

As the ground shifts under executive risks, so do the rules of the road: White collar criminals have gotten a new Get-Out-of-Jail card, but it is not free, especially for the firms involved. Preserving and collecting electronically stored data is a hot litigation topic, one being addressed by innovative eDiscovery enhancements for ER policies and one that legal departments of companies of every size are well advised to take seriously.

A recent court case exemplifies the importance of eDiscovery in conjunction with privacy issues in the workplace and attorney-client privilege. This newsletter tries to shed some light on the road ahead so we don't mistake the edge of a cliff for a mere dip in the road. Consequences can be dire.

NEW SENTENCING GUIDELINES FOR CORPORATE CRIMINALS

The U.S. Sentencing Commission recently submitted to Congress amendments to the federal sentencing guidelines that would increase the alternatives to prison for white collar criminals and alter the sentencing of corporate offenders. Although no longer mandatory, they are important because judges still draw upon the sentencing guidelines in determining appropriate punishments for both individual and corporate offenders.

For individuals, the proposed amendments would provide for alternative sentencing options, such as split sentences: half in prison, half in alternative, home or community confinement. The commission also recommends that courts consider the effectiveness of residential treatment.

For corporations or organizations, the amendments focus on a governance structure that assigns compliance and ethics officers direct reporting obligations to the governing body of the organization (often the general counsel or the audit committee of the board), rewarding those that do with mitigating credits, even where a senior executive may have been involved in the wrongdoing.

The amendment also clarifies for companies the remediation efforts required of an effective compliance and ethics program, describing



CONTENTS

New Sentencing Guidelines for Corporate Criminals	1
eDiscovery Revisited	2
Workplace Emails: Employee Privacy and Attorney-Client Privilege	3
Contacts	4

the reasonable steps that an organization should take to respond appropriately after criminal conduct is detected and to prevent further similar criminal conduct. If undertaken, these actions could reduce the severity of the penalties assessed against these firms. The actions include:

- Notification by the organization to its employees and shareholders of its criminal behavior and its new compliance and ethics program.
- Periodic submissions to the court or probation officer, at intervals specified by the court, on the organization's (A) financial condition and results of business

e-Discovery refers to the information requested by a litigant which is stored in an electronic format and which the litigant intends to use as evidence in a case. Electronically stored information is more commonly referred to as “ESI.” ESI can encompass all forms of information kept in an electronic environment, such as data stored on backup tapes, retained in legacy systems or other data reserved for deletion on hard drives. Data may exist in a variety of data formats: as e-mail and spreadsheets (active); cookies and favorites (internet); and embedded information (metadata). (See *Manual for Complex Litigation* (Fourth) §11.446 (2003).)

Spoliation of evidence is “the intentional destruction of evidence ...” See *Black’s Law Dictionary* (Sixth Ed. 1990).

operations and accounting for the disposition of all funds received and (B) progress in implementing its new compliance and ethics program; including disclosure of any new criminal prosecution, civil litigation or administrative proceeding commenced against the organization, or any investigation or formal inquiry by governmental authorities.

- Notification to the court or probation officer immediately upon learning of (A) any material adverse change in its business or financial condition or prospects or (B) the commencement of any bankruptcy proceeding, major civil litigation, criminal prosecution or administrative proceeding against the organization, or any investigation or formal inquiry by governmental authorities regarding the organization.
- Submission to (A) a reasonable number of regular or unannounced examinations of its books and records at appropriate business premises by the probation officer, experts engaged by the court or independent corporate monitor, (B) a reasonable number of regular or unannounced examinations of facilities subject to probation supervision and (C) interrogation of knowledgeable individuals within the organization.

Prudent organizations will take note: These amendments by the Sentencing Commission to the guidelines automatically become effective on November 1, 2010 if not rejected by Congress.

eDISCOVERY REVISITED

With one major carrier introducing an innovative eDiscovery enhancement for its Executive Risks renewals (on Directors & Officers, Errors & Omissions, Employment Practices and Fiduciary Liability coverage) and another poised to do so, we are pleased to deliver some good news along with warnings about the consequences of failure in this arena. With electronic discovery mandatory in federal courts as well as the majority of state courts, it is a critical issue for legal departments of public and private companies, large and small.

In the recently amended opinion in *Pension Committee*,¹ the court considered – not the deliberate destruction of data – but rather a “careless and indifferent” preservation and collection of data by the plaintiff. In this seminal case, Judge Scheindlin² first noted that “Courts cannot and do not expect that any party can meet a standard of perfection” before stating that “[b]y now, it should be abundantly clear that the duty to preserve [data] means what it says and that a failure to preserve records – paper or electronic – and to search in the right places for those records, will inevitably result in the spoliation of evidence.” After these portentous words, she then provided instructions on just what courts **are** likely to expect.

Some will recognize the irony in that it was the plaintiff in this case, rather than the defendant, whose handling of eDiscovery was questioned and ended up with monetary sanctions, even though the



situation did not involve any “egregious examples” of intentional destruction of documents. An important read, the ruling also tackled the issue of burden of proof as well as remedies which can include cost-shifting, further discovery, fines, special jury instructions, preclusion and most ominously, a default judgment or dismissal of the action.

WORKPLACE EMAILS: EMPLOYEE PRIVACY AND ATTORNEY-CLIENT PRIVILEGE

Do employees have a reasonable expectation of privacy as to attorney-client privileged emails on a workplace computer? As a general matter, employees have no right to privacy as respects workplace emails. But in a case involving employment litigation, the Supreme Court of New Jersey said yes, holding that, under the circumstances presented, the employee/plaintiff **did** have a reasonable expectation of privacy regarding emails with her attorney.³

The plaintiff in the employment discrimination action had used her work computer while still employed to communicate with counsel concerning a potential action against her employer via her personal email account. After employment ceased and litigation had ensued, the employee’s computer was examined as part of the eDiscovery process. Defense counsel for the company found and reviewed this correspondence and failed to alert plaintiff’s counsel as to these otherwise privileged emails. Instead, they referenced and attached some of the plaintiff’s emails in their interrogatory responses.

When plaintiff’s counsel objected and sought to bar use of these emails, she was initially rebuffed with the trial judge’s ruling that the emails “were not protected by the attorney-client privilege because the company’s electronic communications policy put plaintiff on sufficient notice that her emails would be viewed as company property.”

This was reversed on appeal. The higher court discussed two competing policy issues: enforcement of the company’s own electronic communications policy versus the broader public policy supporting preservation of the attorney-client privilege.

In addressing the “enforceability of a company policy, which purports to transform private emails or other electronic communications between an employee and the employee’s attorney into company property” the court found that this would require a balancing of the company’s right to create and obtain enforcement of reasonable rules for conduct in the workplace against the public policies underlying the attorney-client privilege. The court held that, to be enforceable, the regulated conduct should relate to employment and should “reasonably further the legitimate business interests of the employer.”

In examining the company's specific email policy, the court found it to be ambiguous. The policy stated that all communications on the company's systems belong to the employer and that employees should have no expectation of privacy for any communications. However, the policy also allowed for "occasional personal use." The court ruled that an employee could interpret "occasional personal use" as personal, privileged communications. Thus, the appellate court held that the employer's access might not extend to such communications, even from its own systems.

The case was remanded back down to the trial court to determine what, if any, sanctions should be imposed upon defense counsel for reading and utilizing the emails at issue, despite indications that they were protected as privileged.

¹ *Pension Committee of the University of Montreal Pension Plan, et al. v. Banc of America Securities*, No. CIV 05-9016, 2010 U.S. Dist. LEXIS 1839 (SDNY Jan 11, 2010), <http://www.technologyinlitigation.com/PensionCommittee.pdf>

² Yes, this is the same judge and same court that handed down the ground breaking 2004 *Zubulake* decision.

³ *Stengart v. Loving Care Agency, Inc.*, 2010 WL 1189458 (N.J. Mar. 30, 2010)

Executive Risks Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.

CONTACTS

For additional information, please contact your Willis Client Advocate® or

Atlanta, GA

Charles Maxell
404 224 5123
charles.maxell@willis.com

Boston, MA

David Goldstein
617 351 7498
david.goldstein@willis.com

Chicago, IL

Brian Gauen
312 621 4855
brian.gauen@willis.com

Denver, CO

Jim Iacino
303 218 4039
jim.iacino@willis.com

Los Angeles, CA

Brendan Dolan
949 930 1765
brendan.dolan@willis.com

New York, NY

Steve Pincus
212 915 7940
steve.pincus@willis.com

Radnor, PA

Matt Schott
610 254 5642
matt.schott@willis.com

San Francisco, CA

Michael Mahoney
415 291 1535
mike.mahoney@willis.com