within the 30-day limitations period allowed under the applicable state law.

The computer rejected the filing because it was captioned with the docket number of the earlier 2004 case, which had been closed. Nonetheless, the computer forwarded copies to defense counsel. Paper copies followed the electronic filing, but the clerk’s office was closed by the time the courier arrived. The plaintiff’s attorney tendered a new complaint on July 8, but with the docket number left blank. The district court held that it lacked subject matter jurisdiction because the July 8 filing was too late.

Tolling Principles Do Not Apply. The plaintiff argued that equitable tolling covered the brief delay, but the court disagreed. Equitable tolling principles apply when “timely filing is not possible despite diligent conduct,” the court said. “Waiting until the last hours is not diligent; the errors that often accompany hurried action do not enable the bungling lawyer to grant himself extra time.”

The court acknowledged that the 30-day time limit was borrowed from state law in this case. However, no Indiana case law or other authority has been presented to show that the state would permit equitable tolling here, it said.

In any event, tolling is unnecessary because the complaint was filed on time, the appeals court said. The July 6, 2004, electronic filing occurred on the 30th day after the state agency’s final decision on the IDEA matter, and defendant school district personnel clearly received their copies of the complaint within the 120-day time limit allowed under Fed.R.Civ.P. 4(m), it said.

The defendants contended that the computer’s rejection of the complaint meant that filing did not occur, but the court saw things differently. The “computer’s reaction does more to show the limits of some programmer’s imagination than to render the suit untimely,” the court said. If a paper form of the complaint had been hand delivered to the clerk’s office, a deputy clerk “would have crossed out the old docket number, stamped a new one, and filed the document; there is no reason to throw this suit out of court just because the e-filing system did not know how to take an equivalent step.”

Software is ‘the Clerk.’ Fed.R.Civ.P. 5(e), which describes a “filing of papers with the court,” was specifically amended in 1993 to state that the clerk “shall not refuse to accept for filing” any paper presented for filing “solely because it is not presented in proper form as required by these rules or any local rules or practices,” the court pointed out. Characterizing e-filing system software as “the clerk” for Rule 5 purposes, the court said that “a step forbidden to a person standing at a counter is equally forbidden to an automated agent that acts on the court’s behalf.”

Two Seventh Circuit opinions have interpreted Rule 5(e) to require that a complaint must be accepted and filed even if the required fee does not accompany the submission, the court noted. Thus, although dismissal

will occur if the fee is not paid promptly, a brief delay does not trigger that same result, it said.

Turning to other circuits, the court noted a dearth of appellate opinions on the subject. However, it referenced the Fifth Circuit's ruling in *McClellon v. Lone Star Gas Co.*, 66 F.3d 98 (5th Cir. 1995), that a district court must accept a paper that expresses only the plaintiff's bare allegation that "I have been denied the opportunity to return to work after being released from the doctor from an on-the-job injury."

The bottom line is that a clerk "must take in whatever is tendered," the court said. Problems may lead to a rejection later on, "but the initial filing ensures that the process of vetting papers for compliance with the rules does not prevent satisfaction of time limits," it said. Here, the complaint was timely filed on July 6 and should have been accepted, even though revision was in order to indicate that a new suit was being commenced, it said.

In dismissing the complaint, the district court also cited as a reason the fact that the complaint had not been verified as required by Indiana law. The appeals court pointed out, however, that federal law imposes no such requirement, so that "the district court erred" by basing its dismissal on a mandate "that governs only in state court."

Judges Richard A. Posner and Kenneth F. Ripple joined the opinion.

Matthew D. Cohen, Monahan & Cohen, Chicago, argued for the plaintiff. George T. Patton, Bose, McKinney & Evans, Indianapolis, argued for the defendants.

Full text at <http://pub.bna.com/lw/061632.pdf>.

Admissibility

Computer Expert's Opinion on Scope Of Search Was Inadmissible Legal Conclusion

A computer expert could not testify that a defendant charged with distribution and possession of child pornography was "on a fishing expedition" for general porn, not specifically child porn, the U.S. Court of Appeals for the Tenth Circuit ruled Jan. 3 (*U.S. v. Shaffer*, 10th Cir., No. 06-3145, 1/3/07).

The expert's opinion went to intent, or mens rea, which was an essential element of the criminal case, the Tenth Circuit said. Federal Rules of Evidence 704(b), the court said, prohibit an expert from giving "an opinion or inference as to whether the defendant had the mental state or condition constituting an element of the crime charged or of a defense thereto," the court said.

Kazaa's P2P Files. Aaron Shaffer was convicted of distributing child pornography when he downloaded images and videos from a peer-to-peer (P2P) computer network and stored them in a shared folder on his computer accessible by other users of the network.

Kazaa is a peer-to-peer computer application that allows users to trade computer files through the Internet. Kazaa users store the files they download from the shared folders of other Kazaa users. Anything one has in one's own Kazaa shared folder may be accessed and downloaded by other Kazaa users. Kazaa's software shows the user exactly how many of his or her files are being accessed and copied by other Kazaa users.

Ken Rochford, an Arizona-based special agent from the U. S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, noticed that a Kazaa account user with the screen name shaf@Kazaa had in his shared folder accessible to other Kazaa users a large number of files containing images and videos of child pornography. Rochford downloaded some of those images from shaf@Kazaa onto his own computer. Shaffer was charged with and convicted of distributing child pornography.

Shaffer's primary defense at trial was that he did not have the requisite mental state—that he did not knowingly possess or distribute child pornography.

'A Porn Fishing Expedition.' At trial, Shaffer proffered a computer expert to testify that, based upon the file structure of Shaffer's computer hard drive, he was on a "porn fishing expedition with no particular calculation toward any particular type of material, other than generally sexually explicit material."

After a *Daubert* hearing, the trial judge ruled that the proposed testimony went to Shaffer's state of mind—mens rea—vouching that Shaffer did not mean to seek out or disseminate illegal child pornography. The court ruled the proposed opinion was inadmissible, because expert witnesses are "not allowed to testify about the ultimate [issues] in the case."

On appeal, Shaffer argued that the trial court erred in refusing to permit the proffered testimony.

The court of appeals disagreed.

Shaffer's expert tried to suggest to the jury that Shaffer "did not knowingly possess or distribute unlawful child pornography as opposed to simple adult pornography," the Tenth Circuit wrote. "Yet it was precisely this issue that was hotly contested in, and an essential element of, the crimes with which he was charged," the court said.

Judge Neil M. Gorsuch wrote the opinion.

Christopher M. Joseph, Joseph & Hollander, Topeka, Kansas, represented Shaffer. Assistant United States Attorney James A. Brown represented the United States.

Full text of the court's opinion is available at <http://ddee.bna.com>.

Fourth Amendment

Ninth Circuit Rules U.S. Has Broad Authority To Seize E-Files Mixed With Warrant's Target

Federal agents with a search warrant authorizing the seizure of the drug testing records related to 10 named professional baseball players did not violate the Fourth Amendment by seizing an entire computer directory that contained the drug testing records of all major leaguers, as well as other professional athletes, a split U.S. Court of Appeals for the Ninth Circuit decided Dec. 27 (*United States v. Comprehensive Drug Testing Inc.*, 9th Cir., No. 05-10067, 12/27/06).

The court's ruling gives the government broad authority—even in cases involving records implicating strong privacy interests—to seize records outside the scope of a search warrant when they are intermingled with records described in the warrant.

For decades now, courts across the country have struggled with identifying what the Fourth Amendment requires of law enforcement officers when they encounter computerized records that contain files covered by a search warrant intermingled with private information outside the reach of the warrant. In an opinion by Judge Diarmuid F. O'Scannlain, the Ninth Circuit rejected arguments that the Fourth Amendment required the government, prior to seizing intermingled computer files, to conduct "key word" searches or to have a magistrate or a trained computer specialist screen the files to determine which were actually covered by the warrant.

Playing Hard Ball The issue came up in a criminal investigation of the alleged involvement of the Bay Area Lab Cooperative (Balco) in illegal steroid use by athletes.

Companies that administered Major League Baseball's drug testing program, along with the MLB players' union, filed motions to return records and specimens seized from the companies that were unrelated to 10 Balco-connected players who were the initial targets of a grand jury investigation and a search warrant. Ninth Circuit precedent states that one of the factors a court is to consider when determining whether to entertain a motion to return property that has been seized pursuant to a search warrant is "whether the Government displayed a callous disregard for the constitutional rights of the movant."

District courts in this case granted the motions to return after determining that the government callously disregarded the Fourth Amendment by, among other things, seizing a copy of a computer directory and other records that contained information relating not only to the 10 players initially targeted, but also to professional athletes in other sports and to other MLB players who tested positive for steroids during the 2003 season. The players had submitted to drug testing as part of a collective bargaining agreement that assured them of the confidentiality of the test results.

Prosecutors began their quest for the testing records first by issuing a grand jury subpoena to one of the drug testing companies, Comprehensive Drug Testing (CDT). This first subpoena sought all of CDT's MLB drug testing records. The government later issued a second subpoena that sought drug testing records relating only to 11 players the government had linked to Balco.

However, when prosecutors learned of plans by CDT and the players' union to file motions to quash the subpoenas, they obtained a search warrant authorizing the seizure of CDT's drug testing records relating to 10 MLB players tied to Balco, as well as more general records relating to CDT's administration of MLB's testing program. The warrant provided that, if an on-site search of computer files was impracticable, seizure of either a copy of all data or the computer equipment itself was authorized if "law enforcement personnel trained in searching and seizing computer data" determined that such a course was appropriate. If seizure of all data or equipment was necessary, "appropriately trained personnel" would review the data, retaining the evidence authorized by the warrant and designating the remainder for return.

Among the records seized by federal agents executing the warrant were records of all positive drug tests by MLB players and a voluminous computer directory that contained all the files for all of CDT's professional

sports testing programs. On the recommendation of an agent with special computer training, the government copied the entire directory for an off-site search.

After reviewing these records, agents obtained additional warrants expanding the scope of the investigation to include another drug testing company and the testing records and specimens of all MLB players who tested positive.

Intermingled Records The course taken by the government in this investigation deviates from the one charted in Justice Department guidelines, and from the procedures for seizing intermingled records set out in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982). Nevertheless, the Ninth Circuit decided that the government's conduct was not "unreasonable" under the Fourth Amendment, and thus did not demonstrate a callous disregard for the players' and drug testing companies' constitutional rights.

District courts that granted the motions to return property emphasized that DOJ regulations and the U.S. Attorney's Manual state that a search warrant should not be used to obtain treatment records when a subpoena would suffice, and that prosecutors should not resort to a search warrant on the basis of a third-party record holder's decision to move to quash a subpoena.

The appeals court, however, said that any violations of DOJ guidelines in this case would not be "unreasonable" for constitutional purposes and thus would not support granting a motion to return property.

Alternative Investigative Procedures As for the procedures set out in *Tamura*, the court emphasized that *Tamura* involved a wholesale seizure of all of a company's records and that the guidance offered in that case for handling intermingled records was dicta.

The court in *Tamura* states:

In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arrest Procedure.

Although the government in this case had its own agents, rather than a magistrate, review the intermingled records, the Ninth Circuit stressed that *Tamura* recognized that procedures other than sealing and magistrate review might suffice to protect constitutional privacy interests in intermingled records. The court pointed out that the initial CDT warrant required a government agent with computer training to determine a reasonable way to conduct a search of intermingled records. This was more care than the agents exercised in *Tamura*, the court noted.

The players' union argued that even the minimal protective procedures set out in the first CDT warrant were not followed in this case because the lead case agent reviewed the computer directory personally rather than having the specialist review the records by himself. The appeals court, however, said the warrant required a computer specialist only to make the call regarding an off-site search, and that the warrant allowed any "appropriately trained personnel" to review the seized files. The term "appropriately trained personnel" in this context, the court said, could be any agent who knew

how to highlight a file name in a computer directory and hit the enter key.

Key Word Searches Nor did the Fourth Amendment's concept of reasonableness require the government to conduct key word searches of the computer records to identify those that pertained to the players named in the warrant, rather than to copy the entire computer directory for agents' off-site review, the Ninth Circuit continued.

Although the computer subdirectories seized by the government in this case were labeled by a sports organization, and although the files were saved by the players' names, the government could not be sure that searching by key words would turn up everything linked to the 10 players named in the warrant. The court noted, for example, that the other lab that administered MLB drug tests saved records by testing numbers rather than names, and that the numbers could not be linked to specific players through any documents found on the premises of that facility. The court said:

The government had no duty to rely on CDT to illuminate the files seizable under the warrant. Like most searched parties, CDT had an incentive to avoid giving over documents the government might not know to miss. The government had no reason to confine its search to "key words" such as the names of the baseball players. Such a limited search could easily have overlooked relevant documents.

Post-Seizure Remedies While the circuit court disagreed with the district courts' conclusions that the government had callously disregarded constitutional rights, the court ultimately ruled that other factors, including the athletes' strong privacy interests in the records, made it appropriate for the district courts to exercise equitable discretion to hear the motions to return property.

On the other hand, the court said the district courts erred by ordering the return of all records other than the ones pertaining to the 10 players named in the first CDT warrant. After confirming that the government's seizure of all the records and specimens was constitutional, the court went on to hold that post-seizure sealing and review by a magistrate is "necessary to ensure that the seizure of intermingled records remains reasonable."

"We conclude," the court said, "that upon a proper post-seizure motion by the aggrieved parties, the record should be sealed and reviewed by a magistrate—such as the one who originally issued the warrant. This procedure affords the necessary protection against unreasonable retention of property after a seizure of intermingled computer data." Accordingly, the court remanded the cases to the district courts to conduct these reviews of the sealed records.

The court commented that, although most computer files can be pared down, spreadsheets of a only a few pages may be retained in whole, under the authority of 20th century case law approving the seizure of entire ledgers containing any evidence described in a warrant.

Judge Richard C. Tallman joined in the opinion.

Dissent Warns of Broader Implications In a dissenting opinion, Judge Sidney R. Thomas said the record in this case supported a district judge's finding that the search warrant naming the 10 players linked to Balco was a pretext for obtaining the drug testing records of all MLB players. Among other criticisms of the court's holding, Thomas said the majority's rule "would entitle the government to seize the medical records of anyone who had the misfortune of visiting a hospital or belonging to a health care provider that kept patient records in any sort of master file which also contained the data of a person whose information was subject to a search warrant."

Thomas said that the court should require that the government engage in a targeted search of a database to identify only those documents for which it has an approved need. "A relational database, such as the one at issue in this case, is one in which the database is organized and accessed according to the relationships between data items without the need for any consideration of physical orientation and relationship. Software programs allow the examination and correlation of information. A relational database provides the perfect vehicle for segregating non-relevant information," Thomas said.

Erika R. Frick, of the U.S. attorney's office in San Francisco, argued for the government. Elliot R. Peters, of Kecker & Van Nest LLP, San Francisco, argued for Comprehensive Drug Testing Inc. and the Major League Baseball Players Association.

Full text of the 115-page opinion is available at <http://ddee.bna.com>.

Regulatory News

Securities Regulation

NASD Charges Morgan Stanley With Destroying, Failing To Provide, E-Mails to Claimants

NASD announced Dec. 19 that it charged Morgan Stanley DW Inc. with rule violations for routinely failing to provide e-mails to claimants in arbitration proceedings and regulatory investigations, as well as hiding and destroying e-mails from October 2001 through March 2005.

In addition, the self-regulatory organization alleged that Morgan Stanley falsely claimed that millions of e-mails it possessed had been lost in the Sept. 11, 2001, terrorist attacks on the World Trade Center in New York, where its e-mail servers were housed.

In fact, according to the NASD, Morgan Stanley possessed millions of pre-Sept. 11 e-mails that had been restored to its system shortly after the attacks using back-up tapes. Allegedly, many other e-mails were maintained on individual users' computers and were therefore never affected by the attacks. NASD charged that Morgan Stanley often failed to search those computers when responding to requests.

Also, the firm was charged with destroying millions of e-mails during the relevant period.

Morgan Stanley Statement. Morgan Stanley provided BNA with the following statement Dec. 19: "The 9/11 attacks destroyed the Firm's legacy Dean Witter email servers and archives. When prior management learned there were still backup emails from that era that might bear on arbitrations, it informed regulators, plaintiffs' counsel and outside counsel; built searchable databases; produced newly discovered emails; and cooperated fully with the NASD's review."

The statement continued, "Current management has made extensive efforts to reach a fair and appropriate settlement of this matter, but the NASD's disproportionate and unprecedented demands leave us no choice but to litigate. We look forward to having this issue heard by an impartial hearing panel."

Counsel to Morgan Stanley was not immediately available for comment.

Overwriting Backup Tapes. Further, NASD charged that Morgan Stanley later destroyed many of the e-mails it possessed. Allegedly, it did so in two ways—by overwriting backup tapes that had been used to restore the e-mails to the firm's system and by allowing users of the firm's e-mail system to permanently delete the e-mails over an extended period of time. Thus,

the SRO said, between September 2001 and March 2005, millions of the e-mails were destroyed.

In one instance, NASD said, in an NASD investigation into the firm's fee-based brokerage practices, Morgan Stanley falsely claimed that it did not have pre-October 2001 e-mail and failed to produce over 12,000 e-mails and attachments in response to an NASD request. By the time the firm conducted the search that led to the production of the e-mails, the firm had already deleted millions of other e-mails from its servers and the regulatory matter at issue had been settled.

Under NASD rules, a firm or individual named in a complaint can file a response and request a hearing before an NASD disciplinary panel. Possible remedies include a fine, censure, suspension, or bar from the securities industry, disgorgement of gains associated with the violations, and payment of restitution.

In May, Morgan Stanley agreed to pay a \$15 million fine and to reform its e-mail retention practices, resolving Securities and Exchange Commission charges that it failed to produce tens of thousands of requested e-mails over a four and a half-year period, according to the SEC.

Scope

NLRB Refuses to Remove Technology, Access Questions From E-Mail Case

In a case involving workers' use of their employer's e-mail system, the National Labor Relations Board Jan. 24 denied a motion to eliminate some of the questions the board had invited interested parties to discuss in amicus briefs (*Guard Pblng. Co.*, NLRB, No. 36-CA-8743-1, *order* 1/24/07). The board announced Jan. 10 that it would hear oral argument in the case and invited the parties and interested amici to file briefs by Feb. 9 discussing seven specified issues (6 PVL 74, 1/15/07).

The Eugene Newspaper Guild, Communications Workers of America Local 37194, which filed the unfair labor practice charge against the publisher of *The Register Guard* newspaper, Jan. 18 filed a motion asking the board to delete four questions that the union argued have nothing to do with deciding the case. Those questions seek information about access to an employer's e-mail system by nonemployees, the relevance of the location of the employee's workplace, policies on e-mail use issued by employers or included in collective bargaining agreements, and technological issues regarding e-mail systems.

Legal Ethics

Authenticity

Failure to Second-Guess Client's 'Evidence' Results in Attorney's Two-Month Suspension

The Wisconsin Supreme Court Jan. 4 suspended for two months a lawyer who continued to press his client's lawsuit without first making any meaningful inquiry into the authenticity of some fishy documents the client supplied (*In re Nunnery*, Wis., No. 2004AP2542-D, 1/4/07).

In a per curiam opinion, the court rejected the lawyer's argument that he did not violate Wisconsin's rule on competence. The rule requiring lawyers to act competently is designed to protect the system of justice as well as the individual client, the court declared.

Transparent Documents. Willie J. Nunnery represented a woman who claimed that she was subjected to racial discrimination and sexual harassment while working at a college. The woman gave Nunnery a number of laminated memos, e-mails, and letters that she claimed were sent to her by various people who worked at the college.

The papers contained racially derogatory comments, threats, and references to sexual assaults. The client told Nunnery that she had laminated the documents to prevent them from being stolen. Nunnery filed suit in federal court against the college and included damning allegations plucked from these documents. Lawyers for the college presented sworn statements from college personnel stating that the documents were obvious forgeries and cautioned Nunnery about the implications under Fed. R. Civ. P. 11 of going forward; Nunnery replied that he would take his chances.

After the client's lawsuit was dismissed the college moved for Rule 11 sanctions, arguing that Nunnery failed to reasonably inquire into the truth of his client's allegations. The court directed Nunnery to pay the college's attorneys' fees, stating that it was the "most blatant" Rule 11 violation the court had ever seen and that both Nunnery and his client shared the blame for proceeding with an action supported by such obvious forgeries.

The referee hearing the ensuing disciplinary action concluded that by going forward after having made only "a cursory and pro forma effort to validate the documents," Nunnery shirked his duty under Wis. Sup. Ct. R. 20:1.1 to act competently. After evaluating three other ethical missteps charged against Nunnery, involving neglect of client matters, the referee concluded that a two-month suspension from practice was appropriate.

Rule Protects Public Too. Nunnery appealed, arguing that the duty under Rule 20:1.1 to provide competent representation is intended to protect clients only. Moreover, he insisted that the rule could not be used to discipline a lawyer for failing to discover client fraud. He also argued that the sanction was too harsh. The court disagreed on all counts and ordered a two-month suspension.

The court said it was satisfied that Rule 20:1.1 was intended to protect the system of justice as well as individual clients. For one thing, the court noted, the comment to the rule states: "Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem. . . ."

Moreover, the court added, the preamble to chapter 20 of the rules cautions that a lawyer's neglect of his or her responsibilities "compromises the independence of the profession and the public interest which it serves."

Should've Known Better. The court also rebuffed Nunnery's argument that the competence rule does not impose a duty to discover client fraud or to protect clients from frauds that they perpetrate on the court or on their attorney. A client's misdeeds do not relieve an attorney of his obligations to comply with Rule 20:1.1, the court said.

Moreover, the court continued, the referee did not find misconduct because Nunnery failed to unearth his client's fraud; it found misconduct because he failed to make any meaningful inquiry into the veracity of the suspicious documents.

The court stressed that the referee labeled "absurd" the client's professed reason for laminating the incriminating papers and that the federal court described the documents as obviously fraudulent and observed that any minimally competent lawyer would have subjected his client to rigorous questioning and demanded corroboration of details before proceeding.

Conditional Reinstatement. The court said it was mindful of Nunnery's cooperation, previous lack of discipline, good reputation, and his apology. However, it rejected Nunnery's claim that there was a lack of harm that mitigated in favor of a reprimand. "Given the number and seriousness of the infractions, as well as the need to deter other attorneys from similar misconduct, a two-month suspension is appropriate," the court said.

The court further concluded that Nunnery's reinstatement will be conditioned on his payment of the Rule 11 sanction.

Daniel W. Hildebrand, DeWitt Ross & Stevens, Madison, Wis., argued the case for Nunnery. Assistant Litigation Counsel Julie M. Falk, Madison, argued for the Wisconsin Office of Lawyer Regulation.

Records Management

Best Practices

Minding the Gap: Information Management Compliance Gap Analysis

BY BARCLAY T. BLAIR

Many organizations facing the challenges of information management and e-discovery struggle with the right way to get started. There is no shortage of books and articles that clearly identify the issues and challenges, but few that provide practical guidance on how to address them. Gap analysis is one source of such guidance.

What is It and Why Use It? Gap analysis is a process for measuring the gap between a current state and a desired state. This helps organizations assess not only what they are doing wrong, but also what they are doing right, and how to close any gaps that might exist.

There are several reasons for performing a gap analysis. A gap analysis can help promote and support required changes, provide a foundational document that all stakeholders can rally around and use for planning, and mark the progress of change from the current state to the desired state. There is a potential pitfall, however: a gap analysis can sometimes be used as a smoke-screen to delay solving the real problems facing an organization.

Benefits One of the strengths of gap analysis is its utility for assessing progress in either phased processes or iterative processes. A gap analysis is also a generic tool that can be applied within any organization, to any problem.

An information management compliance (IMC) gap analysis is a specific type of gap analysis designed to determine whether or not an organization manages information in a manner that complies with laws, regulations, and business best practices. Ten steps for getting started on one follows.

1. Define Goals

Before a problem can be solved, it must be clearly defined. A gap analysis on its own is useless; it is a means, not an end, to the larger process of problem solving or

Barclay T. Blair is a consultant, frequent speaker, and author specializing in the compliance, policy, and management issues of information technology. He is the co-author of Privacy Nation: Seven Keys to Information Management Compliance and director of the IT compliance practice at Kahn Consulting, Inc. Contact Mr. Blair at: bblair@KahnConsultingInc.com.

change management. For a gap analysis to be a truly useful tool, organizations must define how the gap analysis will help solve a specific problem or manage required changes.

For example, an organization could conduct a gap analysis to explore how its information management program compares with the rest of the industry's programs. The gap analysis would help identify the differences between the organization's current practices and industry standards.

2. Determine Focus and Scope

When performing a gap analysis, it is vital to determine the correct level of analysis. Too broad a scope will not provide enough useful information, and too detailed a scope will take too long and confuse the analysis with unnecessary data.

First, select which areas of the business to analyze. These areas could be functional departments, business units, or legal jurisdictions.

Next, determine the types of information in need of analysis. This could include structured or unstructured information, information contained within specific systems, or specific record or document types.

Third, select which processes to analyze. Depending on the organization's needs, this might include e-discovery, backup and disaster recovery, and e-mail management. After clarifying the focus of the gap analysis, examine the organization's capabilities within the context of the business area, information types, and processes selected.

Within every organization, there are two primary capabilities: organizational and technological.

Organizational capabilities include the people and processes that support information management, the policies and governance structures, and the behavioral and management controls. Examples include records management policies, legal hold policies, e-mail policy, compliance processes, audit schedules, and training programs.

Technological capabilities refer to the relevant information technology that is in place, how it is configured, managed, and used, and other technical controls. Examples include e-mail systems, backup systems, shared storage, configuration management, and database management.

3. Identify and Engage Stakeholders

To have a successful project, all relevant parties must be identified and engaged from the beginning. Who has

the required information? Who “owns” the information, processes, systems and issues to be analyzed? Who must support the process?

It is useful to identify a project sponsor/co-sponsor and project manager at the outset. This ensures that specific individuals will have ownership of the process. Since the legal department typically plays a central role in IMC gap analysis, its role within an organization might put it in the best position to obtain the information and resources required. Consider structuring the gap analysis with a senior legal department representative as the sponsor.

4. Define the Process

Create the project plan. Clearly define what has to be done, by whom, and when. Be realistic about time lines. Remember it will always take longer than expected to obtain the required information, so plan accordingly.

Note who is funding the project, and state clearly the expected results of the project. Also consider the impact of the potential legal sensitivity of the process.

Communication about the process is vital throughout the entire project. Stakeholders must understand all concepts and tasks related to the project. Consider holding a workshop at the beginning to present the project concepts to all of the stakeholders. That way, everyone involved begins with the same information and expectations.

5. Gather Inputs

There are many ways to gather information; accordingly, formalizing the information-gathering process at the beginning will help to ensure consistent data throughout the project. Here are a few suggestions:

- Interviews — When conducting interviews with senior people in the organization, focus on strategic issues, and conduct the interview in a loose, organic style. Don't mix interview groups, as they will have different views, priorities, and roles in the project.

- Questionnaires — They are very useful for collecting factual information efficiently. Consider the design of the questionnaire and the structure of the questions carefully. Use questionnaires to gather “speeds and feeds” about the IT environment and other fact-oriented information about the business.

- Direct Observation — Use direct observation to gather information about actual working practices, tools, and processes.

- Document Review — This involves collecting and reviewing existing written policies, procedures, guidelines, standards, intranet postings, etc. Don't focus only on “formal” policies; try to e-mail memos and other de facto policies as well..

6. Create the Ruler

Determine the criteria for measuring gaps. Criteria should be based on the goals and scope of the gap analysis plus the business and its regulatory environment. Typical sources for benchmarks include laws, regulations, industry standards, and best practices. Don't re-create the wheel unnecessarily; leverage any existing analysis that the legal, records and information management, and compliance departments have al-

ready performed regarding the regulatory environment. Keep in mind that there is no law, regulation, standard, or best practice for everything in information management, and don't be afraid to use the company's existing practices as “best practices.”

7. Use the Ruler

Once all the information is gathered, assess it against the benchmarks (the desired state) and document all observations. Analyze everything that was read, seen, and heard while collecting information. Analyze how that information compares to the benchmarks and offer recommendations for closing the gaps.

At this stage, do not worry about prioritizing the recommendations. Adopt the “unlimited budget and time philosophy,” for now. The prioritization and practical aspects will happen later. Also, validate what was read, seen, and heard with stakeholders during the analysis process. Establish a formal documentation and review process so all relevant stakeholders can review and provide feedback on the observations and recommendations.

8. Report the Gaps

Finding the best way to document and report gap information can present challenges. Many IMC issues are highly sensitive, especially those addressing compliance with laws and regulations. Consider meeting with the legal department or other legal counsel at the beginning to sensitize project staff to the issues.

Discuss the nature of the documentation with the legal department before the project begins. Also discuss the privilege process with legal counsel and how they would like to apply it to the gap analysis process. Applications of the privilege process could include having an attorney present at interviews, creating privilege legends, communicating through an attorney, and identifying specific “loop outs” in the project that must go through the legal department.

9. Create a Plan to Close the Gaps

The focus of the action plan is to prioritize existing gaps and rationalize them against real time lines, real budgets, real resources, and relevant high risk/high value issues. While it is important to focus on high risk/high impact issues, the plan must also be pragmatic and practical for dealing with short- and near-term issues.

IMC is complex, so focus on getting started. If there are many gaps, don't get discouraged. The gap analysis is the first big step towards addressing the issues.

10. Execute the Plan

Focus on real time lines and develop a reporting process to track progress. Communicate to the stakeholders regularly on the progress achieved. Watch for “observed state” changes from external factors.

While a gap analysis is only one part of the larger, more complex process of addressing information management compliance issues, it is a good place to start. It provides, if not a detailed road map, then at least a signpost that says “go this way,” which is often what organizations need to start the journey.

Conference Report

Save the Dates

BNA 2007 Conference Series Finalized

BNA has announced that six federal magistrate judges will participate in its 2007 conference series, entitled Practice Under the New E-Discovery Amendments: The Battlegrounds of Conflict; The Promise of Resolution. The programs will be presented on March 19-20 in Orlando, Fla., on April 11-12 in Washington, D.C., and on May 7-8 in Chicago, Ill.

Magistrate Judge Ronald J. Hedges of the U.S. District Court for the District of New Jersey will moderate all three programs. He is the author of the recently published *Discovery of Electronically Stored Information: Surveying the Legal Landscape* (BNA, January 2007).

In Orlando, Judge Hedges will be joined by Chief Judge James M. Rosenbaum of the U.S. District Court for the District of Minnesota; Magistrate Judge John Hughes of the U.S. District Court for the District of New Jersey; Magistrate Judge David J. Waxse of the U.S. District Court for the District of Kansas; and John L. Carroll, former Chief Magistrate Judge of the U.S. District Court for the Middle District of Alabama.

Judge Waxse will also participate in the D.C. program, along with Magistrate Judge Liam O'Grady of the U.S. District Court for the Eastern District of Virginia. Magistrate Judge Paul W. Grimm of the U.S. District Court for the District of Maryland will join Judges Rosenbaum and Hedges in Chicago.

These leading jurists, together with an equally distinguished private sector faculty, will discuss some of the most troublesome aspects of e-discovery, including: the changing roles of the judge, client, counsel, expert, and advisor; the operation of the safe harbor provision, avoiding sanctions, and how discovery practice has changed since the amendments to the Federal Rules of Civil Procedure became effective.

The programs in each location will be preceded by a workshop on avoiding civil and criminal sanctions. Among the topics to be explored in those sessions will be understanding key technology drivers and the relationship between in-house and outside counsel.

Complete information on the BNA 2007 Conference Series, which is presented with exclusive industry sponsor Kroll Ontrack, is available at <http://legalegde.bna.com/031907.htm>

International News

Employment Issues

Revision of Employer Right to Access Employee E-Mail Is Debated in Norway

COPENHAGEN—A series of public meetings on a Norwegian legal proposal aimed at redefining employers' right of access to employee work-related e-mail came to a close Jan. 17.

The proposal will be the subject of a series of political consultations before it is put before Parliament in the spring.

According to a statement from the Norwegian Ministry of Government Administration and Reform, the decision to revise the rules was made in 2006 after the Norwegian Data Inspectorate (Datatilsynet) reported an increasing number of employer and employee requests for clarification of regulations regarding the legal viewing of employee e-mail. According to the ministry, the rise in such queries displayed a need for simplification and revision of the rules.

Employer access to employee e-mails is regulated by Norway's Personal Data Act, which states that in cases when a "legitimate need" is proven and an employee is sick or on vacation, employers may read work-related mails. Any infringement of the guidelines may result in a coercive fine or liability for damages. Critics of the current system, including the Data Inspectorate itself, believe that the rules are not specific enough and can be misinterpreted by employers.

While grounded in the notion that employers have no automatic right to search through employees' work-related mail, the new law would, according to the government, seek to "balance the needs of employer and employee." However, political agreement is far from assured over the question of what constitutes a "legitimate need" to look at employee e-mail and how much advance notice employers should give before accessing e-mail.

The proposal, which would alter the elements of the Personal Data Act concerned with definition of personal data and coercive fines (Sections 3 and 46) also would apply to students and voluntary workers, and re-

late to other forms of electronic communication, such as chat programs.

In a statement provided to BNA Jan. 17, Aslaug Bendiksen, senior adviser at the Ministry of Government Administration and Reform, confirmed that, if approved, the new measures would provide revised instructions on employees' right to privacy when using electronic communication tools, including regulations on the forwarding and shared storage of e-mail. She confirmed that the proposal would take its starting point in the premise that employers have no right to access employees' mail, although exceptions in a number of areas are under debate, including employee absenteeism, suspicion of a breach of loyalty, and criminality. She added that the proposal would require employers to closely follow a stipulated procedure and said the proposal is due to become law at the beginning of July 2007.

Smooth passage of the bill depends on broad political cooperation, and some politician and employer organizations have expressed their dissatisfaction with the proposal.

Speaking to BNA Jan 16, Nina Melsom, a lawyer at the Confederation of Norwegian Enterprise (NHO) confirmed that her organization opposed a tightening of the rules. In a statement issued Jan. 17, the Melsom said that the proposal "is formulated in such a way that employees' e-mail boxes are defined as 'personal' which gives the impression that they have been established as a personal matter and require protecting." Melsom maintained that "the e-mail system is owned by the employer and is created as a work tool for communication and the sending of relevant company information."

In the statement, the NHO agreed with the principle that the employers should not be granted automatic access to all employee e-mail, but disagreed with the suggestion that access should be further curtailed.

By MARCUS HOY

The current version of the proposal and documents relating to the public hearing are available, in Norwegian, at http://www.odin.dep.no/fad/norsk/dok/hoeringer/paa_hoering/071001-430006/dok-bn.html. The NHO statement is available, in Norwegian, at <http://www.nho.no/article17749.html>.

Journal

CONFERENCES & MEETINGS

Upcoming meetings, conferences, and other events of interest to *Digital Discovery & e-Evidence* subscribers. Entries designated *NEW* were added this week.

February

Managing Complex Litigation. Park Central Hotel, New York City, February 6-7. Hosted by American Conference Institute. *Further information:* <http://www.americanconference.com/complit>.

Evidence Issues and Jury Instructions in Employment Cases. Washington, D.C., February 8 - 9. Hosted by Georgetown CLE and ALI-ABA. *Further information:* <http://www.law.georgetown.edu/cle/pdfs/98.pdf>.

Sixth Annual Symposium on Legal Malpractice and Professional Responsibility. San Antonio, Texas, February 23. Hosted by St. Mary's Law Journal. *Further information:* (210) 436-3439.

Third Annual E-Discovery Conference: Real World Solutions and Practical Strategies for 2007 and Beyond. The Claremont Resort & Spa, Berkeley, Calif; February 26-March 1. Presented by IQPC. *Further information:* <http://www.iqpc.com/cgi-bin/templates/singlecell.html?topic=233&event=12002>.

* **NEW * Electronic Discovery after the New Federal Rules: Strategies for Coping with the Latest Challenges and Intricacies.** Four Seasons Hotel, Los Angeles, Calif.; February 27. Presented by West Legalworks. *Further information:* <http://guest.cvent.com/EVENTS/Info/Summary.aspx?e=59ce74c3-7115-4ef2-934c-c91f3d341a06..>

E-Discovery & Litigation Readiness for Life Sciences. The Affinia Manhattan, New York City; February 27-28. Presented by American Conference Institute. *Further information:* <http://www.americanconference.com/lifescidoc>.

March

2007 Legal Malpractice & Risk Management Conference. Westin River North Hotel, Chicago; March 7- 9. Presented by LMRM. *Further information:* <http://www.lmr.com>.

* **NEW * Electronic Discovery Certification Course.** Eden Prairie, Minn., March 8-9. Presented by Kroll OnTrack. *Further information:* <http://krollontrack.com/2007courses/certcourse/>.

* **NEW * Essentials of Civil Litigation.** University of New Mexico School of Law, Albuquerque, N.M.; March 10-13. Presented by American Association for Justice (for-

merly ATLA) Trial Advocacy College. *Further information:* <http://www.atla.org/education/essentials/>.

* **NEW * Practice Under the New E-Discovery Amendments: The Battlegrounds of Conflict; The Promise of Resolution.** Orlando, Fla., March 19 - 20. Presented by BNA and exclusive industry sponsor Kroll Ontrack. *Further information:* <http://legaledge.bna.com/031907.htm>.

* **NEW * ABA TechShow 2007.** Chicago, March 22-24. Presented by ABA. *Further information:* <http://www.abanet.org/techshow/>.

* **NEW * Trial Evidence in the Federal Courts: Problems and Solutions.** New York City, March 22-23. Presented by ALI-ABA. *Further information:* <http://www.ali-aba.org>.

Advanced Electronic Discovery Certification Course. Eden Prairie, Minn., March 29-30. Presented by Kroll OnTrack. *Further information:* <http://krollontrack.com/2007courses/adcertcourse/>.

Getting Ahead of the eDiscovery Curve: Strategies for Companies and Their Counsel to Reduce Costs and Meet Judicial Expectations. The Peabody Memphis, Memphis, Tenn.; March 29-30. Presented by the Sedona Conference Institute in association with ARMA International. *Further information:* <http://www.thosedonaconference.org/conferences/tsci/20070329>.

April

* **NEW * Practice Under the New E-Discovery Amendments: The Battlegrounds of Conflict; The Promise of Resolution.** Washington, D.C., April 11-12. Presented by BNA and exclusive industry sponsor Kroll Ontrack. *Further information:* <http://legaledge.bna.com/031907.htm>

2007 NAID Annual Conference. Orlando, Fla., April 11-13. Sponsored by the National Association for Information Destruction. *Further information:* <http://www.naidonline.org/conference/conf2007/>

Spring 2007 National Legal Malpractice Conference. J.W. Marriott Hotel, Washington, D.C.; April 25-27. Presented by the ABA Standing Committee on Lawyers' Professional Liability. *Further information:* <http://www.abalegalservices.org/lpl>.

May

* **NEW * Practice Under the New E-Discovery Amendments: The Battlegrounds of Conflict; The Promise of Resolution.** Chicago, May 7-8. Presented by BNA and exclusive industry sponsor Kroll Ontrack. *Further information:* <http://legaledge.bna.com/031907.htm>.

ABA 33rd National Conference on Professional Responsibility and 23rd National Forum on Client Protection. The Fairmont, Chicago; May 30-June 2. Presented by the ABA Center for Professional Responsibility. *Further information:* <http://www.abanet.org/cpr/prconf.html>.