ALM
LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

Volume 21, Number 7 • December 2006

The Bell Keeps Tolling

The Tenth Circuit Deals Selective Waiver Yet Another Blow

By Alexander Y. Thomas

Selective waiver of the attorney-client privilege is a lonely doctrine indeed. Since the Eighth Circuit first adopted it in the 1977 *Diversified Industries* case, the notion that a litigant may disclose privileged material to government enforcers without waiving the privilege as to third parties has hardly won fans among federal courts of appeal. Most recently, in June, 2006, the Court of Appeals for the Tenth Circuit weighed in on the viability of selective waiver. The *In Re: Qwest Communications Int'l* decision is precisely what advocates for selective waiver needed least; it is a comprehensive evaluation, and rejection, of nearly all of the cogent arguments advanced in favor of the doctrine.

The Tenth Circuit's back-to-basics approach to the privilege and work product doctrine is essential reading for corporate counsel faced with the unenviable decision about what to disclose "voluntarily" to government enforcers or investigators. While it was careful to focus its reasoning on the record before it, the court fundamentally determined that selective waiver is inconsistent with, and fails to promote, the original objectives of the attorney-client privilege and the work product doctrine.

continued on page 7

NLRB Rulings Regarding Supervisors Provide Clarity and Controversy

By A. Kevin Troutman

Before the National Labor Relations Board (NLRB) issued its recent decisions in the *Kentucky River* cases, union leaders and activists predicted dire consequences — potentially stripping millions of workers, especially in the healthcare industry, of their rights to join a union. Unions, which are trying to attract more employees to their ranks, staged rallies and other events to draw attention to these cases.

But the decisions did not dramatically redraw the lines for determining which workers are considered supervisors and which are not. Instead, they provided guidance that will be helpful to employers and unions alike in determining the status of workers whose classification falls into the gray area between supervisor and employee. The analysis remains highly fact-specific and appears unlikely to create the dramatic effects predicted.

Some fundamental facts illustrate that the Board's decisions did not usher in sweeping changes. Among the three companion cases considered, the Board classified disputed employees as supervisors in just one (*Oakwood Healthcare, Inc.*). In that one case, the NLRB concluded that 12 full-time charge nurses were supervisors. It found that 112 other nurses that rotated in the same job title were not supervisors. It will take a while before the practical impact of these decisions is completely clear, but two things are already certain. First, the decisions add predictability to the classification question regarding some workers; and second, the issue will continue to be a flashpoint for controversy.

Perspective Regarding the NLRA

The National Labor Relations Act (NLRA) established employees' rights to self-organize, join or assist labor organizations. It also prohibits employers from interfering with or restraining employees' exercise of these rights and provides that employers cannot attempt to dominate or influence a labor union. With this in mind, the Act expressly excludes supervisors from the definition of an "employee," thus making supervisors ineligible for union membership.

Congress recognized that a company may expect strict loyalty from those acting as its agents. Moreover, it recognized that unions and their members should be free from

continued on page 2

In This Issue

Protecting Legal Data 3
Employers Beware EEOC Information Request 5
New Federal Discovery Rules: A Compliance Roadmap 9
Base Salaries Up; Bonus Levels Mixed 11

Supervisors

continued from page 1

supervisory influences within their ranks. Such concerns, including protecting employees from so-called "sham unions," have been critical for years. Thus, an accurate determination as to which employees are supervisors is important to safeguard the interests of *both* labor and management.

BEYOND JOB TITLES

Congress adopted a somewhat cumbersome definition of a supervisor to distinguish between two classes of workers: 1) those vested with "genuine management prerogatives," and 2) "employees" protected by the Act.

The *Kentucky River* decisions make clear the fact-specific nature of this analysis. For example, the Board considered several individuals with the same job title, charge nurse. Yet, as explained below, it found that some of these employees were supervisors and others were not, even among full-time charge nurses working at the same hospital.

FUNDAMENTAL DESCRIPTION OF A SUPERVISOR

The Act defines a supervisor as any individual having the authority, "in the interest of the employer," to engage in *any* of 12 enumerated supervisory functions. These functions include: to hire, transfer, suspend, lay off, recall, promote, discharge, assign, reward or discipline other employees or "responsibly to direct them," to adjust their grievances, or effectively to recommend such action, if the exercise of such authority is not of a merely routine or clerical nature, but *requires the use of independent judgment.*

Therefore, to be considered a supervisor, an individual must exercise authority to engage in one or more of these activities; they must hold this authority "in the interest of the employer;" *and* their exercise of this authority must rise above the "routine or clerical," requiring the use of independent judgment. Among the 12 supervisory functions listed in the Act, the two most ambiguous were a focus of the Board's recent decisions. These functions are to "assign" and "responsibly to direct" employees.

The Board also revisited what it means to exercise "independent judgment," a term the Supreme Court said in 2001 that the NLRB improperly limited in *NLRB v. Kentucky River Community Care*. This is why the recent group of cases was referred to collectively as the *Kentucky River* cases.

CASES DECIDED BY THE BOARD

The question of who is considered a supervisor is contentious because the answer is not only important, but it often turns on very specific facts. These questions often arise in the healthcare and construction industries. So it is not surprising that two of the three *Kentucky River* cases (*Oakwood* and *Golden Crest Healthcare Center*, an acute care hospital and a nursing home, respectively) emerged from the healthcare industry and that the other (*Croft Metals, Inc.*) came from the construction industry.

Oakwood *Decision Clarifies The Meaning of Key Terms*

Regardless of whether they discharge one or more of the 12 supervisory functions listed in the Act, individuals are not supervisors unless they also exercise sufficient independent judgment and supervisory activities comprise a substantial part of their work time. A "substantial part" of work time could be as little as 15%-20%.

In *Kentucky River*, the NLRB decided that an individual did not exercise independent judgment (and was therefore not a supervisor) if she exercised "ordinary professional or technical judgment in directing less-skilled employees to deliver services." The Supreme Court, however, said that the Board was wrong to consider the *kind* of discretion exercised (in this case "ordinary professional or technical judgment"). Instead, it should have focused upon the *degree of discretion* that the individual exercised in making her decisions. Therefore, in *Oakwood*, the Board articulated a far less restrictive standard.

continued on page 6

A. Kevin Troutman is an attorney with Fisher & Phillips, LLP, a national law firm practicing exclusively in the field of labor and employment law. He may be reached at 504-529-3856 or KTroutman@laborlawyers.com.

The Corporate Counselor®

EDITOR-IN-CHIEF . . . . .Adam J. Schlagman
EDITORIAL DIRECTOR . . . . . .Wendy Kaplan Ampolsk
MANAGING EDITOR . . . . .Steven Salkin, Esq.
MARKETING DIRECTOR . . . . .Colin Graf
MARKETING COORDINATOR . . . . .Beth Ann Montemurro
MARKETING ANALYSIS COORDINATOR . . . . .Traci Footes
GRAPHIC DESIGNER . . . . .Crystal Hanna

BOARD OF EDITORS
WHITNEY ADAMS . . . . .Cricket Technologies, Reston, VA
HEATHER R. BADAMI . . . . .Bryan Cave LLP, Washington, DC
ERIC V. BLANKENSHIP . . . .Economic Analysis Group, Ltd., Washington, DC
VICTOR H. BOYAJIAN . . . . .Sonnenschein Nath & Rosenthal LLP, Short Hills, NJ
DAVID M. DOUBILET . . . . . .Fasken Martineau DuMoulin LLP, Toronto
WILLIAM L. FLOYD . . . . . . .McKenna Long & Aldridge LLP, Atlanta
JONATHAN P. FRIEDLAND . .Kirkland & Ellis LLP, Chicago
BEVERLY W. GAROFALO . . .Brown Raysman Millstein Felder & Steiner LLP, Hartford, CT
ROBERT J. GIUFFRA, JR. . . .Sullivan & Cromwell LLP, New York
MICHAEL L. GOLDBLATT . .Tidewater, Inc, New Orleans
HOWARD W. GOLDSTEIN .Fried, Frank, Harris, Shriver & Jacobson, New York
ROBERT B. LAMM . . . . . . .Financial Guaranty Insurance Company, New York
JOHN H. MATHAS, JR. . . . .Jenner & Block, Chicago
MARGARET A. McCAUSLAND . . . . .Private Practice, Philadelphia
PAUL F. MICKEY JR. . . . . . .Steptoe & Johnson LLP, Washington, DC
ELLIS R. MIRSKY . . . . .The Network of Trial Law Firms, Tarrytown, NY
REES W. MORRISON . . . . . .Hildebrandt International, Somerset, NJ
E. FREDRICK PREIS, JR. . . .McGlinchey Stafford, PLLC, New Orleans
SEAN T. PROSSER . . . . .Morrison and Foerster, LLP, San Diego
DAVID B. RITTER . . . . .Neal, Gerber & Eisenberg LLP, Chicago
DIANNE R. SAGNER . . . . . .FTI Consulting, Inc., Annapolis, MD
JOEL SCHNEIDER . . . . .Archer & Greiner, PC, Haddonfield, NJ
MICHAEL S. SIRKIN . . . . . .Proskauer Rose LLP, New York
R. MICHAEL SMITH . . . . . .Dechert LLP, Washington, DC
MICHAEL STARR . . . . .Hogan & Hartson LLP, New York

The Corporate Counselor® (ISSN 0888-5877) is published by Law Journal Newsletters, a division of ALM. © 2006 ALM Properties, Inc. All rights reserved. No reproduction of any portion of this issue is allowed without written permission from the publisher. Telephone: (800) 999-1916
Editorial e-mail: ssalkin@alm.com
Circulation e-mail: subspa@alm.com

The Corporate Counselor P0000-233
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to:
ALM
1617 JFK Blvd., Suite 1750, Philadelphia, PA 19103
Annual Subscription: $365

Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, PA 19103
www.ljnonline.com

Protecting Legal Data

Does Your Legal Technology Provider Compromise Corporate Security?

By Eric Smith

In today's environment of well-deserved hypersensitivity to corporate compliance as mandated by the SEC and the Sarbanes-Oxley Act of 2002 (SOX), the thought of unauthorized parties viewing or altering privileged corporate records should strike fear in the heart of any corporate compliance officer. That threat can quickly evolve into a reality if your corporation's law department implements an electronic invoicing and matter management system in an application service provider (ASP) environment.

In the past 3 years, ASP-based legal electronic invoicing providers have collectively processed an estimated $6-$10 billion worth of privileged legal invoices on behalf of the law departments of Fortune 500 corporations. These third-party providers, popular for their easy-to-install systems, automate the invoice delivery process from law firms through a corporate law department's approval and payment cycle. In doing so, these vendors also accumulate a database of legal information and store it in a warehouse outside of all established security procedures and protocols.

These same providers also host matter-management systems for many of their clients. The matter-management systems catalog and document sensitive legal case information, such as early case assessments, key strategy documents and case-by-case budget reserve amounts. This data is also stored outside of a corporation's infrastructure.

The ease of deployment and the ability to quickly process invoices, track case progress and evaluate legal spend are significant benefits and very attractive to law department staff. However, it is critical for a compliance officer to weigh this against the very real risks of keeping the data on a server outside of the client's network and infrastructure and largely independent of a corporation's internal SOX compliance efforts.

The primary questions surrounding an ASP-based legal e-invoicing and matter management system concern the security of a corporation's legal data. Before implementing this technology, you should ask your vendor the following questions: Will my corporation's privileged invoices and matter data be encrypted while stored on the vendor's system, not simply while in transit? Will my invoice and matter data be viewable by unauthorized corporate representatives or any other third party? Does the third-party vendor controlling the pathway of incoming invoices alter the SOX-mandated chain of control for corporate records? Does the third-party vendor duplicate the corporation's compliance control process?

If the ASP-based legal technology system does not use the same security and audit controls the corporation executes for its other internal and confidential data, there may be compromises to a corporation's SOX compliance.

Background

The core of the issue lies with SOX Section 404. Section 404 requires that each public company's annual reports include a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedure for financial reporting. Additionally, management is bound to confirm the effectiveness of the company's internal control structure and procedures for financial reporting.

The legal penalties for violating Section 404 can be steep; however the business implications can be even steeper. Earlier this year, an audit of the Calgon Carbon Corporation law department uncovered $1.4 million in unreported legal invoice expenses. Consequently, the company's stock dropped by double digits, it was forced to restate earnings for the first three quarters of 2005 and the general counsel was fired.

The Corporate Law Department and its Role

Sarbanes-Oxley audit compliance affects nearly every aspect of corporate operations from the top down, including the corporate legal department, its operations and the manner in which new legal technology is purchased and deployed.

If an audit of the law department is initiated, corporate auditors will want to review key aspects of a legal invoice's life cycle, including:

- Who has access to the system that manages invoices?
- Who has actually accessed those invoices?
- What actions have been taken on each invoice?

These same questions can apply for the law department's matter management system in the event of an audit. Access and the ability to alter privileged legal information — either financial or case-related — is a key concern for the auditing process.

Possible Breaches

Most ASP-based legal e-invoicing and matter management vendors have implemented minimal technical requirements for securing their corporate client's legal invoices and privileged case information. However, these providers routinely face new challenges related to security, especially in the areas of access, security and data storage.

Access

It is critical for a corporation to know who has access to its privileged legal information (*ie*, legal invoices, case assessments and budgeting). In many cases, personnel from ASP-based legal vendors have access to a corporation's privileged data. In fact, many ASP vendors permit their own staff to have access to their clients' financial data and case materials. This is a huge risk for any corporation as client data is often co-mingled on the same server with other corporations' privileged information and therefore at serious risk of exposure.

continued on page 4

Eric Smith, DataCert's chief technology officer and a member of the founding DataCert team, has more than 15 years' experience managing software development. Prior to DataCert, he developed industry-specific software applications for the legal and credit management industries and developed accounting and quality assurance applications for both PWC and Compaq Computer Corporation.

Legal Data

continued from page 3

Once logged into the legal e-invoicing system, ASP, law firm and corporate client personnel can view invoices and export and download sensitive legal information and confidential financial data to personal computers from anywhere outside of the company's network and security infrastructure. The same access is also granted for ASP-based matter-management systems.

However, there is a potential for access-related breach that presents three serious control issues.

First, a company must identify which personnel (company only or company and vendor) have access to the ASP-based system. It must also determine if that access is logged, and if a historical record can be obtained to show that data was acted on, altered and/or approved during the submission process.

Second, the company must verify what controls and restrictions are in place to ensure that only authorized company personnel (and no vendor personnel) have the ability to export sensitive data out of the ASP system.

Finally, the company must determine where the data is being exported. An ASP system can be readily accessed from anywhere using the Internet. Is a corporation comfortable with their personnel — or potentially a vendor's personnel — logging into the ASP system from home and downloading confidential corporate financial and legal data onto a home computer? How does a compliance officer ensure the integrity of the information when law firm personnel are not removed from the system when they leave a firm or are reassigned?

These issues lead to a fair question for corporate counsel and risk management personnel: *Does an environment and opportunity exist for an individual to adversely alter a corporation's legal data without any entrenched independent oversight?*

Unfortunately, the answer with many ASP-based e-invoicing and matter management solution providers is likely to be yes.

Security Protocol

As a user of an ASP-based application, you must ensure that the vendors are particularly careful when it comes to the security of your data. They should be diligent in implementing and maintaining top security standards to protect your data.

Many e-invoicing and matter-management vendors assign login information based on a user's corporate e-mail address. This is a standard practice industry wide. However, if the vendor does not require a complex, alphanumeric password for login access, or permits passwords to be the same as the user's last name, it is easy for an unauthorized user to break into the system.

Likewise, ASP-based vendors must also be wary of unauthorized entry attempts such as "phishing." Phishing involves mirroring a Web site to illegally obtain an authorized user's login and password information.

Finally, a good practice is to revisit the vendor's contract with your law department. Is there a provision in the contract that requires the vendor to notify the corporation of a known or possible breach? The vendor must be responsible for promptly notifying the law department of all suspected and actual breaches.

Data Storage

The basic structure of an ASP-based legal technology solution includes the storing of privileged legal data outside of a corporation's secure infrastructure. Corporate compliance officers should consider not only *where* their data is stored, but also *how* their data is stored.

Typically, ASP-based legal electronic invoicing and matter management vendors do not encrypt corporate client data while it is being stored. If an unauthorized viewer accesses a company's legal database, he or she will have little difficulty reading (and possibly modifying) the privileged legal invoicing and data.

There may be little, if any, encryption or security around the transmission of the payment file back to the corporate client. In many cases, payment files that contain detailed information and result in checks being issued to law firms are routinely e-mailed by ASP-based vendors back to the corporation without any encryption or security.

Problems also arise from *where* a company's invoicing data is stored on a server. If the ASP-based provider has more than one company's legal data stored on a server, there is a chance that the data can be co-mingled with another company's information and accessible by not only hackers, but also by other company personnel. Having your company's data on the same server as a competitor's adds another level of risk to be considered from both a compliance and business perspective.

PROTECT LEGAL E-INVOICING DATA

There are three basic steps that can be taken to help enforce corporate compliance.

1. Require the third-party vendor to deploy the e-invoicing and/or matter management system behind your corporation's firewall;
2. Demand superior security. For a start, discover if your vendor requires user-unique alphanumeric passwords for system access; and
3. Insist that all stored and transmitted data is encrypted. This includes the data itself, backup tapes and media. All forms must be encrypted to guard against inside threats of unauthorized access or theft.

AUDIT THE PROVIDER

Corporate compliance officers should audit their ASP-based legal electronic invoicing and matter management system providers. The following five steps are recommended to determine if a vendor's practices support SOX compliance efforts:

- **Audit Security.** Determine what security policies a vendor follows. If a security breach occurs, is the vendor capable of identifying it? Has a security breach occurred in the past? Verify if the vendor is contractually obligated to share information about the breach with its clients.
- **Audit Encryption.** The vendor should encrypt all sensitive data during each transaction step — from delivery to storage.
- **Audit Storage.** A company's electronic billing and case information

continued on page 10

Employers Beware EEOC Information Request

By Mark Blondman and Brooke Iley

Understandably, companies have become more sensitive about protecting confidential, proprietary business information from disclosure to competitors and others outside the company. A recent ruling by the United States District Court for the District of Columbia, *Venetian Casino Report* v. *EEOC*, 2006 WL 2806568 (D.D. Cir. 2006), demonstrates that such disclosures may occur in the most unexpected ways. The court's holding in *Venetian* makes it clear that the Equal Employment Opportunity Commission (EEOC) can release sensitive, confidential or proprietary company documents submitted in response to a Charge of Discrimination without first providing notice to the employer that submitted the information. Further, the EEOC is empowered to release these documents not only to the charging party *but also to third parties*. Employers should be aware of this potential source of disclosure and consider steps to limit inadvertent misuse of company information.

Facts and Procedure

In the spring of 1999, the Venetian Casino Resort (Venetian) conducted a mass hiring process to staff a new casino and resort in Las Vegas. In its wake, at least 11 people filed employment discrimination complaints with the EEOC against Venetian, alleging discrimination based on age, race and color in violation of the Age Discrimination in Employment Act (ADEA) and Title VII of the Civil Rights Act of 1964. The EEOC opened files and began investigating these charges pursuant to customary administrative procedures. As part of routine information requests, the EEOC requested employee data and statistics from Venetian. Venetian failed to produce the requested documents. The EEOC then issued an administrative subpoena for the information. Venetian filed objections to the subpoena, using the EEOC's administrative process. The EEOC denied those objections, and Venetian was forced to file the instant action against the EEOC for declaratory and injunctive relief in December 2000.

In February 2002, Venetian settled all claims that fell under Title VII, but not the claims of age discrimination. As a result, the EEOC's age discrimination files for the Venetian remained open. Venetian continued to refuse to turn over requested data. Venetian challenged the EEOC's disclosure policy set forth in Section 83 of the EEOC Compliance Manual that permits the Agency to disclose information from closed Title VII and ADA case files without prior notice to the employer and without regard to whether the employer deemed the data to be confidential. Venetian asserted a broad based challenge to the EEOC's policy regarding the disclosure of information deemed confidential and/or proprietary, arguing that it was violative of Title VII, the Trade Secrets Act, the Freedom of Information Act, Executive Order No. 12,600, the Copyright Act and the Administrative Procedure Act. Venetian argued that because the EEOC does not require employers that submit information to be given predisclosure notice, their current policy constitutes a "back door" by which charging parties, their counsel, and incidental third parties may obtain access to case files containing confidential and proprietary information, as well as trade secrets.

On Jan. 12, 2004, the District Court of the District of Columbia granted the EEOC's motion to dismiss on the ground that the issue was not ripe for review. On May 27, 2005, the circuit court reversed, holding that "the question of whether [the] EEOC's disclosure policy is lawful presents a live and focused dispute emanating from Agency action that is both final and consequential to Venetian." On Nov. 10, 2005, the court issued an order requiring both parties to file cross-motions for summary judgment. The sole issue before the court was whether an EEOC disclosure policy or practice, whether written or not, that allows the Agency to release documents that a submitting party has identified as containing trade secrets and/or confidential material without first notifying the submitting party, is lawful.

Court's Decision and Analysis

In its decision, the court disagreed with Venetian's contention on each of the grounds, holding that the EEOC disclosure policy and practice does not violate federal law, even if it allows disclosure of trade secrets or other confidential information to third parties without prior notice to the employer. The court addressed each of Venetian's claims as follows:

Title VII of the Civil Rights Act

Title VII gives the EEOC two formal means of obtaining information when it investigates a charge. First, the EEOC may examine and copy any evidence in the possession of the employer being investigated. Second, it may subpoena evidence and documents. The Act, however, limits the ability of the EEOC to make public disclosures of information gathered during its investigations, directing that "[c]harges shall not be made public by the Commission." The decision in *Venetian* references a 1981 case that explicitly upheld the EEOC's practice of making limited disclosures of confidential information to charging parties in their own Title VII charge files. *EEOC v. Associated Dry Goods, Corp.*, 449 U.S. 590 (1981).

In upholding the EEOC's disclosure policy, the Supreme Court in *Associated Dry Goods* concluded that the EEOC's interpretation of its founding statute is consistent with the coordinated scheme of administrative and judicial enforcement that Congress created to enforce Title VII. First, limited disclosure to the parties can speed the Commission's required investigation in that the EEOC is more likely to obtain information if it can present the parties with specific facts for them to corroborate or rebut. Second, limited disclosure enhances the Commission's ability to carry out its statutory responsibility to resolve

continued on page 6

Mark Blondman and **Brooke Iley** are partners in the Employment, Benefits and Labor practice at Blank Rome LLP in Washington, DC. Blondman may be reached at blondman@blankrome.com or 202-772-5800, Iley can be contacted at 202-772-5816 or iley@blankrome.com. For more information about Blank Rome, please visit www.blankrome.com.

Information Request

continued from page 5

charges through informal conciliation and negotiation. A party is far more likely to settle when they have ample information to be able to assess the strengths and weaknesses of their opponent's case as well as their own. Finally, the EEOC's disclosure policy supports Title VII's scheme of enforcement that includes private rights of action. As the *Associated Dry Goods* court noted: "Congress considered the charging party a 'private attorney general' … [who] could hardly play that role without access to information needed to assess the feasibility of litigation." In the instant case, the court did not find the EEOC's disclosure policy to be violative of Title VII.

The Trade Secrets Act and Freedom of Information Act

The Trade Secrets Act is a criminal statute that regulates conduct of individual officers of the government. The Supreme Court has acknowledged that the Act does not afford a private right of action to enjoin disclosure of information in violation of the statute. *Chrysler Corp. v. Brown*, 441 U.S. 281 (1979). Accordingly, the *Venetian* court rejected the argument that a party submitting confidential information to the EEOC has a private right of action under the Trade Secrets Act. This omission is significant because the D.C. Circuit, in which *Venetian* was decided, "is considerably more reluctant to engraft numerous and significant qualifications onto an apparently clear, unambiguous text where the provision is criminal." *CAN Fin. Corp. v. Donovan*, 830 F.2d 1132 (D.C.Cir. 1976). Therefore, in the case at hand, the Trade Secrets Act alone does not mandate any particular EEOC procedure.

Executive Order 12,600

Executive Order 12,600 provides a requirement that federal agencies create notice procedures to parties submitting records that contain confidential information as to requests for their disclosure. The court in *Venetian* easily dismissed this plank of the plaintiff's argument by finding that the EEOC complied with these requirements by publishing its predisclosure notification procedures in Section 83 of the EEOC Compliance Manual.

The Copyright Act and Administrative Procedure Act

On this contention, the court in *Venetian* simply held that while the Copyright Act proscribes infringement of copyrighted material, nothing in the Act requires confidential treatment by the government of copyrighted material. Further, the Act provides an express remedy for alleged copyright violations — a private right of action for infringement. Nothing in the Act requires the establishment of particular internal agency procedures.

The Administrative Procedure Act

In addition, Venetian challenged the EEOC's disclosure policy as arbitrary, capricious, and a violation of the Administrative Procedure Act. In this case, the court stated that the EEOC's policy cannot be said to be "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with the law," such as to warrant judicial intervention pursuant to the Act.

Practical Advice

This decision represents a clear warning to employers — documents turned over to agencies during the investigation phase of an administrative charge, even if marked as confidential, are subject to disclosure to third parties. A thoughtless response to an EEOC information request could lead to disclosure of confidential and proprietary information, trade secrets and other highly sensitive corporate data. As such, it is critical that companies responding to the EEOC do not ignore the importance of careful response and production of documents to the Commission at all stages of the administrative process. Care must be taken in analyzing the information to be provided, with consideration of whether a response can be made without producing otherwise confidential or proprietary information. Be knowledgeable and understand your rights to challenge and/or limit information requests. Talk to legal counsel about protective measures such as submitting motions to quash a subpoena or for a protective order. At the very least, take the time to carefully review documents and to redact sensitive company information.

Supervisors

continued from page 2

Independent Judgment: A Revised Analysis

Without regard to the *kind* of judgment used, or which supervisory function is exercised, the judgment used must be free from the control of others. This means the action is not dictated by detailed instructions, such as rules, regulations, verbal instructions or a collective bargaining agreement. But the existence of a policy does not mean that no independent judgment is involved, if the individual still assesses and weighs factors in making a judgment.

In applying this standard, the Board explained that making a patient assignment purely on the basis of a policy of equalizing workloads does not implicate independent judgment. Neither does merely following a policy regarding how to respond to an emergency. Having the discretion to determine when an emergency exists or the authority to deviate from policy does involve the exercise of independent judgment. Such discretion, the Board said, rises above being merely "routine or clerical." Independent judgment requires not just making a determination that is essentially free from the control of others, but also weighing various factors and comparing and/or assessing alternative courses of action.

This was key in *Oakwood*, in which the Board determined that certain full-time charge nurses were supervisors and others were not. Oakwood is a 257-bed acute care hospital. The NLRB found that full-time ("permanent") charge nurses in several units exercised independent judgment in discharging one or more supervisory functions.

Charge nurses in the hospital's emergency department (ED) did not meet this test because, unlike their counterparts in other units, they did not weigh patients' needs and nurses' skills in making patient assignments. Instead, they assigned nursing staff to

continued on page 11

Selective Waiver

continued from page 1

The *Qwest Communications* decision leaves the Eighth Circuit as the only federal circuit embracing outright selective waiver of the privilege. It is safe to say the Tenth Circuit's decision extinguishes any hope that federal common law will provide an easy outlet for the huge pressure to which federal enforcers routinely subject the privilege.

Still, not all hope is lost. Even after the Tenth Circuit's ruling, there remains in some federal circuits, the Second in particular, a viable legal basis for accomplishing selective waiver by contract with the government enforcers to whom disclosures are made. Further, the Advisory Committee on the Federal Rules of Evidence has proposed a new Rule 502 that would expressly permit selective disclosure of privileged and work product material to the government, without waiver as to third parties.

'Voluntary' Production of Privileged Material

In many respects, the situation in which Qwest found itself in early 2002 has become unfortunately familiar. In response to subpoenas arising from the SEC and Justice Department's investigation into Qwest's business practices, the company produced hundreds of thousands of pages of documents otherwise protected by the attorney-client privilege and/or the work product doctrine.

Qwest made the production voluntarily, but also pursuant to written confidentiality agreements with both agencies. The agreements provided that the company intended no waiver of the privilege or work product doctrine. While the agreements also obligated the government to maintain the confidentiality of the documents, in the case of each agreement, that obligation was notably porous.

In parallel private securities class action litigation, Qwest declined to produce the privileged documents it disclosed pursuant to the government subpoenas. The plaintiffs moved to compel; the district court granted their motion. Noting that "the issue of selective waiver is of considerable public interest," the Tenth Circuit agreed to consider the merits of Qwest's petition for a writ of mandamus.

A Record-Based Rejection

As part of its exhaustive review of federal and state common law addressing selective waiver, the *Qwest Communications* court identified the three principal categories of selective waiver authority: "selective waiver is permissible; selective waiver is not permissible in any situation; and selective waiver is permissible in situations where the government agrees to a confidentiality order." With particular reference to the third of those categories, the court acknowledged authority from the Second Circuit holding that a *per se* rule of waiver was inappropriate in light of the potential for the disclosing party and the government to enter into an explicit confidentiality agreement.

Interestingly, the Tenth Circuit declined to categorize itself in any of the three approaches to selective waiver. Qwest invited the court to create a rule that would preserve privilege and work product confidentiality for documents produced to government enforcers pursuant to a confidentiality agreement. The

continued on page 8

	Federal Circuit Courts of Appeal Approach to Selective Waiver
First	Generally rejects selective waiver of attorney-client privilege and work product protection; however, leaves open issue of whether waiver applies to opinion work product. *U.S. v. MIT* (1997).
Second	Addresses selective waiver of attorney-client privilege and work product protection on case-by-case basis, with particular focus on the quality of any agreement with government enforcers. *In Re Steinhardt Partners* (1993); *In Re Natural Gas Commodity Litigation* (S.D.N.Y. 2005).
Third	Rejects selective waiver for both attorney-client privilege and work product, even in the instance of confidentiality agreement between government and disclosing party. *Westinghouse Electric Corp.* (1991).
Fourth	Generally rejects selective waiver of attorney-client privilege, but approves use of selective waiver for opinion work product. *In Re Martin Marietta Corp.* (1988).
Fifth	Fifth Circuit has not yet addressed selective waiver; doctrine rejected by one district court, based on 'great weight of authority.' *SEC v. Brady* (N.D. Tex. 2006).
Sixth	Rejects selective waiver for both attorney-client privilege and work product, even in the instance of confidentiality agreement between government and disclosing party. *In Re Columbia/HCA Healthcare* (2002).
Seventh	Court has not yet addressed selective waiver in context of disclosure to government enforcer; recent district court authority strongly suggests rejection of the doctrine. *Burden-Meeks v. Welch* (2003).
Eighth	Recognizes selective waiver of attorney-client privilege; rejects selective waiver of work product protection. *Diversified Industries* (1977); *In Re Chrysler Motors Corp.* (1988).
Ninth	Court has not yet addressed selective waiver in context of disclosure to government enforcer; recent district court authority strongly suggests rejection of the doctrine. *In Re Syncor ERISA Litig.* (2005).
Tenth	Addresses selective waiver of attorney-client privilege and work product protection on case-by-case basis, with particular focus on the quality of any agreement with government enforcers; has, however, rejected traditional rationale for selective waiver. *In Re Qwest Communications* (2006).
Eleventh	Court has not yet addressed selective waiver in context of disclosure to government enforcer.
D.C.	Generally rejects selective waiver of both attorney-client privilege; leaves open possibility for selective waiver of work product material. *In Re Subpoena Duces Tecum* (1984).
Federal	Has not addressed issue head-on, but has rejected selective waiver of privilege and work product in context of inadvertent disclosure. *Genentech, Inc.* (1997).

Selective Waiver

continued from page 7

court declined to adopt such a rule, but carefully attributed that refusal to the record before it. In particular, the court examined the SEC and Justice Department confidentiality agreements and found them insufficiently protective in light of the sensitive nature of the disclosures. Further, the court found insufficient support for the proposition that the rule of non-waiver Qwest promoted was necessary to encourage cooperation with the government. In short, the company sought an "entirely new privilege, *ie*, a government-investigation privilege." The court responded: not on this record is such a creation justified.

The Tenth Circuit's ruling undoubtedly adds to the difficulty faced by firms contemplating a voluntary production of privileged material to the government. However, one need not be a wide-eyed optimist to see that the Tenth Circuit's analysis clearly admits of the possibility that a different record — one, for example, with far tighter confidentiality commitments from the government — could produce a different result. In this sense, the Tenth Circuit aligns itself with the Second Circuit in that each appears willing to make a record-based judgment, on a case-by-case basis, about the appropriateness of selective waiver.

The most recent example of such an analysis in the Second Circuit — the *In Re Natural Gas Commodity Litigation* decision — found in favor of selective waiver based largely on the strength of the agreements negotiated between the disclosing party and the federal investigators. Short of relief through legislation or Federal Rules changes (and setting aside the Eighth Circuit's isolated position), the analysis now employed by the Second and Tenth Circuits is the corporate target's best hope for placating the government with privileged disclosures and maintaining the privilege as to others.

Thus, the key lessons from this latest installment in the selective waiver saga are: 1) the party must determine the applicable law on selective waiver and; 2) the party advocating such a position must make a record that will allow the court to reach a narrow judgment in favor of selective waiver based only on the facts before it. For the firm contemplating privileged disclosures to the government, one key decision point must be the quality of the confidentiality commitments the government is willing to make. Agreements such as those in *Qwest Communications* should cause the firm contemplating disclosure to give up on any expectation that selective waiver can be accomplished. Of course, as set out in the chart on page 7, in some federal circuits, such as the Sixth, not even the tightest confidentiality restrictions on the government will spare the disclosing firm from an outright waiver of the privilege.

The legal landscape for selective waiver has become clearer with the Tenth Circuit's addition. That may be cold comfort to the firm considering disclosure to the government. Pre-dictability, however, has its virtues, and corporate counsel can now evaluate the risk of privileged disclosures with greater confidence.

Proposed Rule 502 of the Federal Rules of Evidence

Proposed changes to the Federal Rules of Evidence could significantly impact the direction of selective waiver of the privilege and work product protection in federal cases. Proposed Rule 502(c) stakes out a bright-line rule in favor of selective waiver:

> **(c) Selective Waiver.** In a federal or state proceeding, a disclosure of a communication or information covered by the attorney-client privilege or work product protection — when made to a federal public office or agency in the exercise of its regulatory, investigative, or enforcement au-thority — does not operate as a waiver of the privilege or protection in favor of non-governmental persons or entities. The effect of disclosure to a state or local government agency, with respect to non-governmental persons or entities, is governed by applicable state law. Nothing in this rule limits or expands the authority of a government agency to disclose communications or information to other government agencies or as otherwise authorized by law.

The commentary to the new rule notes the conflict between courts holding that a waiver is a waiver for all purposes and those that allow selective waiver if accompanied by a sufficient confidentiality agreement with the government. The Committee Notes state the objective to resolve this conflict by a rule protective of selective disclosure, a rule that "furthers the important policy of cooperation with government agencies, and maximizes the effectiveness and efficiency of government investigations."

On the one hand, the proposed rule would provide disclosing parties considerable relief from the requirement that privileged material produced to the government be provided to third parties in parallel litigation. On the other hand, if adopted, the proposed rule would surely embolden government enforcers demanding a waiver of the privilege, as the consequences for making such disclosures could be greatly mitigated.

The Advisory Committee is accepting public comments on the proposed rule until Dec. 15, 2007, and a decision on adoption of the proposed rule will occur before December 2008. Under the Federal Rules Enabling Act, presumably, Proposed Evidence Rule 502, which will likely be transmitted to the Supreme Court after December 2007 will take effect Dec. 1, 2008, unless Congress passes a law that provides otherwise.

The decision to produce privileged information or work product to the government is never easy. However, either through recent case developments such as the Tenth Circuit's *Qwest Communications* decision or Proposed Rule 502(c) of the Federal Rules of Evidence, corporate counsel face less ambiguity in evaluating the consequences of such a decision.

Alexander "Sandy" Thomas is a partner and commercial litigator in Reed Smith's Falls Church, VA office. He previously served as a Trial Attorney in the Antitrust Division of the United States Department of Justice and a Special Assistant United States Attorney in Alexandria, VA. He frequently advises corporate counsel on issues relating to the attorney-client privilege and has written and spoken extensively on the subject.

New Federal Discovery Rules: A Compliance Roadmap

By Deidre Paknad

The *Zubulake* Checklist for Legal Holds

The *Zubulake* Checklist is virtually black letter law. It provides a straightforward, significant and difficult standard for your duty to preserve and duty to produce. This checklist reflects the *Zubulake V* opinion as well as trends in 30(b)(6) witness testimony, the Delaware standards, and aspects of the proposed Federal Rules for discovery.

- Affirmatively and repeatedly communicate legal holds to all affected parties.
- Monitor compliance with legal holds on an ongoing basis.
- Interview affected employees to determine sources of information.
- Actively manage and monitor document collections.
- Integrate retention policies and coordinators with discovery challenges and responsibilities.
- Enable the "discovery liaison" to readily describe information custodians, systems, storage, and retention policies.
- Thoroughly document and demonstrate the efficacy of your process.
- Prepare to take responsibility for ensuring that information is preserved, collected, and produced.

Revised Federal Rules of Civil Procedure have likely gone into effect as you read this. They place a very early focus on existing retention practices and the preservation and discovery of information. For companies without modern enterprise retention programs and robust legal holds processes, a thoughtful gap analysis and readiness plan should be completed immediately.

Some companies will face significant hurdles to readiness and compliance because:

- Many companies don't have modern enterprise retention programs that incorporate the vast amount of electronic information used and generated in the business;
- Companies may not have responded to earlier mandates by instituting formal legal holds procedures that include frequent notices, interviews with key players, ongoing compliance monitoring, and traceable document collections. Or, they may have manual procedures that lack continuity, repeatability and consistency; and
- Litigation departments (and IT organization in some cases) lack an inventory or map of the systems used across diverse businesses, the data created by them and the procedures and protocols for managing, recycling and archiving that data.

Four key areas that should be addressed by in-house counsel and compliance officers include:

1. Early E-discovery. Litigants must meet very early in litigation to discuss preservation and the discovery plans. This new requirement makes electronic evidence and discovery a central discussion in every case. Companies should also expect to testify on their retention practices very early in the matter to help their adversary better prepare for this process. This accelerated discovery discussion leaves little time to conduct early evidence inventories, get acquainted with retention practices or institute new preservation processes. This new rule puts a tremendous premium on readiness, transparency and process controls for in-house litigators — those with both offensive and defensive avenues and those without either. E-discovery compliance steps should include:

- Institution of a modern, global retention program that the litigation team can rely upon, including what types of information are generated in which businesses, where information is stored and who is knowledgeable about it; and
- Implementation of reliable preservation processes that quickly communicate holds, ensure preservation and provide defensive process integrity.

2. Disclosure. All parties will need to disclose the potential sources of relevant information, including those deemed inaccessible or those they don't intend to search or produce. This rule presumes that you can readily identify inaccessible information with some degree of specificity. Few companies have an accurate understanding of accessible data, much less inaccessible data. Without a map of information by location, compliance with this rule will be fraught with risk. This rule highlights the need for a reliable map that can be used to scope legal holds immediately and effectively. Disclosure compliance steps should include:

- Development and maintenance of a map of information sources. Leverage your past Sarbanes Oxley internal controls work, records coordinators and IT to develop and sustain it;
- Systematic synchronization of this map with corporate retention practices that identify the proper location not just the proper retention period; and
- Assurance that you can communicate and monitor holds even on inaccessible data with some degree of specificity as this will be a hotly contested element of litigation.

3. Form of Production. The default form for producing electronically stored information is that "in which it is ordinarily maintained [or] reasonably usable." With the vast majority of business information generated electronically, this requirement will force companies to revisit their retention programs to ensure that electronic information is included and adequately addressed. Chain of custody from the time of collection to production will be more important. A critical aspect of this will be the metadata and pseudo-data in native files, which increases the complexity. For example, you can reasonably anticipate that spreadsheets must be collected and produced with their formulas and calculations intact, just as a business user would need these to work with the file. Compliance steps should include:

- Development of the ability to collect evidence in its native forms without altering or over-processing it;

continued on page 10

Deidre Paknad is president of PSS Systems (www.pss-systems.com) in Mountain View, CA, a developer of information retention and preservation solutions for complex regulatory and litigation environments.

Discovery Rules

continued from page 9

- Assurance that you can demonstrate collection traceability and chain of custody on all electronic files and related metadata and pseudo data; and
- Institution of retention programs that define, enforce and audit lifecycles for electronic information as well as paper.

4. Failure to Make Disclosure or Cooperate in Discovery. The safe harbor provision provides that "absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system." While this provision appears to offer some relief from sanctions in routine instances of destruction of information, it also raises the bar on legal holds processes. Other provisions available to the courts continue to provide avenues to address spoliation and this does not exempt companies from their obligations to identify and preserve information. This provision shines a bright light on "routine, good faith operation" which arguably must include the ability to communicate legal holds promptly and repeatedly and to monitor compliance with them. Without a good process, the safe harbor will be difficult to invoke and may offer little safety at all. Compliance steps should include:

- Assurance that you have a good defense in a consistent, repeatable holds process that is easy to demonstrate; and
- Clear, consistent and affirmative legal holds communications within a process that includes the ability to identify the people and systems affected and effective ongoing monitoring capabilities.

Technical Solutions For Cost-Effective Control Options

A few companies with very early experience in complex electronic discovery and those that were stung first with sanctions and punitive damages or losses were quick to build their own in-house tools for sending notices, tracking collections and automating processes and record keeping.

There are now commercial solutions for managing legal holds, evidence collection, and global retention policies that can reduce the burden, risk, and complexity for corporations. These solutions can provide a critical information map and the necessary process and control framework to enable litigation and compliance managers to manage multiple concurrent holds and collections to meet more exacting process standards and reduce litigation costs and risks.

The New Rules: How Should Attorneys Prepare?

Considering the revised Federal Rules of Civil Procedure, companies should consider and plan for five areas of preparedness:

- **Legal Holds Process Review**. Companies should establish a threshold for anticipating litigation is, using *Zubulake V* for guidance. Decide in advance when and how often hold notices will be sent, institute confirmations of compliance, establish the interview process, determine necessary collection models and team members, develop reusable collection plans, and create an audit plan to test the process.
- **Control and Transparency**. The in-house attorney responsible for litigation should have rapid access to a current list of all legal holds, all custodians under a hold, and all active collections. Attorneys for each matter should have ready access to accurate information regarding all notices distributed for each matter, interviews conducted and findings, all evidence collected in the matter, and how and when it was collected.
- **Map of Data Sources**. Create a map that includes each data source and the individual responsible for it. This should include data sources and storage locations for active, inactive, and archived data. In addition, companies should clearly note the business processes that generate the data, the business units with ownership, and the staff responsible on both the business and IT sides.
- **Retention Program.** Often a weak spot, retention programs should be updated to address all records and to enable efficient, effective preservation. Upgrade the retention program to address electronic information and enterprise legal holds. The policy and schedules should specify lifecycles for all data, not just paper records. A critical element of this upgrade is the identification of records coordinators, offices of record, and custodial systems.
- **Communicate and Educate**. Educate the executive team on the changes in Federal Rules and brief senior management on the importance of legal holds — cite recent events as examples. Update corporate ethics and governance training to include compliance with legal holds and retention policies. Publish revised retention and legal holds policies and consider employee certifications of training and compliance.

Legal Data

continued from page 4

should be stored in a secure, dedicated environment installed behind that company's firewall. If that sensitive data is stored off site, it may be co-mingled with other companies' invoices.

- **Audit Access.** Vendor employees should *not* have the authority to view, alter or distribute your confidential legal and invoicing data.
- **Audit Termination Procedures.** An employee — either of the vendor or the corporation — should have access to confidential matter management and invoicing data cut off immediately upon termination of employment. Any lag in revoking privileges can lead to unauthorized access and SOX violations.

Security of legal and financial data is a critical matter that is often overlooked when selecting a technology provider for a law department. In addition to legitimate compliance concerns, there is also an array of potentially serious business implications. As a compliance officer, who may or may not be a member of the law department, this is an important issue that should be explored before any compliance concerns arise.

LAW JOURNAL NEWSLETTERS REPRINT SERVICE
Promotional article reprints of this article or any other published by LAW JOURNAL NEWSLETTERS are available.
Call Matt Solomon at 212-545-6289 or e-mail msolomon@alm.com
Reprints are available in paper and PDF format.

Base Salaries Up; Bonus Levels Mixed

Altman Weil In-House Counsel Survey Results Are In

The recently released *2006 Altman Weil Law Department Compensation Benchmarking Survey* of U.S. corporate law departments, published in partnership with LexisNexis Martindale-Hubbell, shows base salaries up across the board for in-house lawyers in 2006.

"Corporations have two tools to set in-house cash compensation — guaranteed base salary and at-risk, performance-based bonus dollars," notes Altman Weil principal James S. Wilber. "Each year we see a balancing act between these two components. Last year, salaries rose slightly, augmented by big bonuses. This year, we're seeing bigger salary increases reflecting greater corporate confidence, along with a mixed bag of bonus levels which seem designed to catch up some of the more junior in-house positions that were overlooked in past years."

"Increased mobility between law firms and law departments forces corporations to compensate more competitively in the war for talent, especially at the senior level," remarks Barry Solomon, Vice President and General Manager of LexisNexis Martindale-Hubbell. "As a result, corporations will reward their top law department officers first, and only later adjust compensation for junior managers and staff lawyers."

Base Salaries Rise

Median salaries for all positions in law departments increased between 2.2% and 9.5% in 2006. Chief Legal Officer (CLO) salaries were up 8% and Division General Counsel (mid-level management lawyers) took home 7.1% more. Lawyers in non-management positions also saw increases, with High Level Specialists up 9.5%, Senior Attorneys (non-managers with eight or more years experience) up 8.5% and Staff Attorneys (attorneys with at least one year of experience) reporting an increase of 3.5%. Recent graduates reported a modest 2.2% raise.

All trend comparisons are drawn from a super-group of over 200 law departments that have participated in the survey over sequential years.

The survey reports national median salary for Chief Legal Officers in 2006 at $280,000. The Senior Attorney position drew $140,000, while a new law school graduate earned a starting salary of $65,000.

Bonuses a Mixed Bag

Bonuses were up across the board for non-management positions in law departments — in some instances dramatically. Senior Attorneys reported bonus increases of 14.4% while more junior Attorneys and Staff Attorneys received bonus increases of 62.5% and 71% respectively. In the management ranks, Division General Counsel bonuses went up 20.29% and Managing Attorneys 25.32%. Chief Legal Officers and their Deputies received bonuses that were down from the prior year.

The national median bonus for Chief Legal Officers was $132,000, according to the Survey. Division General Counsel received $104,000 in bonus dollars, and Senior Attorneys took home a $29,200 bonus.

Stock Options

Stock options for Chief Legal Officers had a median fair market value of $919,400 in 2006, more than twice the same group's' total cash compensation. Deputy CLOs received $230,100 in stock options, Senior Attorneys $87,900 in options, and Staff Attorneys $24,700.

Other Variables

Size of law department is a key factor in the top officer compensation. Chief Legal Officers in departments with over 25 lawyers took home 88.9% more than the national median in total cash compensation. Deputy CLOs in large law departments earned 57.5% more than the national median.

The survey reveals a significant difference in CLO compensation by industry. Median total cash compensation for CLOs in the Information / Telecommunications sector was 75% more that their colleagues in the Service sector and 39.9% more in total cash compensation than their peers nationally.

In non-management positions, practice specialty is also a significant differentiator. High Level Specialists with a Mergers & Acquisitions specialty earn top dollar, 23.8% more than the national median in total cash compensation. For Senior Attorneys and Attorneys (with four-plus years experience), a Patents specialty is the most lucrative, at 22% and 33% above the national norms, respectively.

Survey Methodology

The complete *Law Department Compensation Benchmarking Survey, 2006 edition* contains data from 277 law departments providing compensation data for 6,255 lawyers. Information on an additional 41 one-lawyer departments is included separately.

The Survey reports data on nine in-house positions: Chief Legal Officer, Deputy Chief Legal Officer, Division General Counsel, Managing Attorney, High Level Specialist, Senior Attorney, Attorney, Staff Attorney and recent law school graduate. Data are analyzed by industry, company size (revenue and employees), law department size, region, metropolitan area, years of experience and other key parameters. Data are reported as of March 1, 2006.

—❖—

Supervisors

continued from page 6

areas of the department pursuant to a predetermined practice. Further, staff nurses in the ED rotated assignments without input from the charge nurses.

In *Oakwood*, the Board also evaluated whether 112 RNs who occasionally served as charge nurses were supervisors. It found there was not an established pattern or schedule for when and how often these RNs took turns in the charge role.

The Meaning of 'Assign'

Addressing one of the key supervisory functions at issue, the Board explained that giving employees significant overall duties, designating employees to work at a particular place or time, or instructing them to work overtime suggest classification as a supervisor, if these functions involve the exercise of independent judgment and constitute a substantial part of the individual's job.

To "assign" means to determine the time, place or overall work of an individual. This includes giving "significant overall duties," such as sending a worker to a particular department or shift or, in healthcare, assigning him a particular group of patients. While delegating a *group* of tasks is to "assign," simply determining

continued on page 12

Supervisors

continued from page 11

the order in which to perform those tasks is not. Designating an employee to be the one to carry out the general duty to administer medication to a group of patients is also to "assign." On the other hand, merely instructing the worker to give a sedative to particular patient is not.

The emergency department charge nurses in the *Oakwood* case "assigned" other employees within the meaning of the Act by designating them to work in specific areas. Unlike "straw bosses or lead men" who are not supervisors, these duties were more than "incidental" to their primary responsibilities.

In *Golden Crest*, the Board found the charge nurses did not "assign" work in a manner that made them supervisors. Specifically, these charge nurses lacked the authority to send other employees home early or to move workers from one floor to another. Likewise, they could not require an off-duty employee to report to work. Thus, lacking the authority to assign overall tasks or the time or place of the employee's work, these charge nurses were employees, not supervisors.

Likewise, they could not require an off-duty emplyee to report to work. Thus, lacking the authority to assign overall tasks or the time or place of the employee's work, these charge nurses were employees, not supervisors.

'Responsibly to Direct'

Even if an individual does not "assign" other employees, he or she may be a supervisor if he or she "responsibly" directs others. Like all of the supervisory functions, the purported supervisor must also hold authority in the interest of the employer and exercise a sufficient level of independent judgment. The key to this analysis is that the supposed supervisor must be held to a meaningful level of accountability.

The individual must have the authority to direct work, take corrective action and most importantly, must face the possibility of adverse consequences for shortcomings in the work.

Even in *Oakwood*, the Board found no evidence that the charge nurses responsibly directed other workers. They were responsible only for their own work. (The 12 "supervisors" were so designated because they carried out the "assign" function and exercised independent judgment in doing so.)

In *Croft Metals*, on the other hand, lead persons were held responsible for the direction of others. There, however, the Board found that these individuals were not supervisors because they did not exercise a sufficient level of independent judgment. This is because most of their decisions were, according to the record, either "pretty routine" or controlled by pre-established guidelines. Likewise, in *Golden Crest*, the Board found the charge nurses were not held accountable for the work of other employees.

The Board explained that this concept of accountability for the work of others helps create a clear distinction between supervisors (whose interests must align with management) and employees (who may have contradictory interests). In the Board's view, a supervisor sometimes may have a somewhat adversarial relationship to employees.

What Do These Decisions Mean For Employers

While many union members and advocates have denounced these decisions, they provide useful guidance that makes this analysis more predictable. As has been clear since the Supreme Court's *Kentucky River* decision, the exercise of a sufficient *degree* of independent judgment is essential to any supervisory function. The Board cannot insert artificial restrictions as to the *kind* of discretion being exercised. Further, the Board has provided some fairly specific examples of circumstances that it considers indicative of supervisory status and some that it does not, particularly in healthcare.

A job title does not determine whether someone is considered a supervisor or an employee. On the other hand, an organization's policies and its actual practices are critically important.

Union supporters insist that these decisions give employers a roadmap to deprive millions of workers, especially nurses, of their right to join a union. But in today's competitive environment, it appears unlikely that many employers will make broader business decisions in an effort to classify more workers as supervisors under the NLRA.

Conclusion

The *Kentucky River* decisions provide employers with new opportunities to assess job classifications, policies, practices, who to include in supervisory training programs and host of other issues. It also provides opportunities to engage in positive communications with employees and supervisors. Finally, the decisions give both management and labor the opportunity to evaluate the composition of current and prospective bargaining units.

All of these activities can reduce uncertainty, delays and controversy when classifying workers as employees or supervisors. The analysis of who is a supervisor and who is not remains controversial, but all sides should be able to agree that when it comes to the law, predictability is a good thing.

For even FASTER service, call:
Tel: (215) 557-2300 or (800) 999-1916

On the Web at:
www.ljnonline.com

Yes! *I'd like to order* ***The Corporate Counselor***® *today!*

Now just $329* (regularly $379...save $50!)

*Offer valid to new subscribers only

Publisher's Guarantee! You may cancel your subscription at any time, for any reason, and receive a full refund for all unmailed issues.

3038-2006