

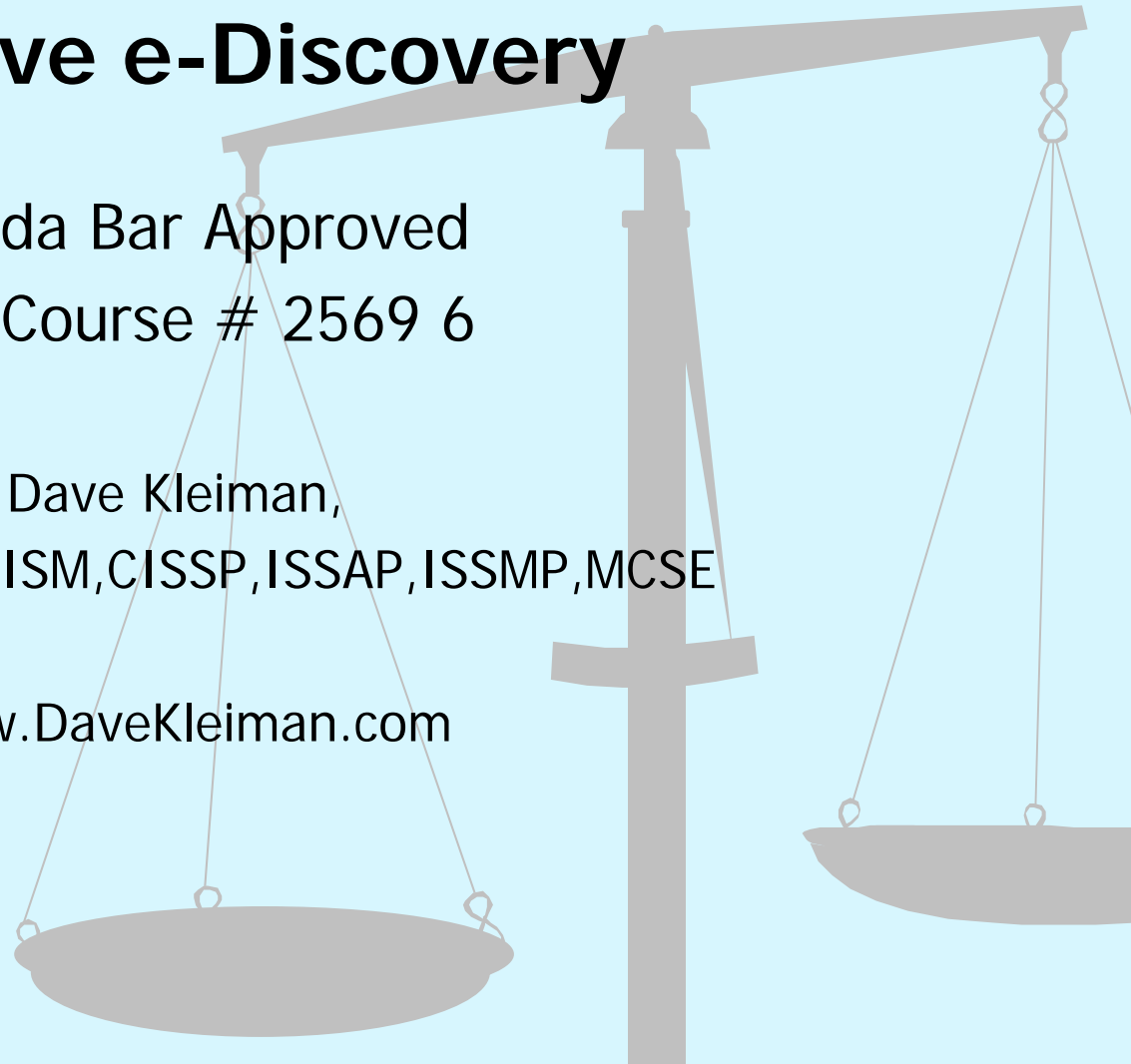
# Welcome!!

## Effective e-Discovery

Florida Bar Approved  
CLE Course # 2569 6

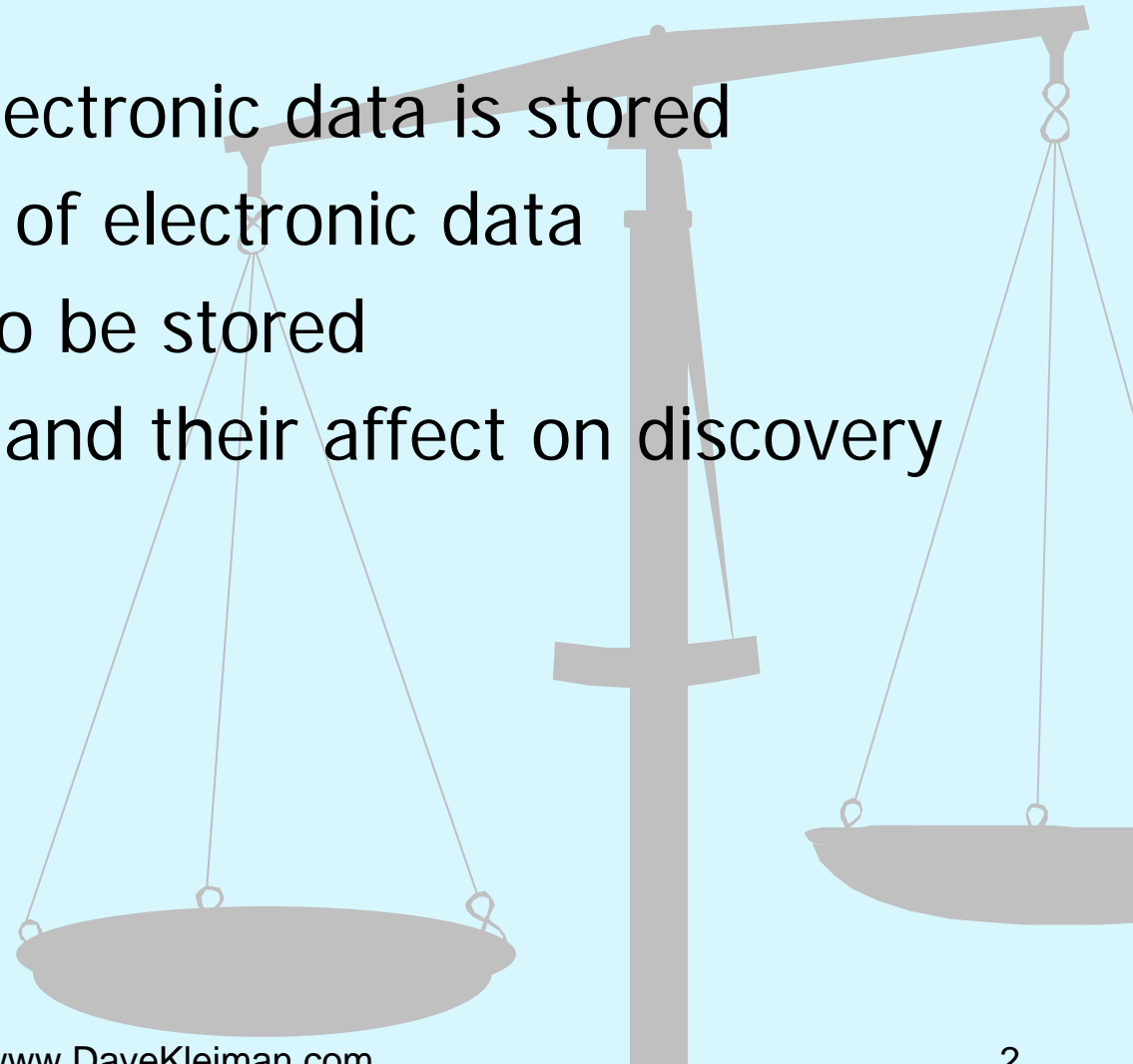
Dave Kleiman,  
CAS, CCE, CIFI, CISM, CISSP, ISSAP, ISSMP, MCSE

[www.DaveKleiman.com](http://www.DaveKleiman.com)



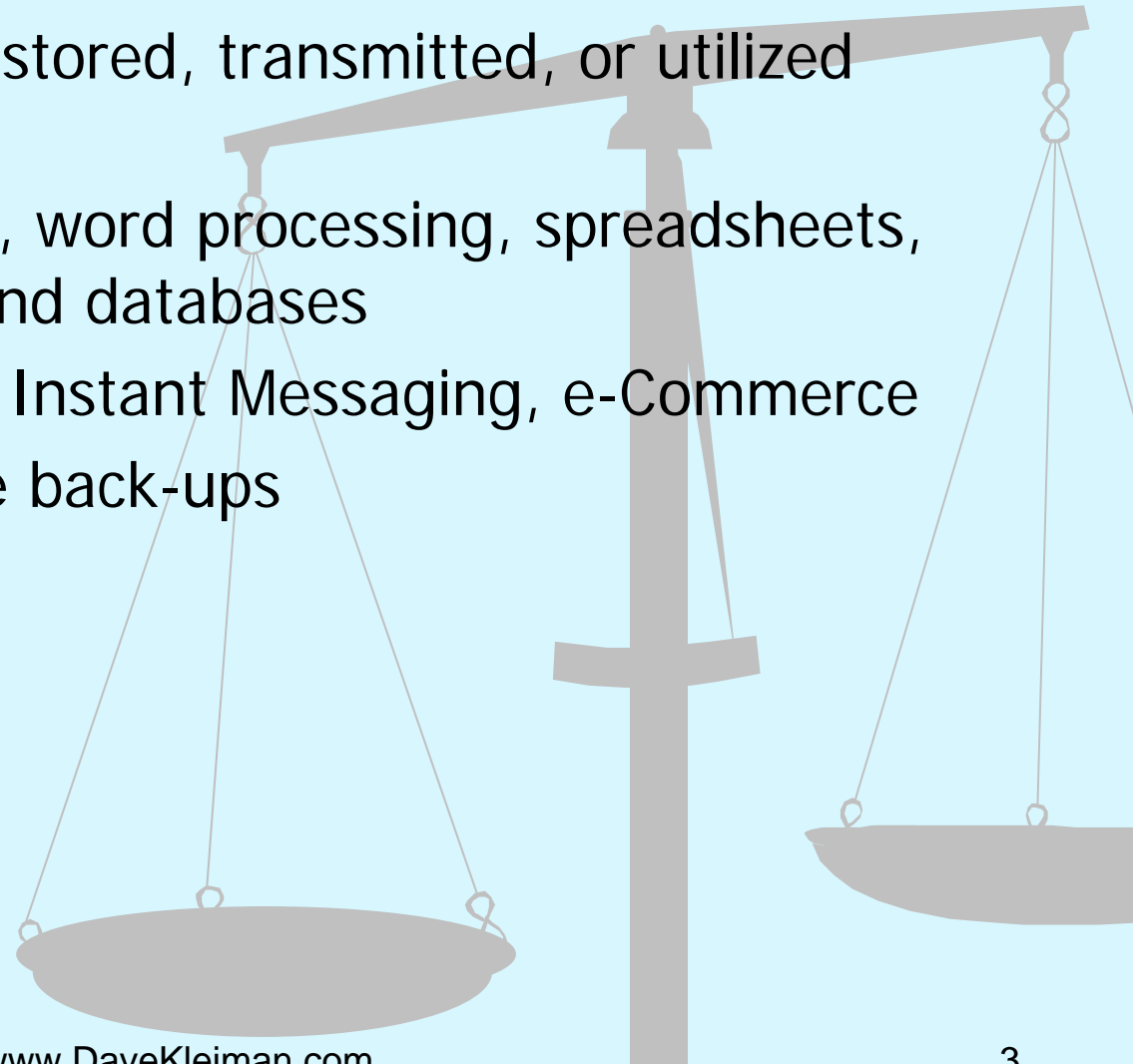
# Understanding the world of e-Discovery

- Where and how electronic data is stored
- The sheer volume of electronic data
- What is required to be stored
- Retention policies and their affect on discovery requests.



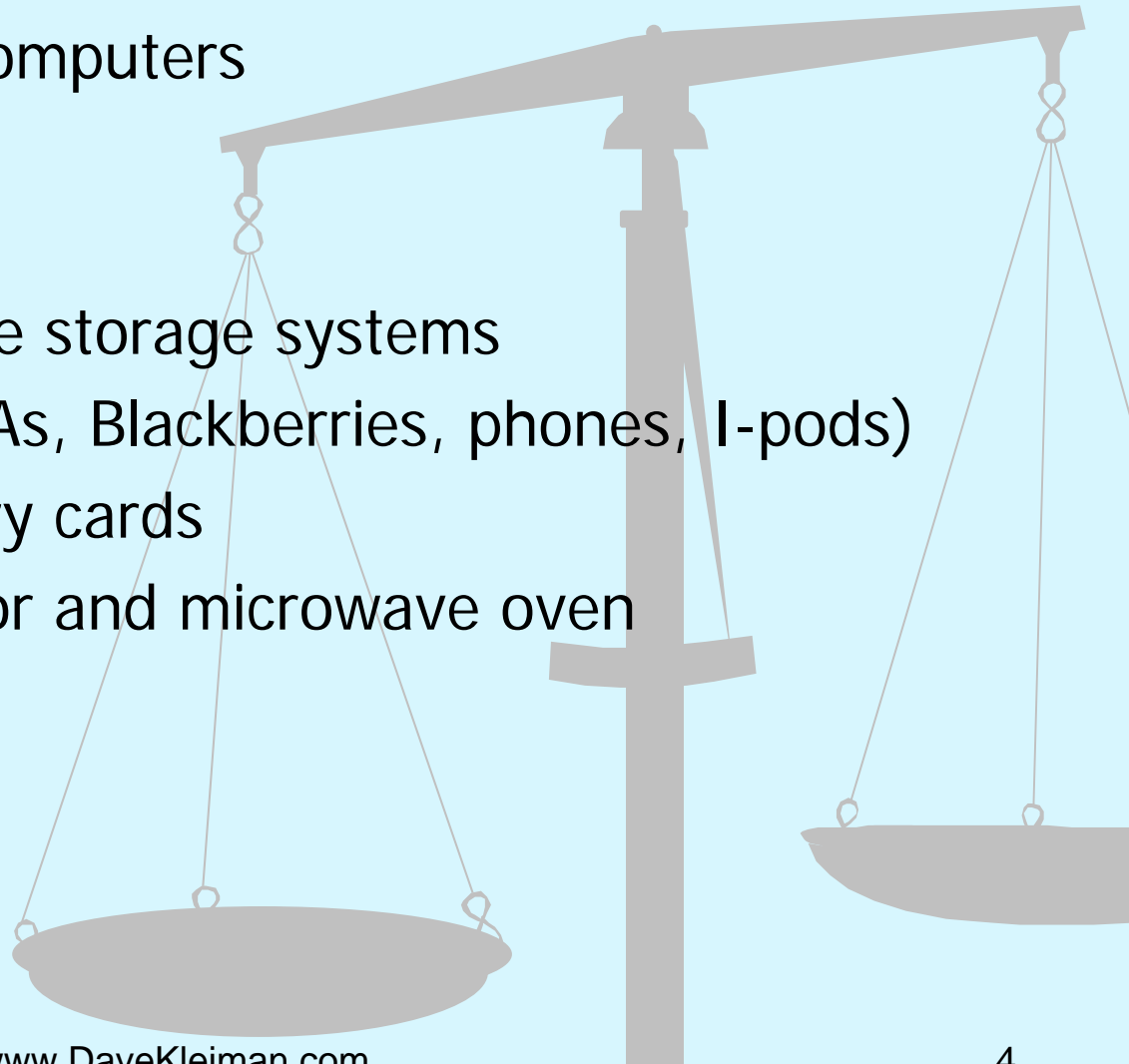
# What is electronic data?

- Information created, stored, transmitted, or utilized electronically
- Business applications, word processing, spreadsheets, financial programs, and databases
- The Internet, e-mail, Instant Messaging, e-Commerce
- DVDs, CDs, and Tape back-ups



# Where do we find electronic data?

- Desktop and Laptop computers
- Network servers
- Internet
- Backup and Removable storage systems
- Handheld devices (PDAs, Blackberries, phones, I-pods)
- Cameras, cars, memory cards
- Maybe your refrigerator and microwave oven

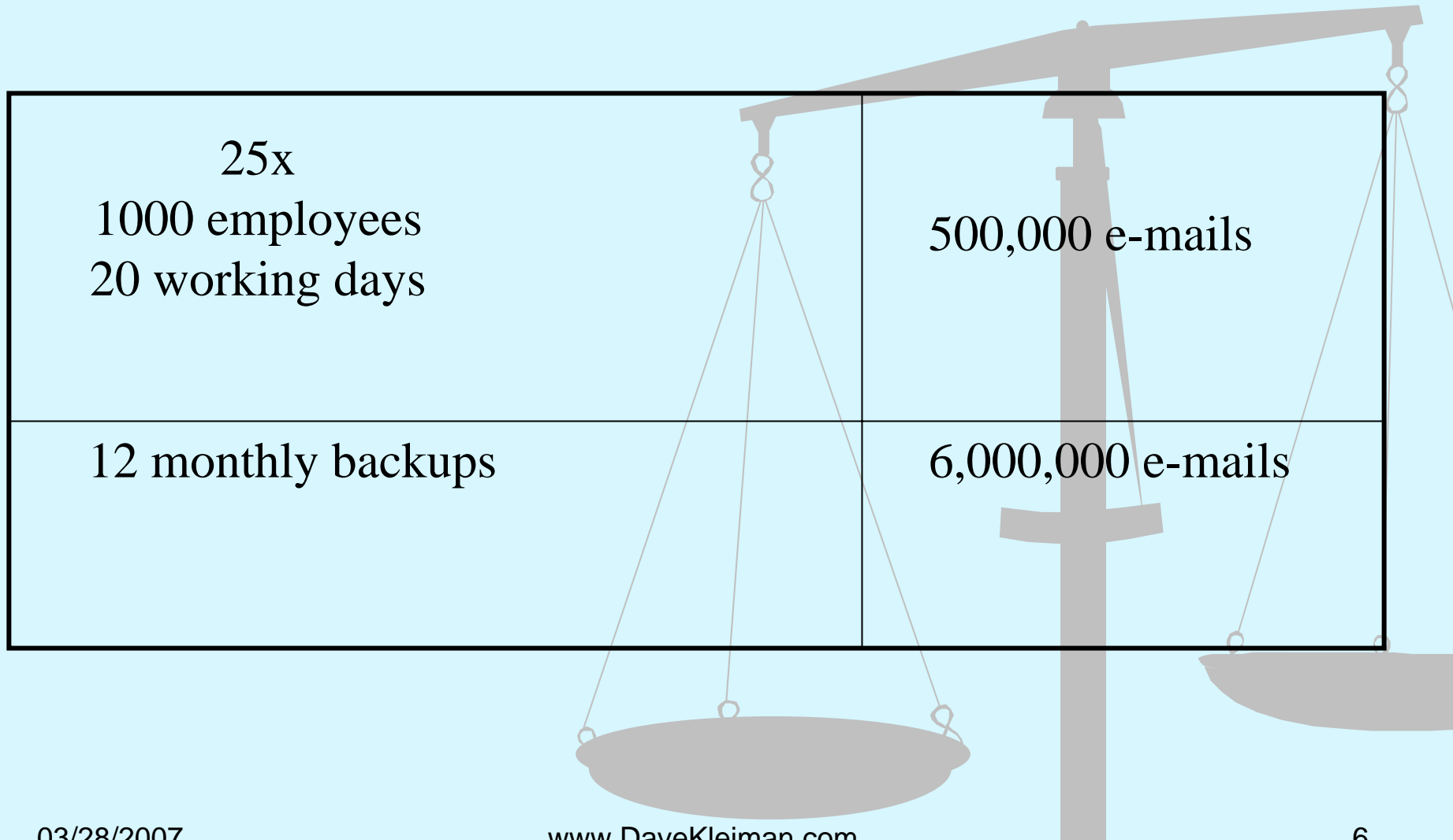


# How much electronic data is there?

92% of all information generated in 2003  
was on “magnetic” media

University of California at Berkeley/School of Information Management and Systems,  
“How Much Information,” <<http://www.sims.berkeley.edu/how-much-info-2003>>

# 25 e-mails a day?



# What is required to be “stored”

- There are currently over 10,000 U.S. federal, state, and local laws and regulations addressing what, how, when and why records must be created, stored, accessed, maintained, and retained over increasingly longer periods of time
- Many of these mandates carry stiff penalties, including fines and imprisonment.
- As a result, companies in all industries are now scrambling to gain “compliance”

# Compliance Roles (SOX)

BEHAVIOR	SENTENCE
The alteration, destruction, concealment of any records with the intent of obstructing a federal investigation.	Fine and/or up to 10 years imprisonment.
Failure to maintain audit or review “workpapers” for at least five years.	Fine and/or up to 5 years imprisonment.
Anyone who “knowingly executes, or attempts to execute, a scheme” to defraud a purchaser of securities.	Fine and/or up to 10 years imprisonment.
Any CEO or CFO who “recklessly” violates his or her certification of the company’s financial statements.  If “willfully” violates.	Fine of up to \$1,000,000 and/or up to 10 years imprisonment.  Fine of up to \$5 million and/or up to 20 years imprisonment.
Two or more persons who conspire to commit any offense against or to defraud the U.S. or its agencies.	Fine and/or up to 10 years imprisonment.
Any person who “corruptly” alters, destroys, conceals, etc., any records or documents with the intent of impairing the integrity of the record or document for use in an official proceeding.	Fine and/or up to 20 years imprisonment.
Mail and wire fraud.  Violating applicable Employee Retirement Income Security Act (ERISA) provisions.	Increase from 5 to 20 years imprisonment.  Various lengths depending on violation.

\* Source: Sarbanes-Oxley Act of 2002 and New York City Office of the Comptroller.

# Counsel's Responsibility

Zubulake II (LAURA ZUBULAKE, plaintiff)

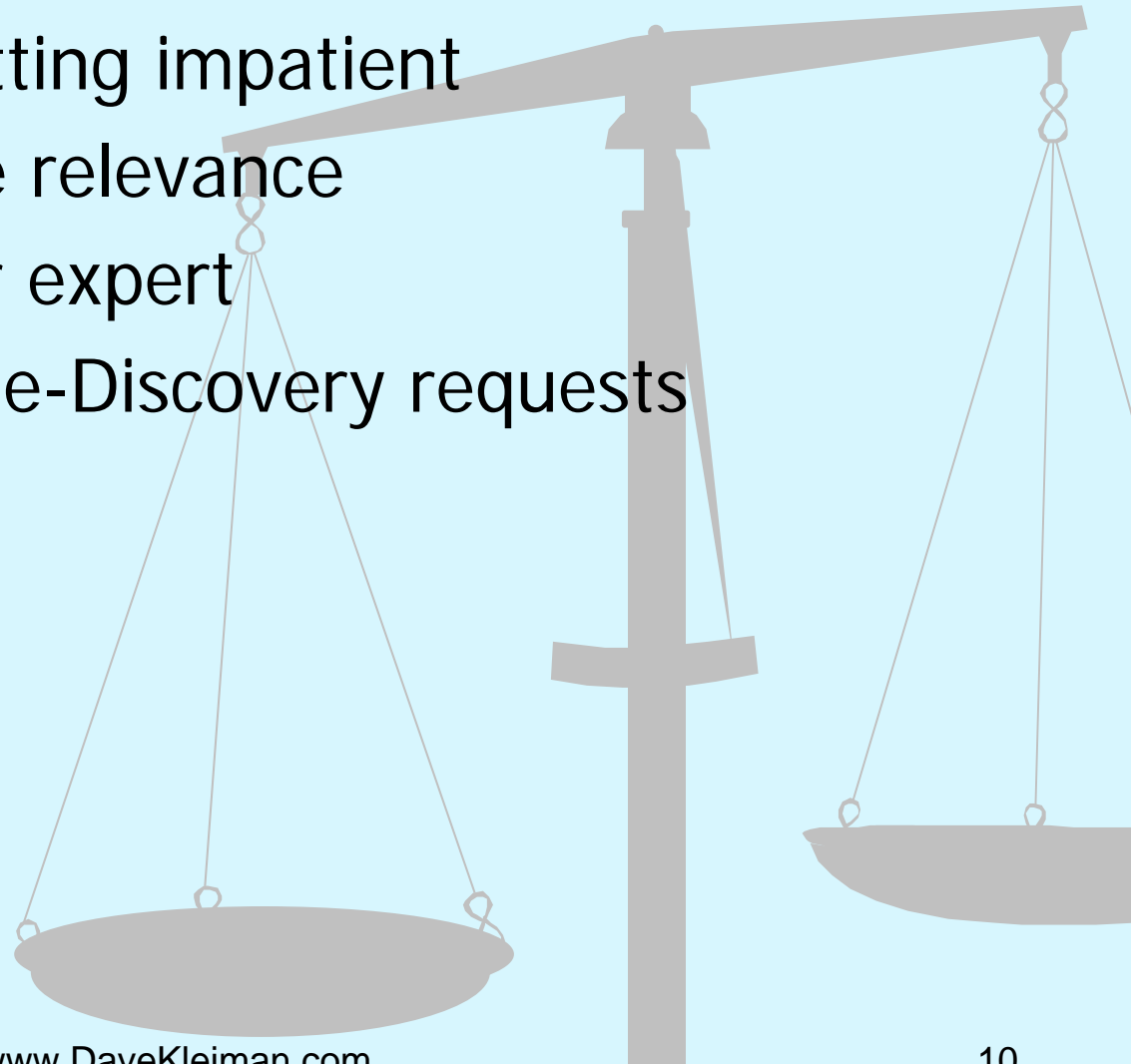
Vs.

UBS WARBURG LLC, UBS WARBURG, and UBS AG

- This decision addresses counsel's obligation to ensure that relevant information is preserved by giving clear instructions to the client to preserve such information and, perhaps more importantly, a client's obligation to heed those instructions.
- Early on in this litigation, UBS's counsel — both in-house and outside — instructed UBS personnel to retain relevant electronic information. Notwithstanding these instructions, certain UBS employees deleted relevant emails. Other employees never produced relevant information to counsel. As a result, many discoverable e-mails were not produced to Zubulake until recently.

# Costs of performing and ignoring e-Discovery

- The courts are getting impatient
- Understanding the relevance
- Working with your expert
- Streamlining your e-Discovery requests
- Spoliation



# Cost is borne by demanding party?

- Courts continue to struggle with apportioning the substantial costs of e-discovery
- Decisions from New York in *Zubulake v. UBS Warburg* have had significant impact in cost shifting
- NY Opinion – e-discovery costs apportioned between the parties
- Producing party usually pays cost of production
- Producing party must translate data stored electronically into a “reasonably usable form.”
- Google: “**Passing the Buck: Cost-Shifting in Electronic Discovery**”

## Fines and Sanctions



- We have seen an increasing willingness by courts to impose extraordinary and costly sanctions for e-Discovery violations.
- July 2004 - the federal court in Washington D.C. sanctioned Philip Morris \$2.75 million for the deletion of emails by senior executives
- April 2005 - a verdict was rendered in the much discussed Zubulake case in an amount of \$29.3 million - failure to properly preserve email

## 1.4 Billion Lesson of Morgan Stanley

- A Florida jury awarded 1.4 billion in damages to Ronald Perelman on his claim that Morgan Stanley defrauded him as part of a 1998 sale of his controlling stake in Coleman Co. to Sunbeam Corp.
- The court found that Morgan Stanley failed to preserve e-mail by allowing e-mail to be overwritten after 12 months, despite an SEC regulation requiring all e-mail to be retained in readily accessible form for two years
- The court also found that Morgan Stanley failed to comply with discovery deadlines and the timely notification to the court of over 2000 later discovered e-mail back-up tapes relevant to the pending litigation

## Florida 1.280

- Florida 1.280 General Provisions Regarding Discovery
- 1.280 b(4)C.....**party seeking the discovery pay the expert a reasonable fee for time spent in responding to discovery**
- ...an expert shall be an expert witness as defined in rule 1.390(a)

## Florida 1.280

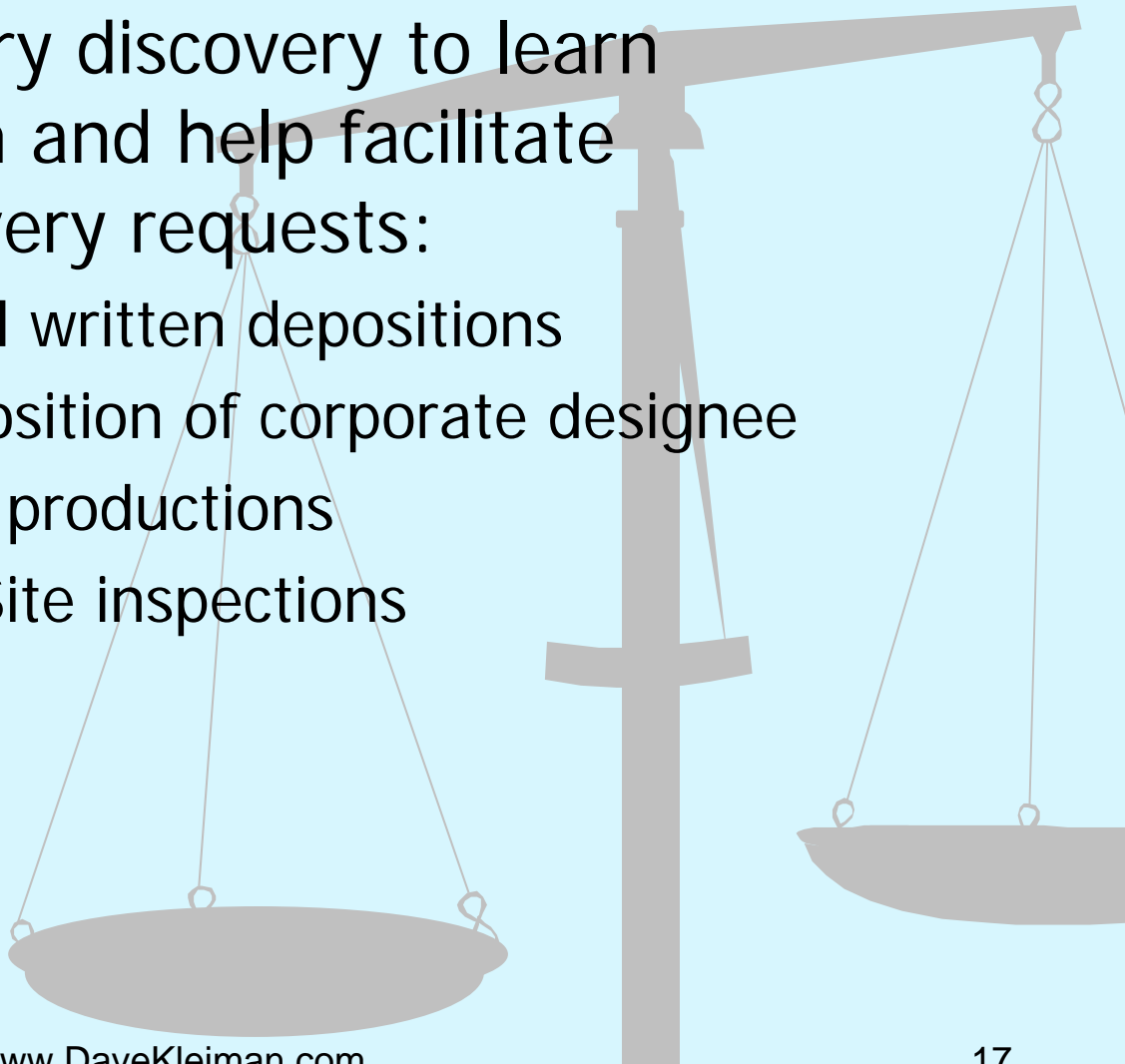
- ...note the rule is derived from FRCP 26...general rearrangement is more logical and is the result of 35 years experience under the federal rules
- Further amended in Supreme Court *Elkins v. Syken*...avoid annoyance....undue expense while still permitting the adverse party to obtain relevant information.....

# Know your expert

- Florida RULE 1.390 DEPOSITIONS OF EXPERT WITNESSES
- (a) Definition. The term "expert witness" as used herein applies exclusively to a person duly and regularly engaged in the practice of a profession who holds a professional degree from a university or college and has had special professional training and experience, or one possessed of special knowledge or skill about the subject upon which called to testify.
- (b) Procedure. The testimony of an expert or skilled witness may be taken at any time before the trial in accordance with the rules for taking depositions and may be used at trial, regardless of the place of residence of the witness or whether the witness is within the distance prescribed by rule 1.330(a)(3). No special form of notice need be given that the deposition will be used for trial.

# Working with your expert

- Conduct preliminary discovery to learn opponent's system and help facilitate streamlined discovery requests:
  - Interrogatories and written depositions
  - Rule 30(b)(6) Deposition of corporate designee
  - Rule 34 Document productions
  - Rule 34(a)(2) On-Site inspections



# Test your expert

- Always “Clone” Relevant Data First
  - *Gates Rubber Co. v. Bando Chemicals Industries, Inc.*, 167 F.R.D. 90 (D. Colo. 1996) (court criticized expert for failure to create an image copy of hard disk, concluding party has duty to “utilize the method which yields most complete and accurate results”)
- References?
- Certified?

# Streamline discovery requests and responses

- These will probably be viewed as overly-broad; or, if they can be done in a timely manner, at least shift the cost to the requesting party because they are burdensome
  - Let us copy (image) all of your computers
  - Give us **all** readily accessible electronic documents
  - Give us **all** active, deleted, fragmented, archived, etc. electronic documents

## Streamline discovery requests and responses (Con't)

- *In Zubulake III*, the time frame noted by the requesting party was approximately 18 months and the request was limited to only 5 individuals
- The court specifically noted that this was “a relatively limited and targeted request”

# Streamline discovery requests and responses (Con't)

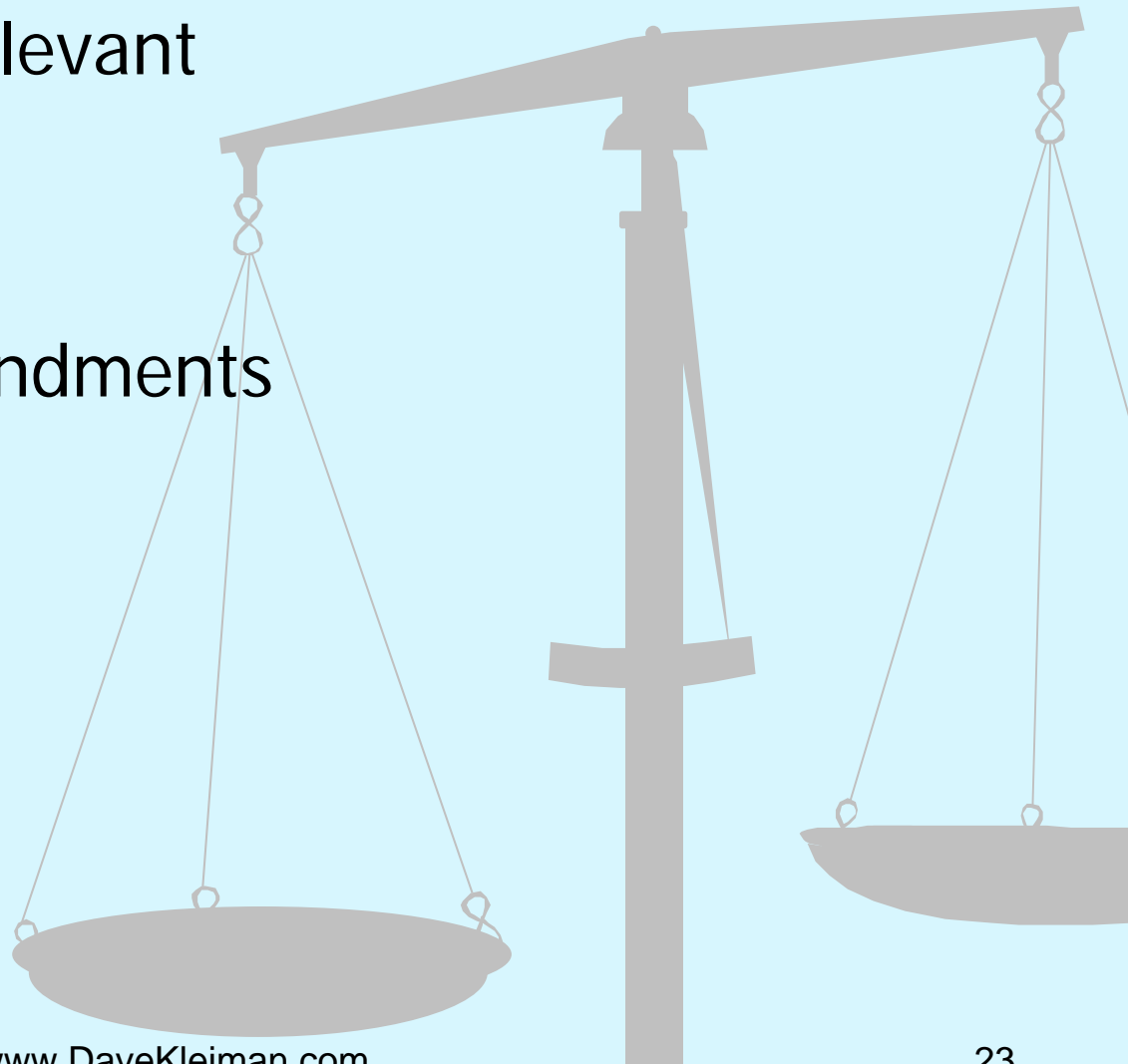
- Limit the discovery requests to particular time periods
- Limit the discovery request to specific party or parties
- Limit the discovery request to relevant information (e.g. if you are looking for e-mails specify e-mails)
- Know where it is located
- Know if it is "accessible" or "inaccessible"
- Many of the cost-shifting cases center on inaccessible data
- Cost-shifting is less likely to be granted for accessible data

# Spoliation

- Unless justified by the responsible party, .....it can be the intentional destruction, concealment,.... **or failure to preserve documents**... or other evidence reasonably known at the time of it's elimination, to be relevant to the issues.... shall be subject to sanctions.... that could cause significant prejudice to the ability to prove or disprove a element of the cause of action or defense.
- Send Preservation/Spoliation Notice Letters
- Seek Preservation Orders

# Understand importance of the rules

- Which rules are relevant
- Protective orders
- Recent cases
- Changes and amendments



## Example Rule 26(c)

- Rule 26(c) specifies a nonexclusive list of provisions that could be adopted in a protective order, including:
- the disclosure or discovery not be had;
- the disclosure or discovery may be had only on specified terms and conditions, including a designation of the time or place;
- the disclosure or discovery may be had only by a method of discovery other than that selected by the party seeking discovery;
- certain matters not be inquired into, or that the scope of the disclosure or discovery be limited to certain matters;
- that discovery be conducted with no one present except persons designated by the court.....etc

# Proposed Electronic Discovery Rule Amendments

Could Take effect on December 1, 2006

*Already passed by the Supreme Court*

- For additional information, including the proposed amendments, public comment, and transcripts of the public hearings, see:

<http://www.uscourts.gov/rules/proposed0205.html>

# Already approved by Supreme Court

- On April 12, 2006 the United States Supreme Court approved, without comment or dissent, the entire package of proposed amendments to the Federal Rules of Civil Procedure concerning the discovery of "electronically stored information." The package includes revisions and additions to Rules 16, 26, 33, 34, 37, and 45, as well as Form 35. The proposed amendments were transmitted to the Supreme Court last September, after the Judicial Conference unanimously approved them.
- The new rules and amendments have now been transmitted to Congress and will take effect on December 1, 2006, unless Congress enacts legislation to reject, modify, or defer the amendments. The amendments may be accessed on the U.S. Court's Federal Rulemaking website at:  
<http://www.uscourts.gov/rules/newrules6.html>

# Subjects of e-Discovery rule amendments

- Electronic discovery issues, including form of production, preservation of electronically stored information (ESI), and review of such information for privilege;
- Discovery of ESI that is not reasonably accessible
- Assertion of privilege after production
- Application of Rules 33 and 34 to ESI; and Limit on sanctions under Rule 37 for the loss of ESI as a result of the routine operation of computer systems.

## FRCP 26 and 34

- Initial Disclosures and Document Production
- The phrase "electronically stored information" (ESI) was added to the disclosure requirement to align with the amendment to the definition of document.
- ESI changed to a separate category.
- The default option for form of production was revised from "...production in a form in which it is ordinarily maintained or in an electronically searchable form" to "in a form or forms that are reasonably usable by the requesting party or in which it is ordinarily maintained."

## FRCP 26(b)(5) – Inadvertent Waiver

- When information is produced subject to a claim of privilege, the producing party may, within a reasonable time, notify any party that received the information of the claim and the basis for it.
- After being notified, the receiving party must promptly return/destroy the specified information (or file it under seal) and may not use or disclose it until the privilege claim is resolved.
- If the receiving party already disclosed the information before being notified, it must take reasonable steps to retrieve it.

## FRCP 33 - Interrogatories

- An answer to an interrogatory involving review of business records should involve a search of electronically stored information
- An answer may permit the responding party to answer by providing access to that information.

## FRCP 37(f) – Safe harbor

- Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide ESI deleted or lost as a result of the routine, good faith operation of the party's electronic information systems.
- Dropped from the original version are the requirements that to take advantage of the safe harbor, the producing party must
  - “[take] reasonable steps to preserve the information after it knew or should have known the information was discoverable” and
  - “not have violated any court order requiring it to preserve electronically stored information.”

# How We Can Help

- Helping firms with digital data
  - Meeting the challenges of the discovery process
    - Becoming routine part of business
    - Help identify key components for the discovery process

We provide strategic and technical expertise on handling electronic evidence

- Educating firms and helping them facilitate e-data management
- Ensuring compliance with subpoenas and e-Discovery requests
- Internal investigations, civil, and criminal matters
- Evidence preservation:
  - Locating, preserving, and analyzing data, maximize evidence availability and quality; and maintain evidence integrity during process