

# Digital Evidence

How to Preserve, Discover and Use it.

***ATTORNEY WILLIAM C. GLEISNER, III***

Hartland, Wisconsin 53029

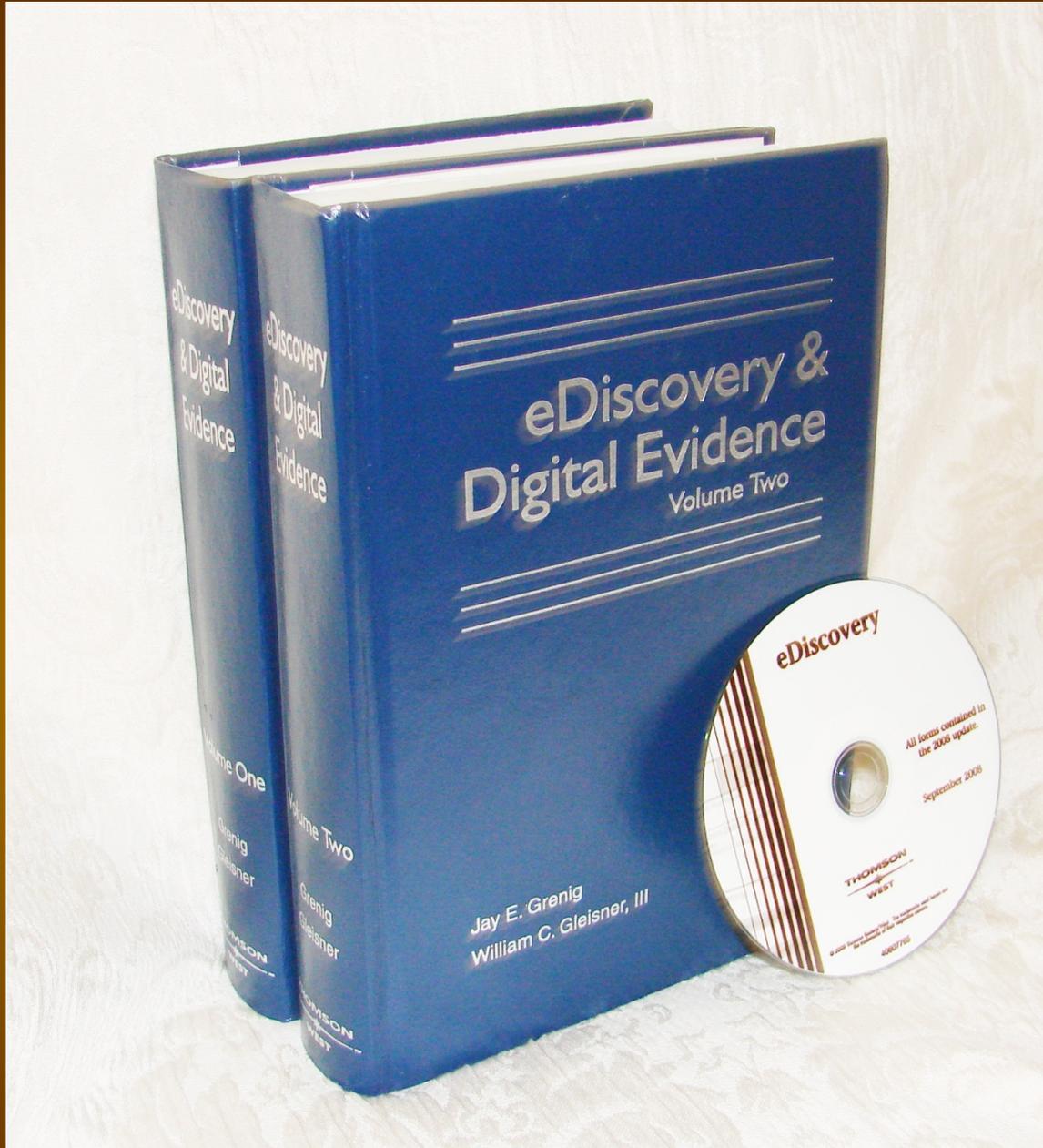
Telephone: 262-367-1222

Fax: 262-367-1236

Email: [wgleisner@sbcglobal.net](mailto:wgleisner@sbcglobal.net)

# A little about me...

- I retired several years ago to the Lake Country of rural Wisconsin; which means I only work 50 hours per week. 😊
- But I started doing electronic litigation 20 years ago as a civil rights litigator.
- I became fascinated. I became a MCSE and a Summation Certified Trainer and consulted with law firms all over the U.S.



© William C. Gleisner, III 2012. All Rights Reserved.

# WISCONSIN JUDICIAL COUNCIL

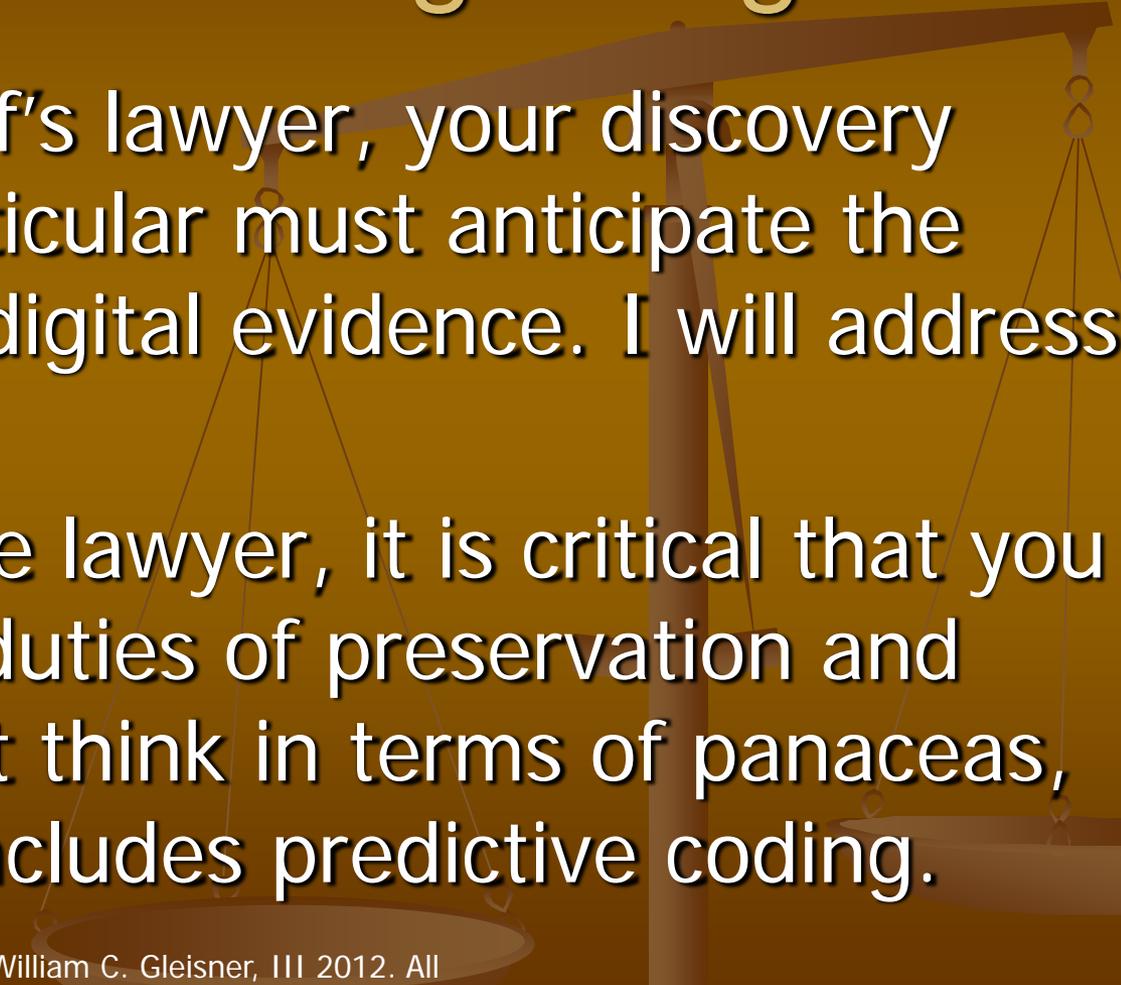
- The Judicial Council is well represented at this seminar. Professor Grenig, Judge Leineweber, Assistant Attorney General Moriarity and Waukesha District Attorney Schimel have served or still serve on the Council. I have served on the Wisconsin Judicial Council since 2008. Two years ago I was elected to a three year term as one of 3 State Bar Representatives.
- I was on the Council Committee Chaired by Judge Leineweber which spent three years studying e-discovery. This led to the adoption of Wisconsin's new e-discovery rules, based on the 2006 federal rules.

# The Need for a New Legal Education Paradigm



- The Legal profession has been very slow to adapt to the realities of the digital age.
- The problem starts in law school.
- You can't learn "best practices" from CLE courses. You need a new mindset.
  - Lawyers must learn to "think digital."
  - Litigators especially need to adopt a digital mindset and corresponding methodologies.

# The Mindset of a Good Litigator in the Digital Age



- If you're a plaintiff's lawyer, your discovery techniques in particular must anticipate the pervasiveness of digital evidence. I will address this later today.
- If you're a defense lawyer, it is critical that you understand your duties of preservation and policing. You can't think in terms of panaceas, and I think that includes predictive coding.

# Best Practices in the Digital Age

- Forget about chasing every new fad.
- It seems like every month there is a new iteration of digital software or hardware.
- You need to focus on mindset and methodology instead of each new fad.
- In the end, digital is digital; whether we're talking about the clouds, the latest social media or the newest "i-phone" phenomena.

# Plaintiffs' perspective

- Plaintiffs' counsel is always looking for the "magic bullet." They want the gold quick and cheap. E-discovery is neither.
- It is more about methodology than location.
- Smoking guns are not that easy to find.
- Don't fall into "predictive coding" mindset; for plaintiffs' counsel it is about careful review and that requires good management.

# Plaintiffs continued

- Don't confuse comprehensive "shotgun" discovery with solid investigative technique. I will talk about:
  - ❖ The "smell" of discovery deception.
  - ❖ Two step discovery methodology.
  - ❖ Use of the 30(b)(6) deposition.
- Most of all, as a plaintiffs' counsel, don't forget about your own obligations to preserve and policy your clients.

# Defense perspective

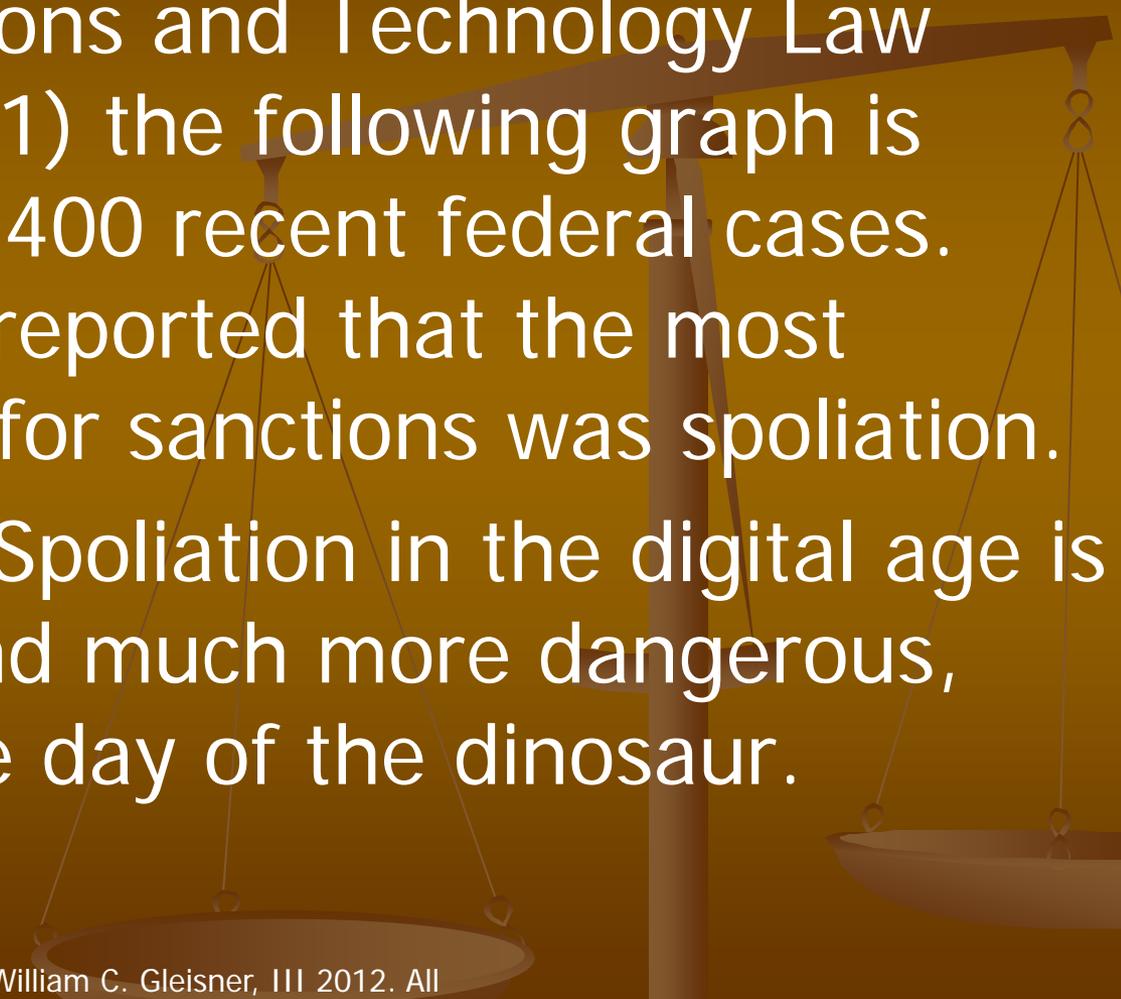
- You need to become a fan of the Sedona Conference and its principles.
- Historically, Defendants and their counsel underestimate the danger of "appearances."
- In the digital age, it's dangerous to be uncooperative or less than candid or appear so.
- Don't confuse preservation with production.
- Don't be blinded by your own "magic bullets" like cost shifting and Predictive coding.

# Defense continued

- **Predictive Coding:** In *Moore v. Publicis Groupe*, 287 FRD 182 (SDNY 2012) the Court concluded that it “would approve use of computer-assisted coding in large-data-volume employment discrimination case, where the parties agreed to its use, although they disagreed about how best to implement such review, there were over 3,000,000 documents that had to be reviewed, computer-assisted review was superior to available alternatives, and computer-assisted review was cost effective and complied with discovery rule's doctrine of proportionality.”
- **Expect Plaintiffs' counsel to resist this approach.**

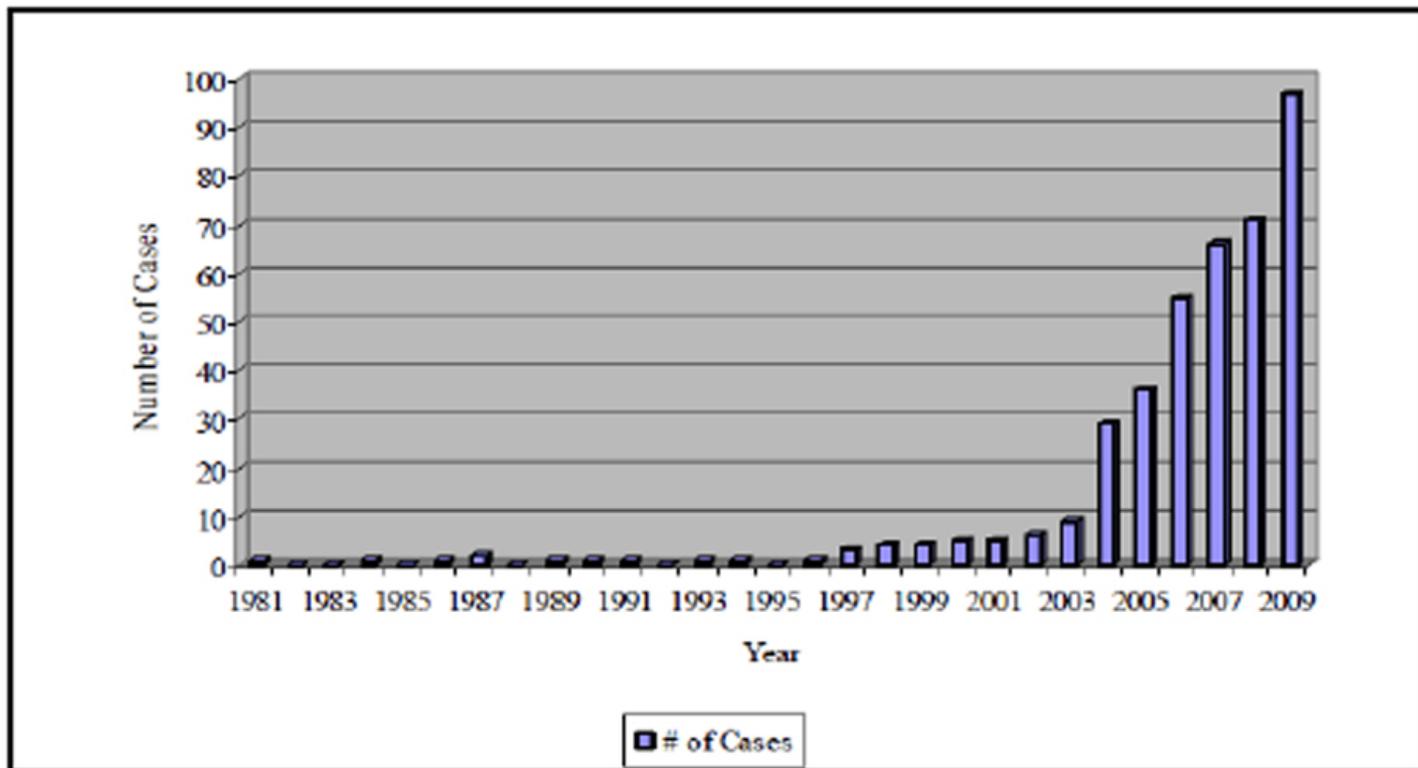
# My Approach Today

- I intend to demonstrate software and techniques that I use in discovering and managing digital evidence. They are by no means the best or the only way to slice the orange. But they work for me.
- And now, let's begin with the end game: How do you present digital evidence in Court? I use Indata's Trial Director.

- 
- According to Professor Adams, 18 Michigan Telecommunications and Technology Law Review 1, 4 (2011) the following graph is from a survey of 400 recent federal cases. This survey also reported that the most frequent ground for sanctions was spoliation.
  - And believe me, Spoliation in the digital age is very different, and much more dangerous, than it was in the day of the dinosaur.

# e-Discovery sanctions are increasing at an Alarming Rate

*Figure 1. Annual Number of E-Discovery Sanction Cases*

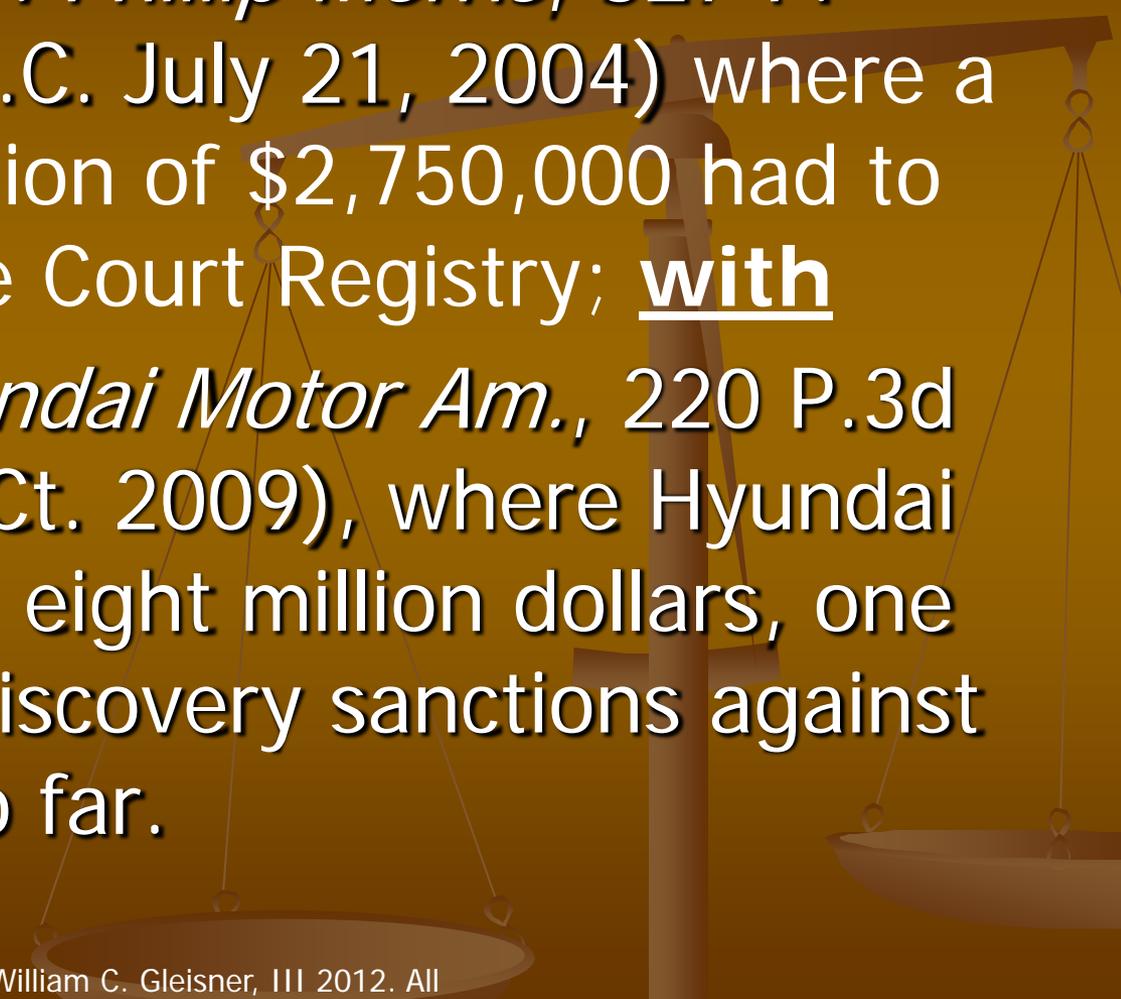


# The Good Old Days...

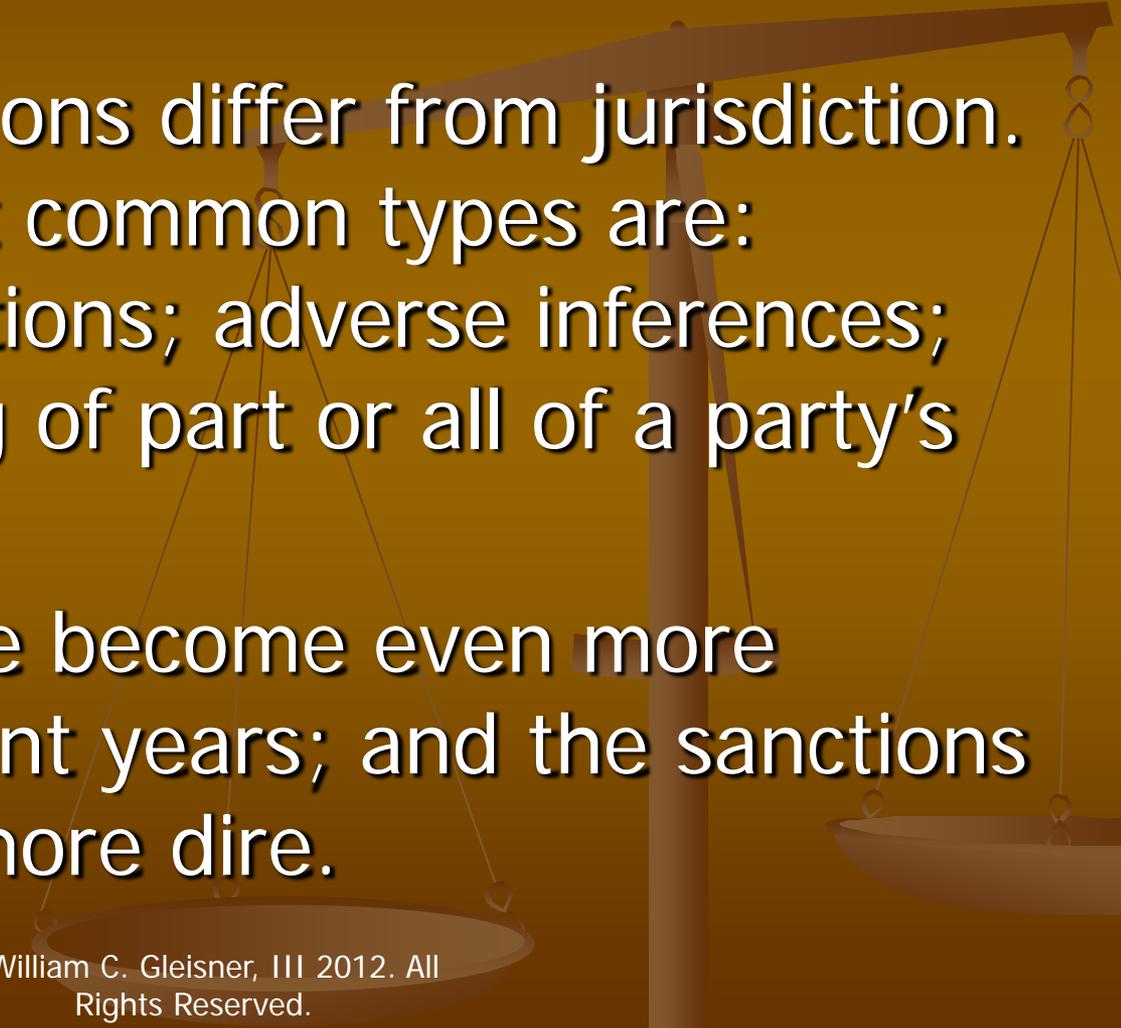
- It used to be that sanctions for spoliation arose mainly out of intentional misconduct or conduct bordering on stupidity.
- *For example, in Sentry Ins. v. Royal Ins. Co., 196 Wis. 2d 907, 918-19, 539 N.W.2d 911 (Ct. App. 1995) spoliation was found where a party's expert intentionally removed components of a refrigerator, thereby precluding testing by an opposing party.*

# The Digital Era has Completely Changed Spoliation

- Spoliation litigation is becoming a blood sport.
- Now, woe be to the litigator or party that does not take steps to properly preserve digital evidence. And “death” to the person who intentionally destroys it.
- But here’s the rub; due to the ephemeral nature of digital evidence irreparable harm can happen in an instant yet destruction of digital evidence is fairly easy to detect.

- 
- Monetary sanctions are increasing:
  - Compare *U.S. v. Phillip Morris*, 327 F. Supp. 2d 21 (D.C. July 21, 2004) where a monetary sanction of \$2,750,000 had to be paid into the Court Registry; with
  - *Magana v. Hyundai Motor Am.*, 220 P.3d 191 (Wash. S. Ct. 2009), where Hyundai was sanctioned eight million dollars, one of the largest discovery sanctions against a company... so far.

# Courts are Leveling Different and more creative sanctions



- Available sanctions differ from jurisdiction. The three most common types are: monetary sanctions; adverse inferences; and the striking of part or all of a party's pleadings.
- But Courts have become even more creative in recent years; and the sanctions have become more dire.

- In *Green v. Blitz U.S.A, Inc.* (E.D. Tex. Mar. 1, 2011), the U.S. District Court for the Eastern District of Texas found the defendant's abuse of the discovery process to be so egregious that it ordered the offending party to provide a copy of the court's highly detailed opinion to every plaintiff in every lawsuit it has had litigation with during the two previous years. Moreover, the court ordered that a copy of its opinion must be filed with the abusing party's *first pleading with the presiding court in every new lawsuit in which it is a party*, whether as a plaintiff, defendant, or any other capacity, *for five years.*

# Next Gen eDiscovery Law & Tech Blog

SKIP TO CONTENT

- HOME
- ABOUT OUR BLOGGERS
- ABOUT X1 DISCOVERY



NOVEMBER 15, 2011 · 9:10 PM

[↓ Jump to Comments](#)

## Facebook Spoliation Costs Lawyer \$522,000; Ends His Legal Career



In what many are calling the largest eDiscovery sanction penalty ever leveled directly against an attorney, a Virginia state judge ordered lawyer Matthew Murray to pay \$522,000 for instructing his client to remove photos from his Facebook profile, and for his client to pay an additional \$180,000 for obeying the instructions. A copy of the final order in *Lester v. Allied Concrete Company* is available [here](#).

FILED  
U.S. DISTRICT COURT  
EASTERN DISTRICT OF LOUISIANA

MAR 20 AM 10:12

MARICETTA G. WHYTE  
CLERK

**FELONY**

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF LOUISIANA

SUPERSEDING INDICTMENT FOR OBSTRUCTION OF JUSTICE

UNITED STATES OF AMERICA	*	CRIMINAL NO. 12-171
v.	*	SECTION: "K" (1)
KURT MIX	*	VIOLATION: 18 U.S.C. § 1512(c)(1)
	*	
	*	*

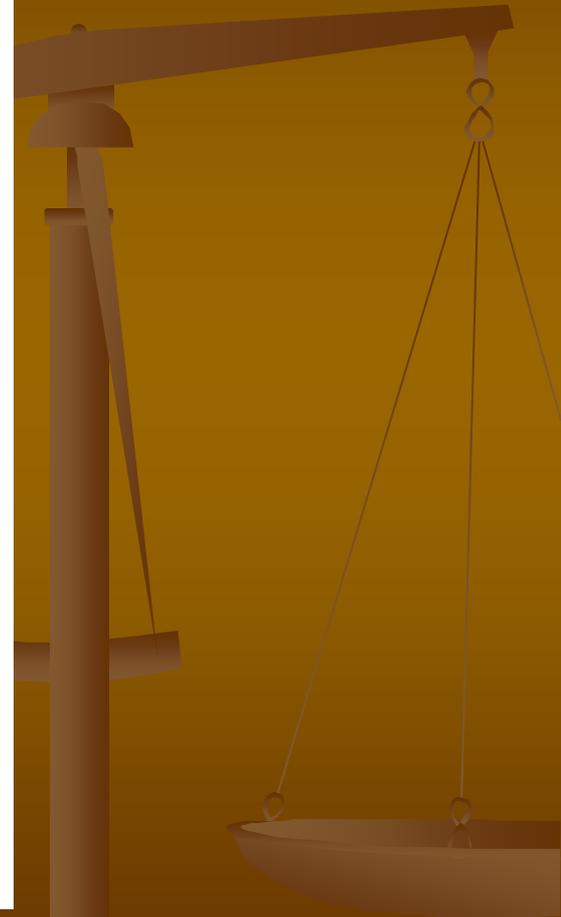
**THE GRAND JURY CHARGES THAT:**

BACKGROUND

At all times relevant to this indictment:

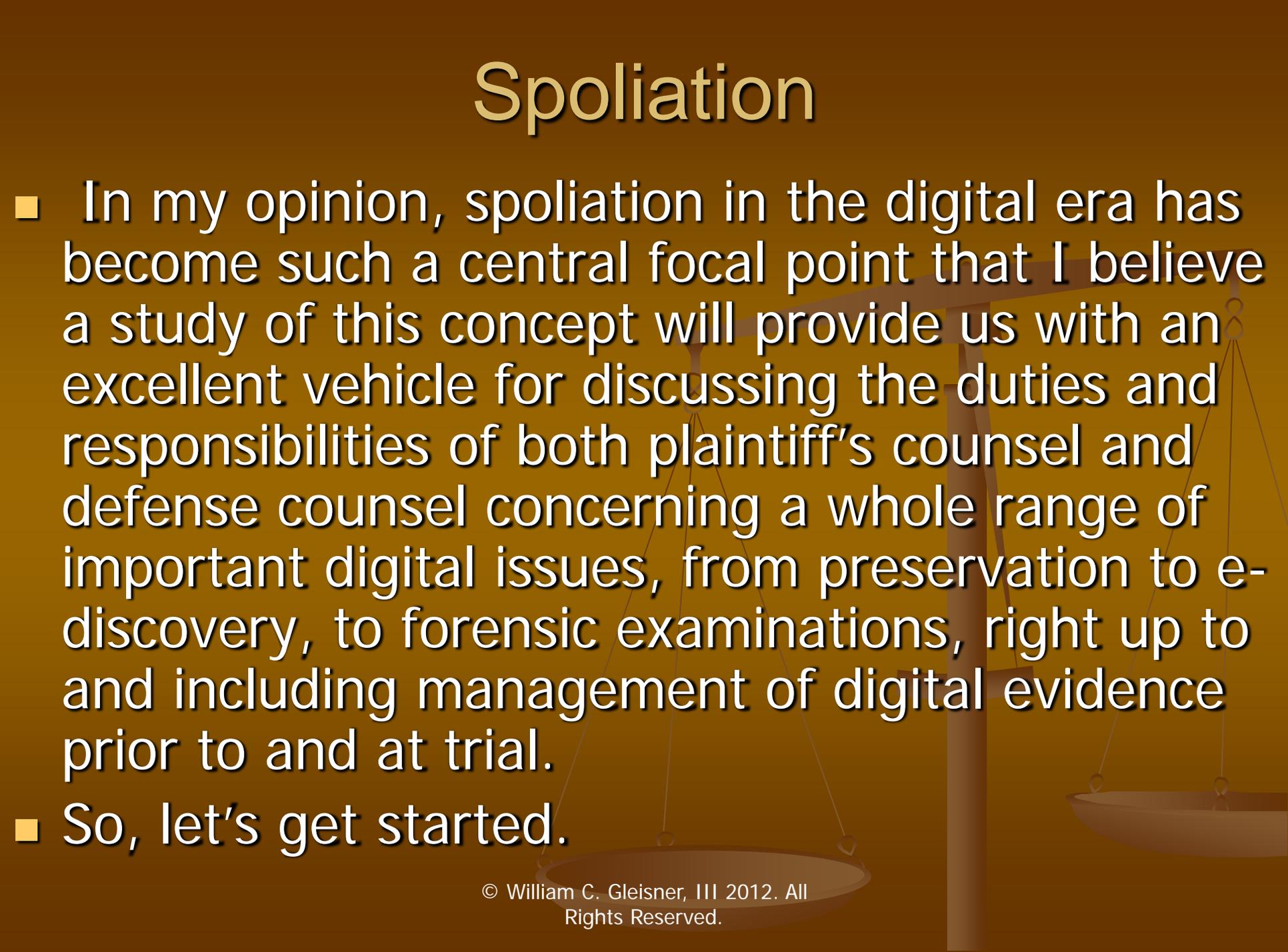
1. Defendant KURT MIX was a Drilling Engineer for BP plc ("BP"), a multinational oil and gas company headquartered in London, England.
2. On or about April 20, 2010, the *Deepwater Horizon* drilling rig, leased by BP, was completing work on the Macondo well in the Gulf of Mexico. That evening, the rig experienced an uncontrolled blowout of gas and oil, which quickly led to two massive explosions resulting in the deaths of eleven men and the largest oil spill in United States history. Oil spilled from the Macondo well for almost three months.
3. Following the Macondo well explosions, Defendant KURT MIX worked on a

by WLN  
 Processed \_\_\_\_\_  
 Filed \_\_\_\_\_  
 Clerk Dep \_\_\_\_\_  
 ED 0048

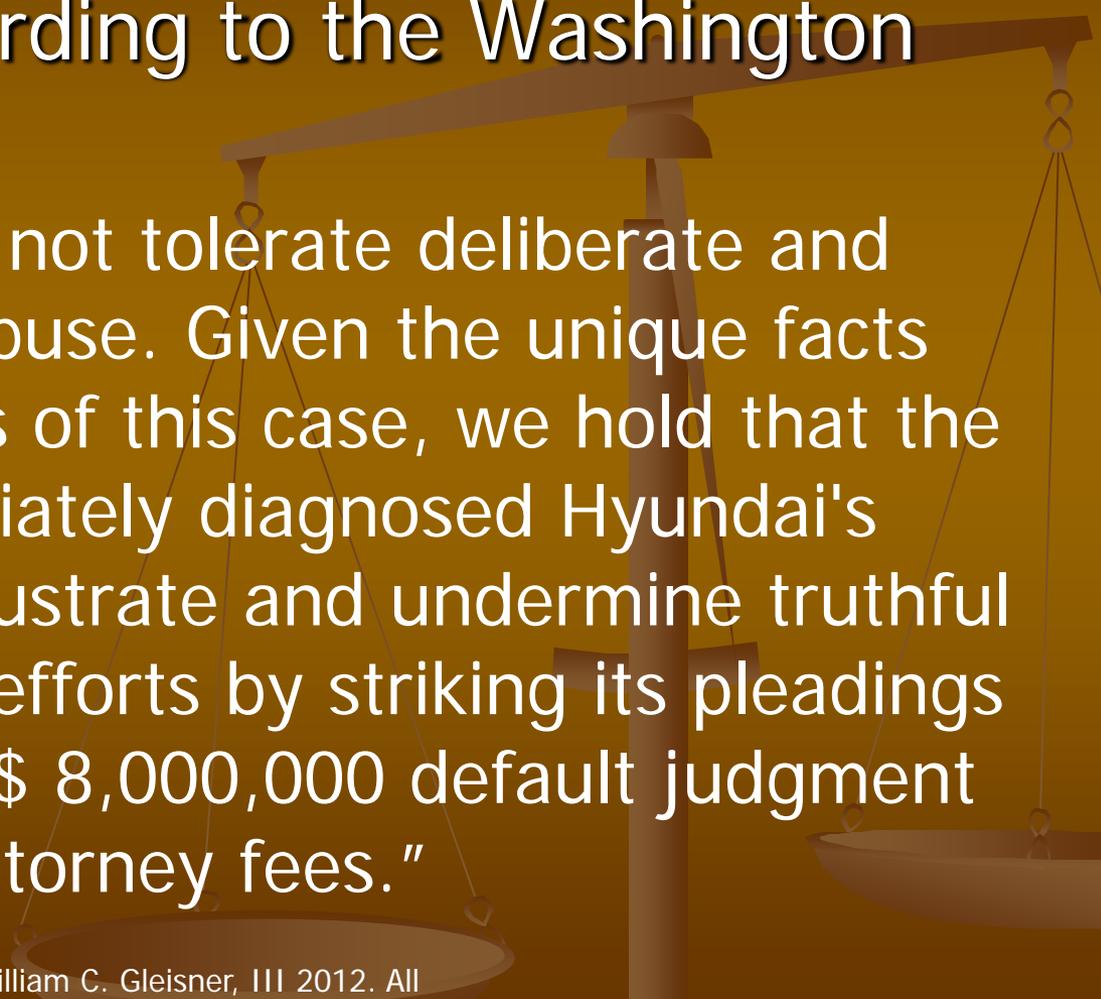


- In some cases, spoliation sanctions appear to have almost taken the form of damage relief. In the case of *SK Hynix v. Rambus*, 2013 WL 1915865 (N.D. Cal. 2013) a Court imposed a sanction of \$250 Million dollars against a party which had otherwise substantially prevailed in patent infringement litigation. The court concluded that the sanction of \$250,000,000 was to be applied as a credit against the prevailing party's judgment...

# Spoliation



- In my opinion, spoliation in the digital era has become such a central focal point that I believe a study of this concept will provide us with an excellent vehicle for discussing the duties and responsibilities of both plaintiff's counsel and defense counsel concerning a whole range of important digital issues, from preservation to e-discovery, to forensic examinations, right up to and including management of digital evidence prior to and at trial.
- So, let's get started.

- 
- A good place to start is to find out just what went wrong in *Magana v. Hyundai Motor Am.* According to the Washington Supreme Court:
  - “Trial courts need not tolerate deliberate and willful discovery abuse. Given the unique facts and circumstances of this case, we hold that the trial court appropriately diagnosed Hyundai's willful efforts to frustrate and undermine truthful pretrial discovery efforts by striking its pleadings and rendering an \$ 8,000,000 default judgment plus reasonable attorney fees.”

- The Hyundai Court found: "A corporation must search all of its departments, not just its legal department, when a party requests information about other claims during discovery... Hyundai had the obligation to diligently respond to Magaña's discovery requests about other similar incidents. It failed to do so by using its legal department as a shield. Hyundai had the obligation to diligently and in good faith respond to discovery efforts, [and] maintain a document retrieval system that would enable the corporation to respond to plaintiff's requests."

- Acknowledging that discovery sanctions should be proportional, the Hyundai Court stated: “In addressing whether a monetary fine would suffice, the trial court found it would be difficult to know what amount would be suitable since ‘Hyundai is a multi-billion dollar corporation.’ It also found a monetary sanction would not address the prejudice to Magaña or to the judicial system. ... The trial court also denied a continuance, which Hyundai had proposed. The trial court held that sanctions for discovery violations should not reward the party who has committed the violations and that granting a continuance would only exacerbate the situation.”

- According to the head of King & Spaulding's Discovery Center, writing at 60 Duke L.J. 789 (2010): "For the most serious violations, courts have imposed the most draconian of sanctions: dismissal of all claims or defenses. ... In cases of lesser violations, courts have used a continuum of penalties... Such penalties have included evidence preclusion, witness preclusion, disallowance of certain defenses, reduced burden of proof, removal of jury challenges, limiting closing statements, supplemental discovery, and additional access to computer systems. In some instances, more creative courts have imposed nontraditional sanctions, such as payments to bar associations [for] educational programs..."

# FAILING TO PROPERLY PRESERVE IS A GIFT TO DISCOVERING COUNSEL

- According to the Court in *Danis v. USN Communications, Inc.*, 2000 WL 1694325 (N.D. Ill. 2000):  
"The Court's authority to sanction a party for the failure to preserve and/or produce documents is both inherent and statutory. ... **The duty to preserve documents in the face of pending litigation is not a passive obligation. Rather, it must be discharged actively.**... The obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers. .... The scope of the duty to preserve is a broad one, commensurate with the breadth of discovery permissible under Fed.R.Civ.P. 26. ... '[A] litigant 'is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, ... Moreover, the case law establishes that a discovery request is not necessary to trigger this duty."

# THE GAMES CORPORATIONS PLAY AND HOW THEY BACKFIRE.

- In *Cliff v. DaimlerChrysler*, Case No. 3:01-cv-186 (ED Tenn. 2002), I obtained the following order on April 11, 2002:  
“... [Defendant] is ORDERED to produce the following by Wednesday, April 24, 2002: legible and properly scanned documents to replace the illegible ones previously provided on the CDs; [and] the 5,000 graphical images claimed to be undecipherable by plaintiffs; ... Within the relevant time frame, defendant is also ORDERED to allow plaintiffs access to any available searchable databases that may contain relevant discovery material. Plaintiffs shall have unrestricted right to use and examine the databases subject to the protective order currently in place in this case. [Defendant] must also provide information as to how documents are organized on [defendant’s] main database and further explain the [unindexed] information divulged on the CDs.”

- In *MSF Holding, Ltd. v. Fiduciary Trust Co. International*, 2005 U.S. Dist. Lexis 34171 (S.D. NY December 7, 2005) the court placed limitations on claims of attorney client privilege with respect to email from corporate in-house counsel. The court concluded: "...[T]he e-mails at issue here reflect the exercise of a predominantly commercial function. Susan Garcia, the author of the communications and FTCI's Senior Vice President and Deputy Corporate Counsel, never alluded to a legal principle in the documents nor engaged in legal analysis."

- In *Metropolitan Opera Ass'n v. Local 100, Hotel Employees*, 212 FRD 178 (SDNY 2003), the Court severely sanctioned defense counsel because: "(1) [Counsel] never gave adequate instructions to their clients about the clients' overall discovery obligations, ... [and] (3) delegated document production to a layperson who ... did not even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; ..." *Id.* at 222.

- In the case of *In re Old Banc One Shareholders Securities Litigation*, 2005 U.S. Dist. Lexis 32154 (N.D. Ill. December 8, 2005), which addresses a party's obligation to prepare and disseminate a retention policy for digital records, the Court observed: **"In order to meet its obligations, Bank One needed to create a comprehensive document retention policy to ensure that relevant documents were retained and needed to disseminate that policy to its employees...."** *Id.* at \*11-12.

# How to “smell” the existence of missing data.

- You don't always need the services of a forensic computer expert to “smell” missing data (although such an expert is essential to prove missing data). See *Telxon v. PricewaterhouseCooper*, 2004 WL 3192729 (N.D. Ohio July 16, 2004) which involved failures to disclose digital evidence, and the methods used by the plaintiffs' counsel to prove its existence.

According to the plaintiffs in *Telxon* :

- 1) Because "PwC ... **produced hardcopy documents in a version different from any version of the documents in electronic form**, the conclusion is inescapable that PwC has not yet made available to Telxon and plaintiffs all of its electronic databases relevant to this action."
- 2) **"[T]he absence of electronic versions** of internal audit workpapers, and the absence of the electronic version of the 1998 workpapers **from which the hard copies were produced** raises questions as to whether PwC is still withholding discoverable material." at \*23.

The *Telxon* plaintiffs showed prejudice in the following manner:

- **“[T]he failure to note all modifications and all persons modifying documents on the hard copies produced during discovery caused Telxon and plaintiffs to choose not to depose certain persons or not to ask certain questions of the people whom they did depose.”** at \*22.
- 4) **“[T]he failure to produce documents in the order in which they were kept and the failure to produce all indices allowing the sorting of produced documents according to topic of interest slowed Telxon's and plaintiffs' discovery of relevant information and increased the cost of discovery.”** at \*23.

The Magistrate in *Telxon* concluded:

- “PwC failed at the start of discovery to check thoroughly its local servers and its archives for relevant documents, failed to compare the various versions of relevant documents on those databases, failed to produce documents as they were kept in the ordinary course of business, and failed to reproduce thoroughly and accurately all documents and their attachments. Prior to litigation PwC had permitted destruction of documents despite committing to their preservation.” at \*33.

# MORE GAMES

- Then there is the decision in *U.S. v. Phillip Morris*, Civil Action 327 F. Supp. 2d 21 (D.C. July 21, 2004), where the Court held:

“A monetary sanction is appropriate. It is particularly appropriate here because *we have no way of knowing what, if any, value those destroyed emails had to Plaintiff's case;* because of that absence of knowledge, it was impossible to fashion a proportional evidentiary sanction that would accurately target the discovery violation. Consequently, Philip Morris and Altria Group will be jointly required to pay a monetary sanction of \$2,750,000 into the Court Registry ...”

# ON THE OTHER HAND...

## *The Issue of Cost Shifting*

- Cost shifting is the new method by which defense counsel attempt to avoid the strictures of electronic discovery. Cost shifting has even been requested from plaintiffs seeking documents from a non-party. *See e.g. In re Automotive Paint Antitrust Litigation*, 229 FRD 482 (E.D. Penn. 2005), where the Court stated: "...

"nonparty witnesses are powerless to control the scope of litigation and discovery, and should not be forced to subsidize an unreasonable share of the costs of a litigation to which they are not a party." /

*Id.* at 496.

## ■ ZUBULAKE and COST SHIFTING

- Which brings us to the most important series of cases to date, known as the *Zubulake* collection. In *Zubulake I*, 217 FRD 309, 322 (SD NY May 13, 2003) the Court announced what has come to be known as the touchstone for cost sharing in electronic discovery proceedings. The Court identified seven factors:

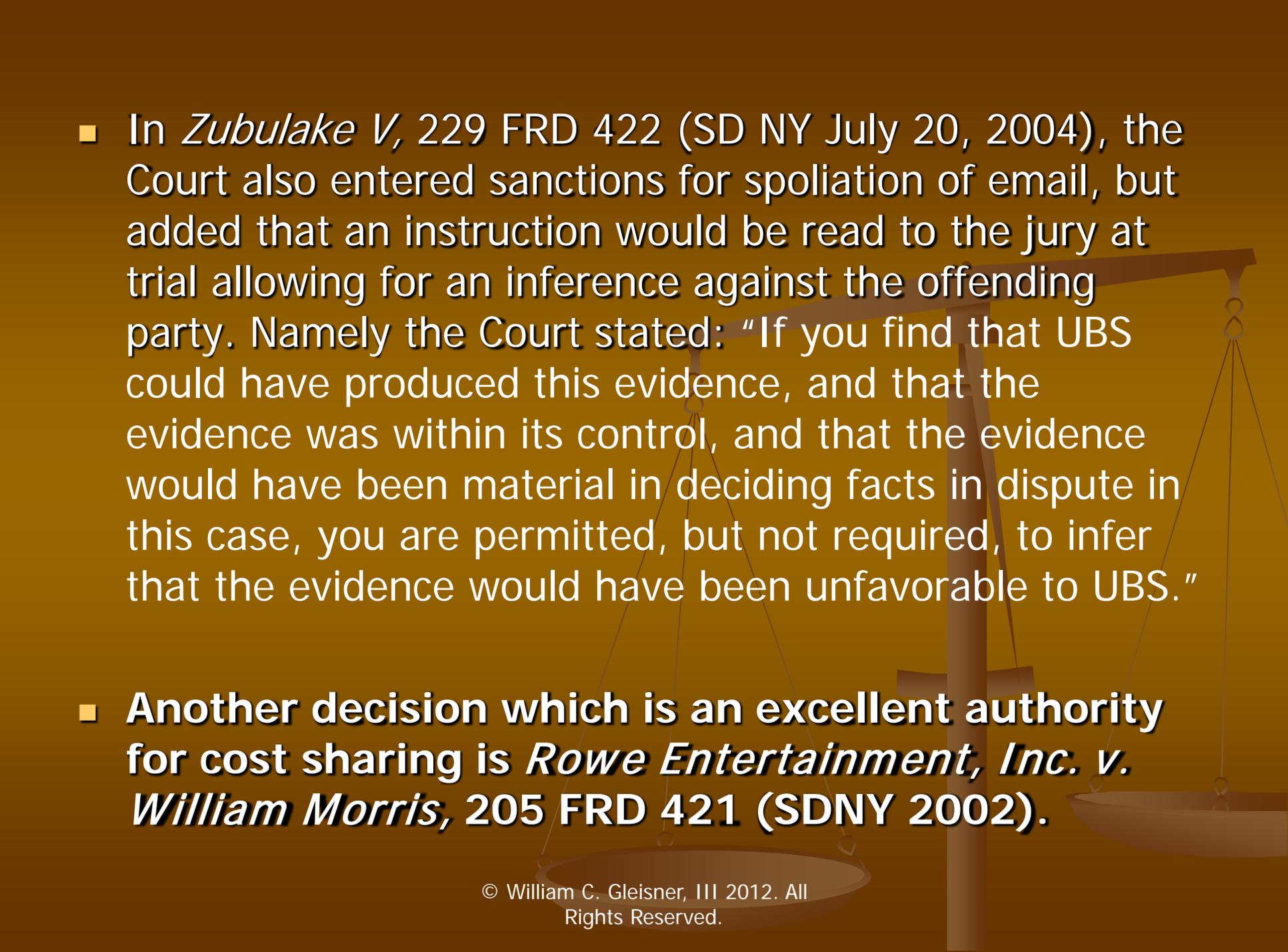
1. **The extent to which the request is specifically tailored to discover relevant information;**
2. **The availability of such information from other sources;**
3. **The total cost of production, compared to the amount in controversy;**
4. **The total cost of production, compared to the resources available to each party;**
5. **The relative ability of each party to control costs and its incentive to do so;**
6. **The importance of the issues at stake in the litigation; and**
7. **The relative benefits to the parties of obtaining the information.**

# Other pronouncements in the *Zubulake* litigation

- In *Zubulake IV*, 220 FRD 212, 218 (SDNY October 22, 2003) [1] the Court noted:

"The scope of a party's preservation obligation [of digital evidence] can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention [or] destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold."

[1] There is also a *Zubulake II*, 2003 WL 21087136 and a *Zubulake III*, 216 FRD 280.

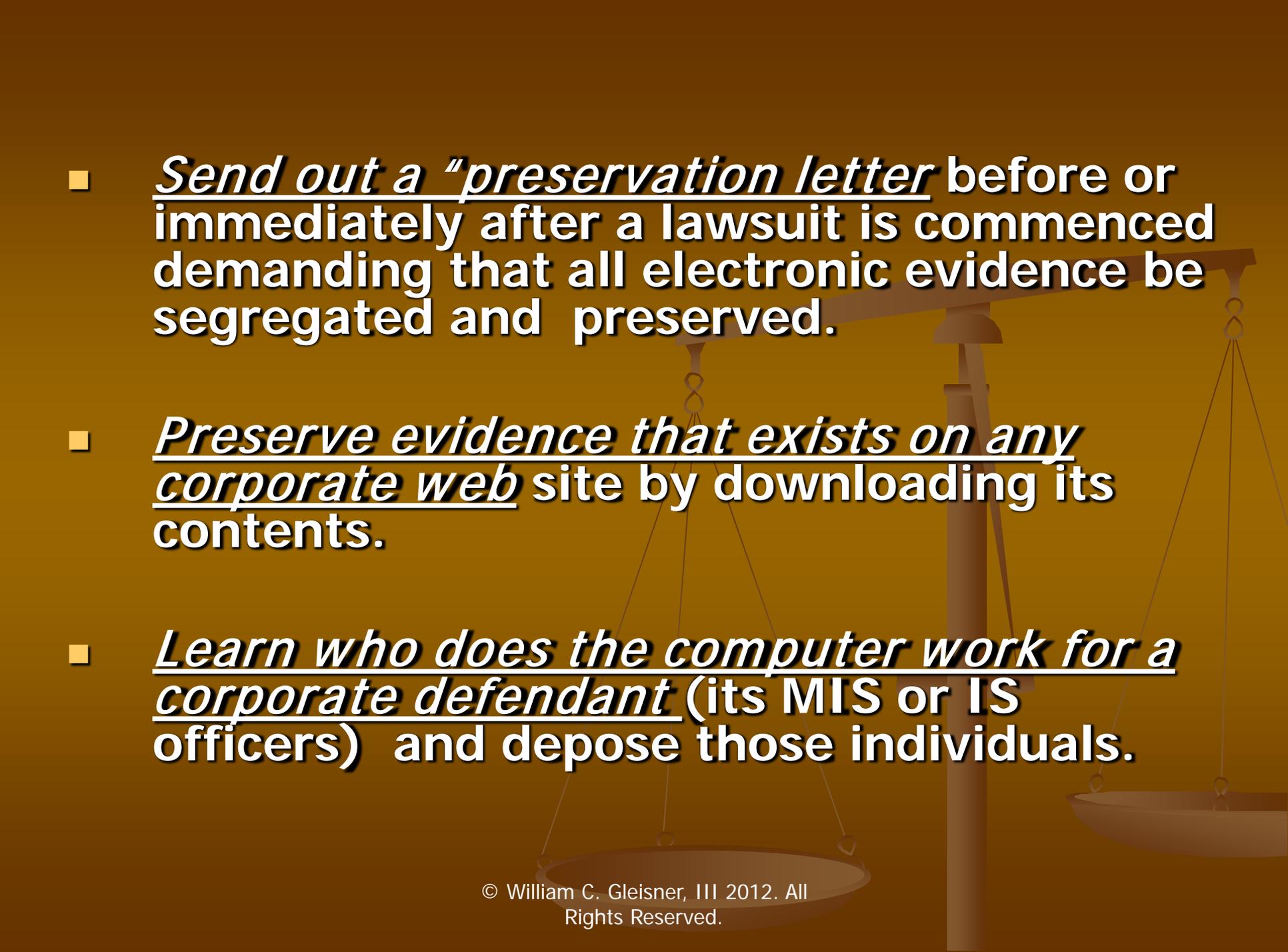
- 
- In *Zubulake V*, 229 FRD 422 (SD NY July 20, 2004), the Court also entered sanctions for spoliation of email, but added that an instruction would be read to the jury at trial allowing for an inference against the offending party. Namely the Court stated: "If you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS."
  - **Another decision which is an excellent authority for cost sharing is *Rowe Entertainment, Inc. v. William Morris*, 205 FRD 421 (SDNY 2002).**

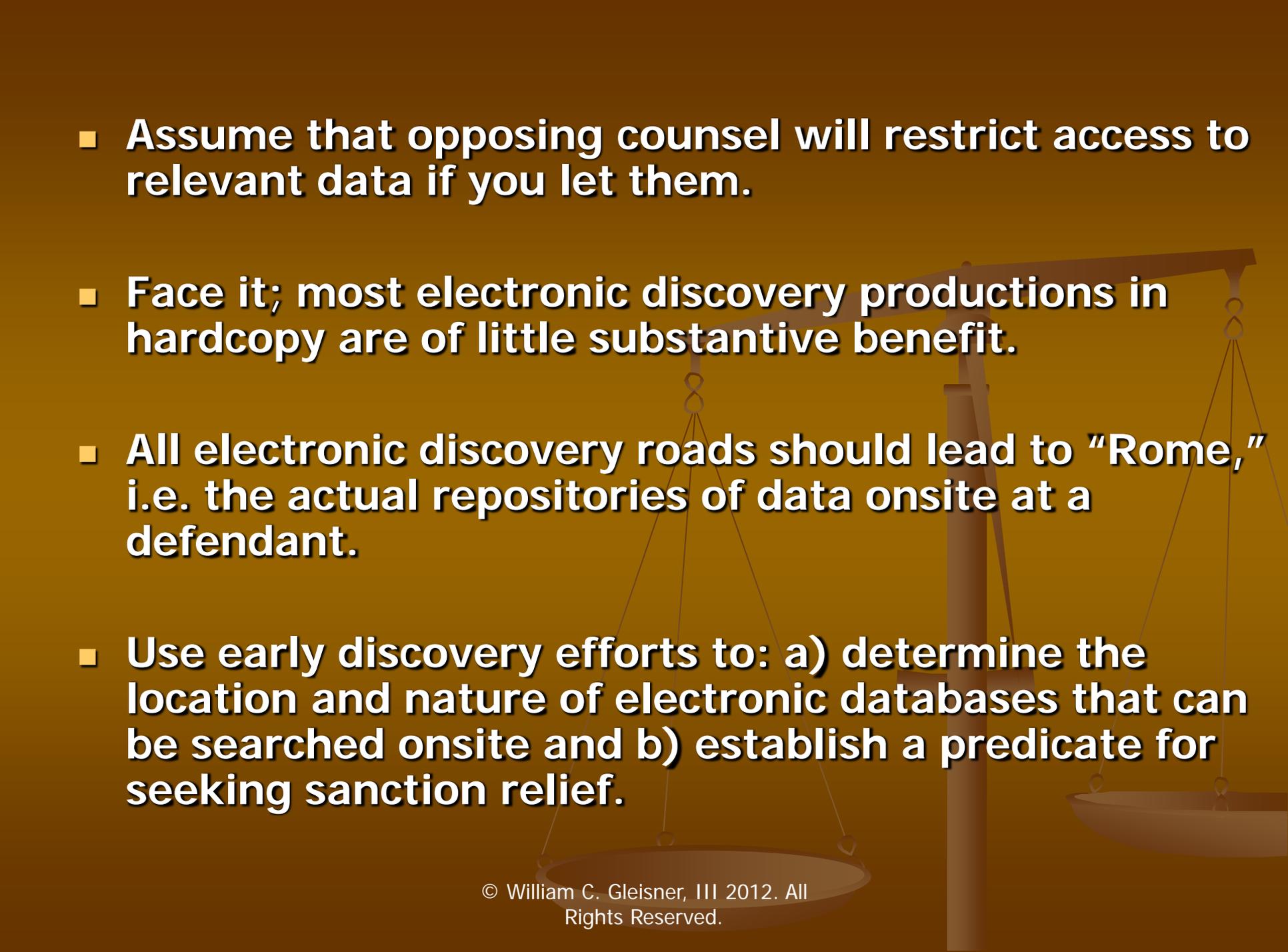
# CONDUCTING E-DISCOVERY

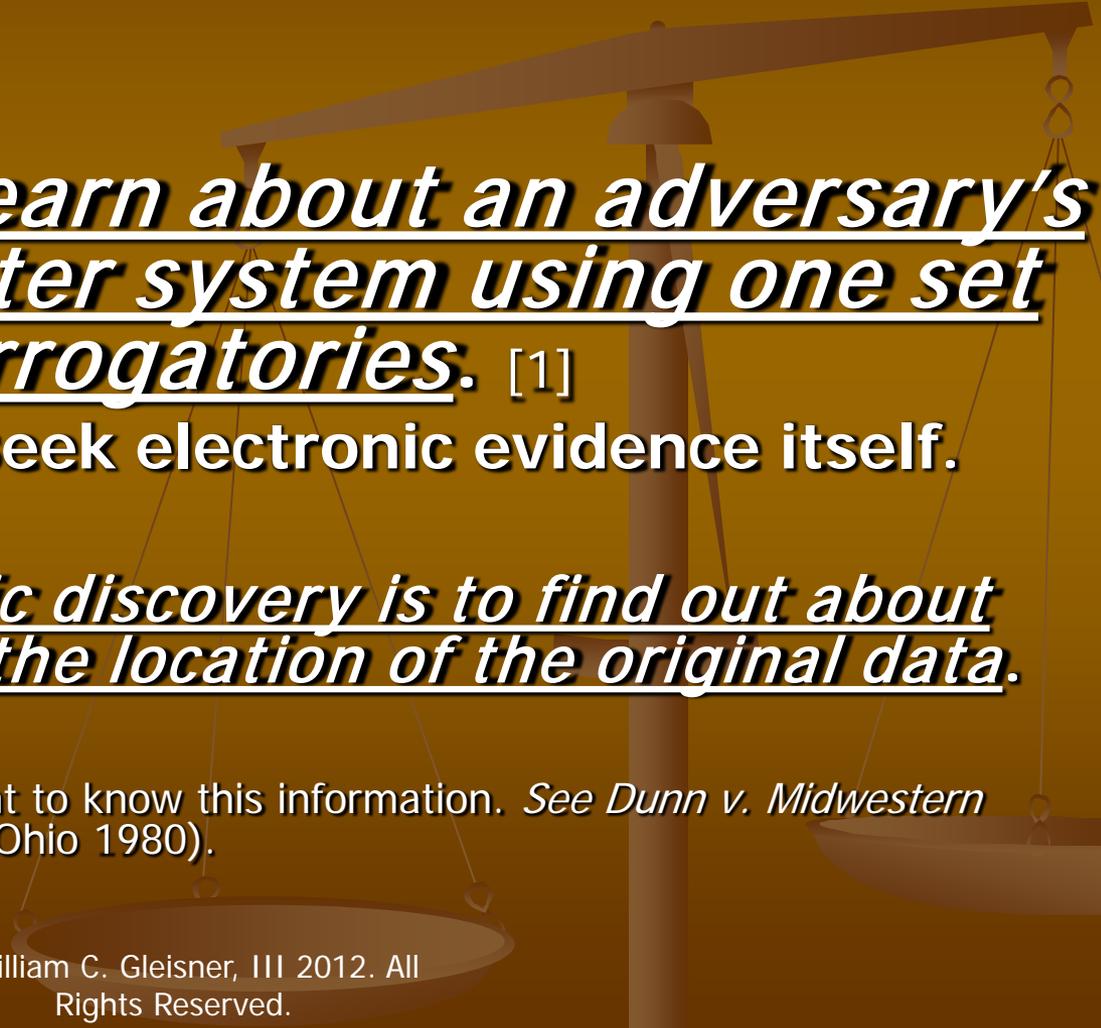
- There are many ways to conduct e-discovery, but they all begin with a very competent forensic consultant. I have used a variety of consultants, but for a number of reasons I prefer Digital Intelligence, <http://www.digitalintelligence.com>. Matt Stippich is a lawyer and techie. They are local but are nationally recognized for the forensic skills, software & hardware.

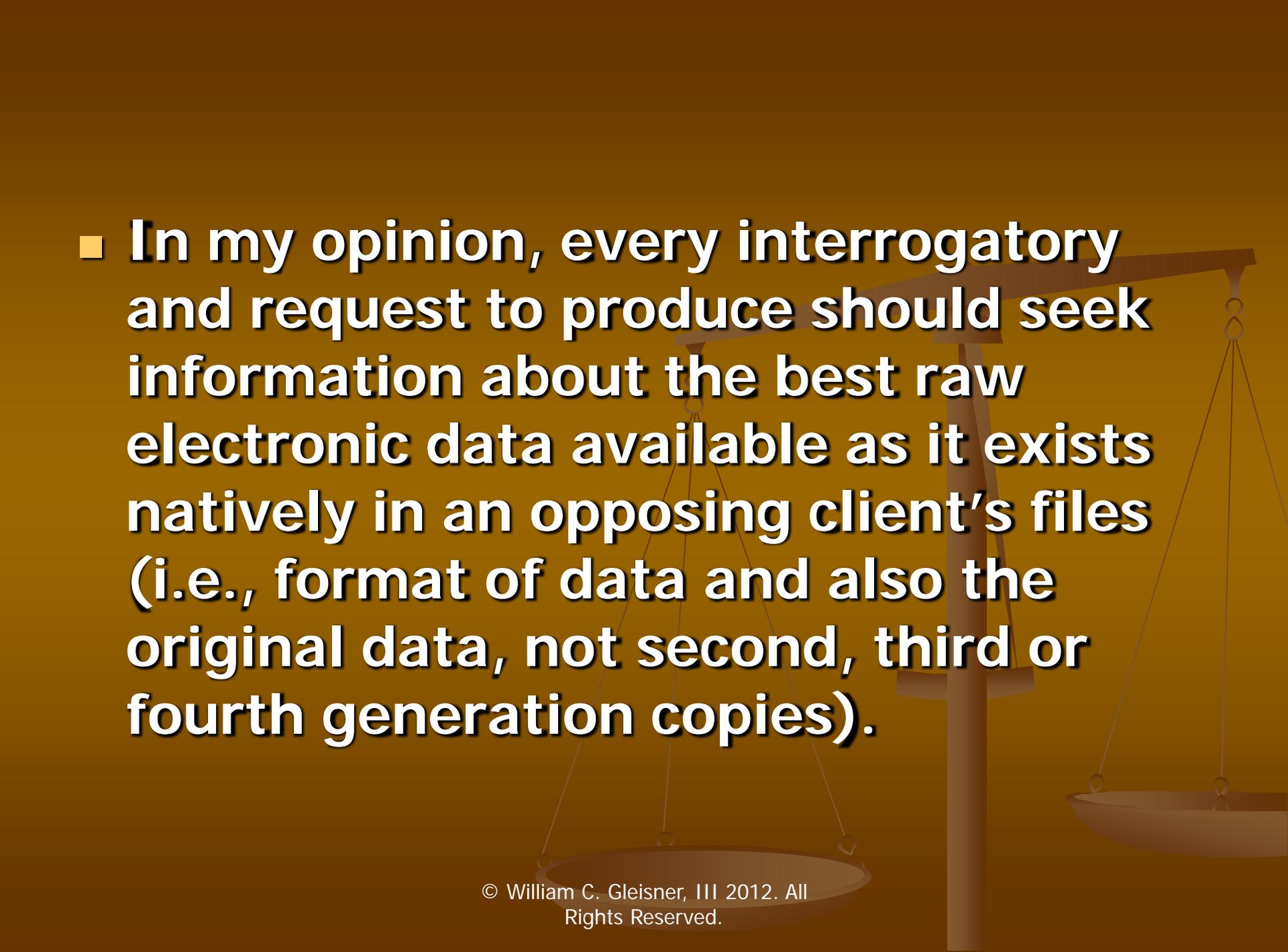
# *Some Discovery Practice Tips*

- There are two main types of corporate electronic databases:[1]
- 1. Databases containing actual electronic copies, or images, of data, which consist of:
  - Keyed in info about data tied to scanned copies; and
  - The management software which indexes and controls access to that data.
- 2. Databases containing an index to data stored elsewhere as hardcopy, microfiche, etc.
  - [1] An excellent case discussing database technology is *NAACP v. Acusport Corp.*, 210 F.R.D. 268, 278-282 (ED NY 2002).

- 
- **Send out a "preservation letter" before or immediately after a lawsuit is commenced demanding that all electronic evidence be segregated and preserved.**
  - **Preserve evidence that exists on any corporate web site by downloading its contents.**
  - **Learn who does the computer work for a corporate defendant (its MIS or IS officers) and depose those individuals.**

- 
- Assume that opposing counsel will restrict access to relevant data if you let them.
  - Face it; most electronic discovery productions in hardcopy are of little substantive benefit.
  - All electronic discovery roads should lead to "Rome," i.e. the actual repositories of data onsite at a defendant.
  - Use early discovery efforts to: a) determine the location and nature of electronic databases that can be searched onsite and b) establish a predicate for seeking sanction relief.

- 
- *Interrogatories seeking electronic evidence should take place in two phases.*
    - *First, learn about an adversary's computer system using one set of interrogatories.* [1]
    - Second, seek electronic evidence itself.
  - *The goal of electronic discovery is to find out about an item of data and the location of the original data.*
  - [1] A discovering party has the right to know this information. *See Dunn v. Midwestern Indemnity*, 88 FRD 191, 194 (S.D. Ohio 1980).

- 
- **In my opinion, every interrogatory and request to produce should seek information about the best raw electronic data available as it exists natively in an opposing client's files (i.e., format of data and also the original data, not second, third or fourth generation copies).**

**Serve a first set of discovery seeking just information about an adversary's computer system.**

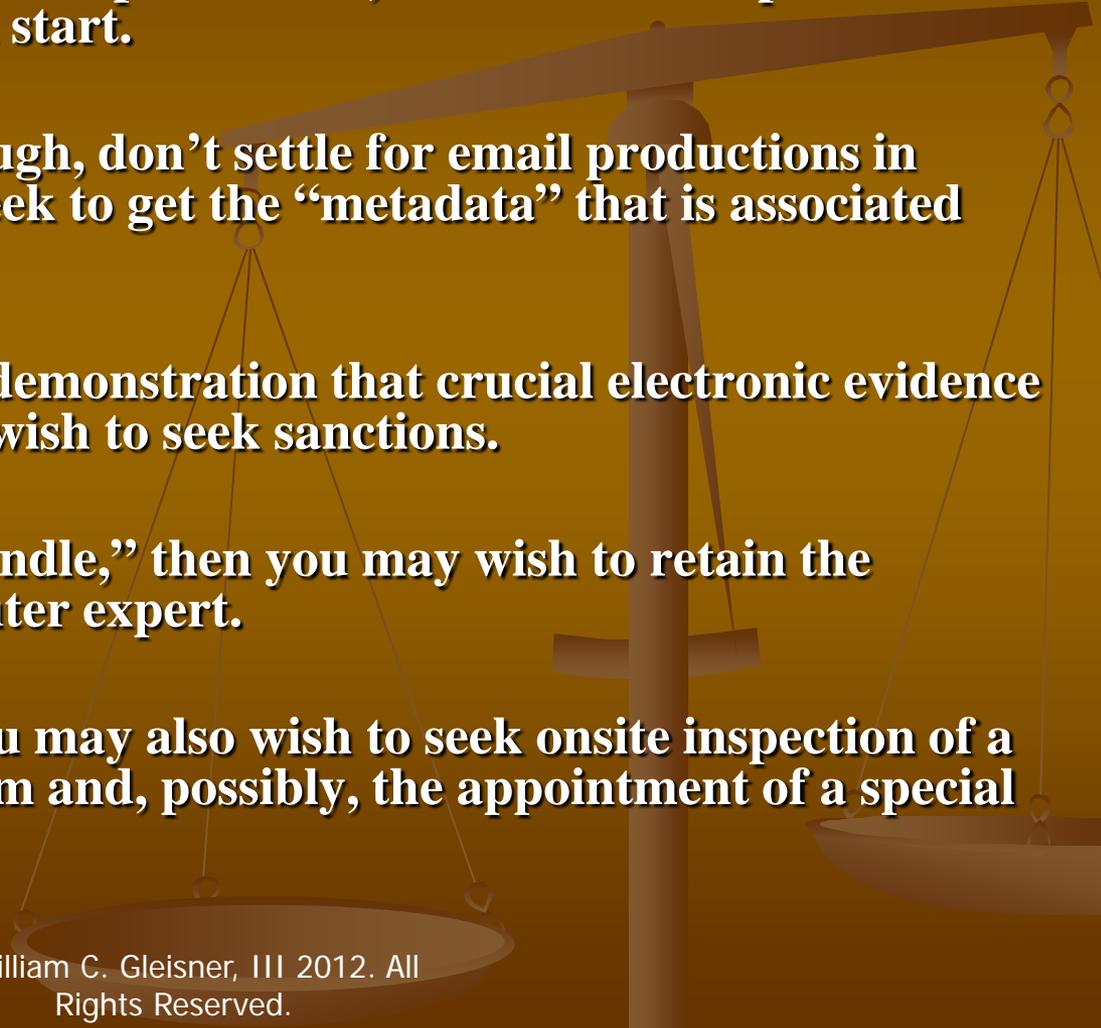
- **At this stage, what electronic or hardcopy data an opposing party possesses is unimportant.**
- **Where is the electronic data actually located?**
- **In what format or formats does it exist, or has it existed?**
- **What are the retention policies, the backup policies and the server, network and authorization protocols regarding the data?**
- **Regarding electronic data, are copies contained in a searchable database, or just referenced in a searchable database?**
- **What is the configuration of the database where the data is housed, how is it normally searched and by whom?**
- **Ask for copies of operation manuals and names of operators and those authorized to access the database?**
-

# FRCP 30(b)(6)

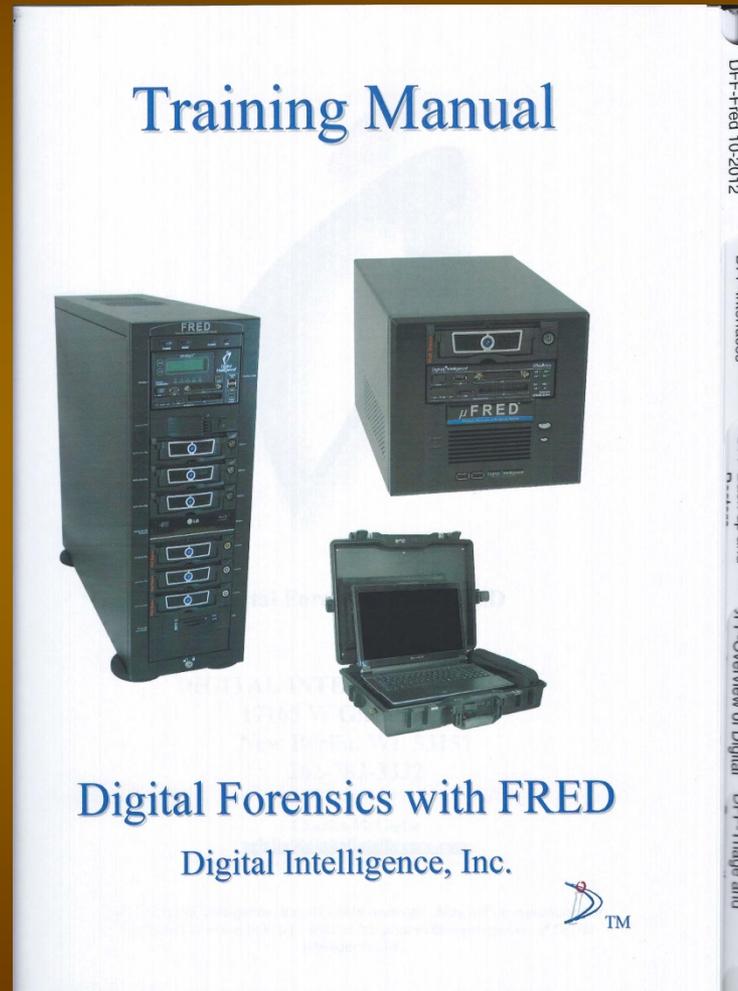
- *(6) Notice or Subpoena Directed to an Organization.* In its notice or subpoena, a party may name as the deponent a public or private corporation, a partnership, an association, a governmental agency, or other entity and must describe with reasonable particularity the matters for examination. The named organization must then designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on its behalf; and it may set out the matters on which each person designated will testify. A subpoena must advise a nonparty organization of its duty to make this designation. The persons designated must testify about information known or reasonably available to the organization. This paragraph (6) does not preclude a deposition by any other procedure allowed by these rules.

## THEN SERVE A SECOND SET OF INTERROGATORIES SEEKING SUBSTANTIVE EVIDENCE

- **Serve a second set of interrogatories that seeks disclosure of facts and evidence, and include in that set a separate section that specifically seeks disclosure of relevant electronic evidence.**
- **When you seek electronic discovery, ask that any evidence that exists in electronic format be provided to you just as it exists in the computer systems of the defendant (be sure to get proprietary software and users' manuals!).**
- **This may occasion a number of battles, relating to format, metadata, convenience and cost. However, in the best of all worlds you want evidence that exists electronically to be provided in the native electronic format if at all possible.**

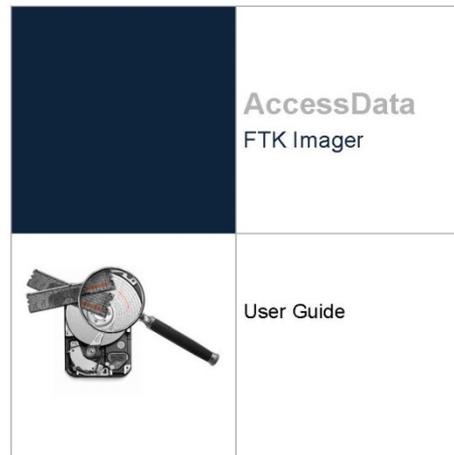
- 
- **You should review all evidence received, in hardcopy or in electronic format, quickly.**
  - **While you should request native production, evidence that is provided in .pdf or .tiff format is a good start.**
  - **If the case is important enough, don't settle for email productions in hardcopy or .pdf format. Seek to get the "metadata" that is associated with email productions.**
  - **If you can make a credible demonstration that crucial electronic evidence is being withheld, you may wish to seek sanctions.**
  - **If "the game is worth the candle," then you may wish to retain the services of a forensic computer expert.**
  - **If the case is big enough, you may also wish to seek onsite inspection of a defendant's computer system and, possibly, the appointment of a special master.**

# Get your Forensic Expert involved



© William C. Gleisner, III 2012. All Rights Reserved.

# AccessData's FTK Imager



## Chapter 3 Working With Evidence

Use FTK Imager to preview evidence prior to creating the image file(s). You can then choose to image the entire evidence object, or choose specific items to add to a Custom Content (AD1) image. This chapter discusses working with evidence and using FTK Imager to accomplish the creation of forensic images that meet your exact needs.

### Previewing Evidence

Evidence items can be previewed prior to deciding what should be included in an image. Beginning with FTK Imager 3.0 support is included for VXFS, exFAT, and Ext4 file systems.

**WARNING:** If the machine running FTK Imager has an active Internet connection and you are using Imager to preview HTML content from the systems cache, there is a potential risk associated with Microsoft Security Bulletin MS-09-054. AccessData recommends that, wherever possible, users not have an active internet connection while Imager is running.

### Preview Modes

FTK Imager offers three modes for previewing electronic data: **Automatic mode**, **Text mode**, and **Hex mode**. These modes are selectable from the Mode menu, or from the *Toolbar*, as introduced in Chapter 2. Each is described in more detail here.

#### Automatic Mode

Automatic mode automatically chooses the best method for previewing a file's contents, according to the file type. For example:

- Web pages, Web-related graphics (JPEGs and GIFs), and any other media types for which Internet Explorer plug-ins have been installed are displayed by an embedded version of Internet Explorer in the Viewer.
- Text files are displayed in the Viewer as ASCII or Unicode characters.
- File types that cannot be viewed in Internet Explorer are displayed outside of FTK Imager in their native application provided those applications are installed locally, and the appropriate file associations have been configured in Windows.
- File types that cannot be viewed in Internet Explorer and that do not have a known native viewer are displayed by default in Hexadecimal Mode in the Viewer.

#### Text Mode

Text mode allows you to preview a file's contents as ASCII or Unicode characters, even if the file is not a text file. This mode can be useful for viewing text and binary data that is not visible when a file is viewed in its native application.

# AccessData's Summation

- You can use the program for real time feeds of a deposition in progress.
- You can load a large number of transcripts into the program and conduct sophisticated Boolean searches of those transcripts.
- You can load evidence into the program and then create hyperlinks the transcript so that you can call up a referenced exhibit.
- You can conduct Boolean searches across evidence and transcripts.
- You can link up transcripts and videotapes of transcripts.
- There are strong redaction tools and "production set" tools (including bate stamp tools) that will enable you to prepare appropriate discovery productions.
- You can view many "e-doc" productions without having to acquire the native software (thus expediting document review).
- With Summation, you can upload case material into secure cloud locations to share with co-counsel or experts.
- **Let's have a look at Summation.**

- One court has required a producing party to design a computer program to extract data from its computerized business records.<sup>[1]</sup> Even deleted computer files are discoverable, if they can be restored without unreasonable expense.<sup>[2]</sup> If a court can be convinced that computer files may be destroyed or lost, it may well enter a preservation order, allow for onsite inspection of a computer system or require the imaging of computer hard drives.<sup>[3]</sup> All types of digital files are discoverable, including voice mails, web sites, web pages, <sup>[4]</sup> blogs and instant messages.

<sup>[1]</sup> *Anti-Monopoly, Inc. v. Hasbro*, 1995 US Dist. Lexis 16355 (SDNY 1995). Of course, this type of ruling today ought to prompt defense counsel to seek to compel cost shifting to the requesting party. : *Zubulake v. UBS Warburg*, 217 FRD 309, 318-322 (SDNY May 13, 2003); *Medtronic Sofamor Danek, Inc. v. Michelson*, 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. 2003); *Byers v. Illinois State Police*, 2000 US Dist. Lexis 9861 at \*35-37 (ND Ill. 2002); and *Rowe Enter v. William Morris Agency*, 2002 US Dist. Lexis 8303 at \*23 (SD NY 2002)

<sup>[2]</sup> *Simon Property Group v. mySimon, Inc.*, 194 FRD 639 (SD Ind. 2000).

<sup>[3]</sup> *Gates Rubber Co. v. Bando Chemical*, 167 FRD 90, 112 (D. Colo. 1996).

<sup>[3]</sup> *Kleiner v. Burns*, 2000 WL 1909470 (D. Kan. 2000).

# Ever hear of Mr. Peabody, Sherman & the Wayback Machine?



# WAYBACK MACHINE

- I will demonstrate the Wayback Machine (Wayback: <http://archive.org>).
- . But before I do, you should know that web and digital archiving is a trend and it is rapidly becoming international. Even if you get your web pages removed from Wayback, maybe I can track you down using a version of Wayback at the new Library of Alexandria... that's in Egypt!

# HOW I HAVE USED THE WAYBACK MACHINE

- In fact, I used it against a large Corporation in a lawsuit in 2002.
- I also recently used it against a New York law firm which was being sued for malpractice.
- And as an "of counsel" consultant (e.g., as a Summation Trainer).

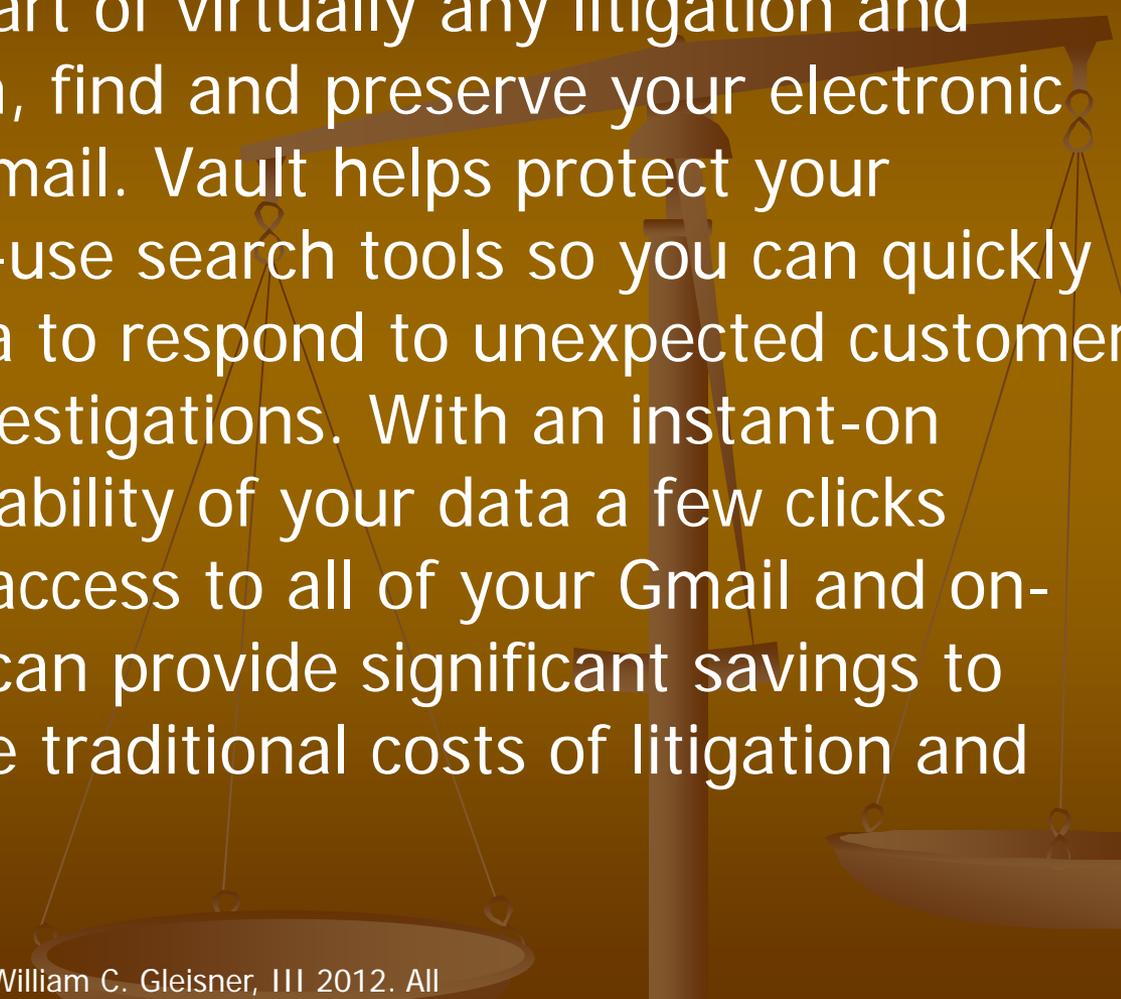
# OTHER WEB RESOURCES

- Legal Tech Directory:
- <http://legaltechdirectory.com>
- Law Technology News:
- <http://www.law.com/jsp/lawtechnologynews/index.jsp>.
- Summation:
- <http://accessdata.com/products/ediscovery-litigation-support/summation>

# MORE WEB RESOURCES

- Case Vault
- <http://crp.casevault.com>
- Trial Director:
- <http://www.indatacorp.com/TrialDirector.html>
- Google Apps Vault:
- <http://googleenterprise.blogspot.com/2012/03/google-apps-vault-brings-information.html>

# GOOGLE APPS VAULT



- “E-discovery can be part of virtually any litigation and requires you to search, find and preserve your electronic information such as email. Vault helps protect your business with easy-to-use search tools so you can quickly find and preserve data to respond to unexpected customer claims, lawsuits or investigations. With an instant-on functionality and availability of your data a few clicks away, Vault provides access to all of your Gmail and on-the-record chats and can provide significant savings to your business over the traditional costs of litigation and eDiscovery.”

# Metadata

- *"It's the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate. Metadata sheds light on the context, authenticity, reliability and dissemination of electronic evidence, as well as providing clues to human behavior. Metadata can be found in many locations. Some is crucial evidence; some is digital clutter. But because every active file stored on a computer has some associated metadata, it's never a question of whether there's metadata, but what kind, where it resides and whether its potential relevance demands preservation and production."*

From Ball, *Make Friends with Metadata*, [www.Law.com](http://www.Law.com), January 26, 2006.

# Types of Metadata

- Wescott, [The Increasing Importance of Metadata](#), 14 Rich. J. L. & Tech. 10 identifies 3 types of metadata:
- ***System metadata*** [is] 'data that is automatically generated by a computer system." Examples of system metadata include 'the author, date and time of creation, and the date a document was modified.
- ***Substantive metadata***... is data that reflects the substantive changes made to the document by the user and which can be viewed or hidden by the user at will. Examples in a minute.
- ***Embedded metadata*** is defined as the text, numbers, content, data, or other information that is directly or indirectly inputted into a Native File by a user and which is not typically visible to the user viewing the output display of the Native File on screen or as a print out. For example, spreadsheet formulas, hidden columns, externally or internally linked files, etc. This may be the most important category, as demonstrated below.

- Some courts have gone to the extreme in ordering the production of metadata. Most famously, *Williams v. Sprint/United Mgmt Co.*, 2005 WL 2401626 (D. Kan. Sept. 29, 2005), where the court held:

**"when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, ...."**

- However, some Courts have expressed a great deal of skepticism concerning metadata. In *U.S. v. Zerjav*, 2009 WL 2143756 (E.D. Mo. 2009) the Court opened its opinion by stating: "While the Parties may exchange metadata by agreement, the Court has no intention of requiring any party, in any case, to produce metadata without showing that other means of obtaining the discoverable material failed." In *Kingsway Financial Services v. PriceWaterhouseCoopers*, 2008 WL 5423316 (S.D. N.Y. 2008) the Court stated that in the absence of an issue concerning the authenticity of a document or the process by which it was created, most metadata has no evidentiary value.

# The Evolving Concept of Metadata

- In *Dahl vs. Bain Capital Partners*, 2009 WL 1748526 (D. Mass. 2009), the Shareholders sought all of the metadata associated with emails and word documents produced by the company. In *City of Phoenix v. Lake*, 207 P.3d 725 (Ariz. App. 2009), a citizen filed public records requests with a municipality. Suspecting that the notes had been backdated, the citizen requested the metadata that accompanied those notes. Despite a strong public policy in Arizona favoring disclosure of public records, the Lake Court concluded that there was a distinction between a public record and a "metadata record," and that disclosure was only required for public records.

- In *Indianweekly.com v. Nehaflix, Inc.*, 596 F. Supp. 2d 497 (D. Conn. 2009), the issue involved the metadata of a webpage and the metadata's content. *See also State ex rel. Toledo Blade v. Seneca County*, 120 Ohio St. 3d 372, 899 N.E.2d 961 (Ohio 2008) where a newspaper was permitted to conduct a forensic examination of government computers to seek restoration of email deleted by public officials in violation of open record law.
- Metadata has become such a recognized component of electronically stored information that there are now patents pending which define and control access to metadata. See *Fotomedia v. AOL, LLC*, 2009 WL 2175845 \*2-3 (E.D. Tex. 2009).

## STATEMENT OF AMICUS INTEREST OF THE WISCONSIN ACADEMY OF TRIAL LAWYERS

The Wisconsin Academy of Trial Lawyers ("WATL") is dedicated to the proposition that every citizen should have the opportunity to be heard in the laws of Wisconsin. The Wisconsin Constitution declares that government draws its power from the consent of the governed. Citizens agree to obey the law in return for the protection of government. This contract is effective only to the degree that people have confidence that most other citizens will do as they do, and that our local

dual litigants  
important that  
law in order to  
the insurance  
rers who do  
support of the  
ical Lutheran

**FINAL TRINITY AMICUS DRAFT.doc Properties**

General Summary Statistics Contents Custom

Created: Tuesday, November 19, 2002 3:51:00 PM  
Modified: Thursday, January 26, 2006 12:39:54 PM  
Accessed: Saturday, January 28, 2006  
Printed: Tuesday, November 19, 2002 5:36:00 PM

Last saved by: Administrator  
Revision number: 17  
Total editing time: 216 Minutes

Statistic name	Value
Pages:	12
Paragraphs:	64
Lines:	294
Words:	2869
Characters:	14481
Characters (with spaces):	17453

OK Cancel

**New Document**

Open a document

- FINAL TRINITY AMICUS DRAFT.doc
- MORE NAMES FOR MAILING LIST.doc
- OUTLINE FOR 3-3-06 SEMINAR.doc
- MAILING LIST.doc
- 74 list.doc
- 7-20-04 - FINAL DRAFT.doc
- CALFEE ITEMS TO CALL UP - OHIO.doc
- stwd0206.doc
- stwd0206.doc
- More documents...

New

- Blank Document
- Blank Web Page
- Blank E-mail Message

New from existing document

- Choose document...

New from template

- Batch Conversion Wizard
- General Templates...
- Templates on my Web Sites...
- Templates on Microsoft.com

Add Network Place...

Microsoft Word Help

Show at startup



General

Summary

Statistics

Contents

Custom

Created: Tuesday, November 19, 2002 3:51:00 PM  
Modified: Thursday, January 26, 2006 12:39:54 PM  
Accessed: Saturday, January 28, 2006  
Printed: Tuesday, November 19, 2002 5:36:00 PM

Last saved by: Administrator  
Revision number: 17  
Total editing time: 216 Minutes

Statistics:

Statistic name	Value
Pages:	12
Paragraphs:	64
Lines:	294
Words:	2869
Characters:	14481
Characters (with spaces):	17453

OK

Cancel

General

Summary

Statistics

Contents

Custom

Name:

Add

Date completed ▲

Department

Destination

Disposition

Division

Document number ▼

Delete

Type:

Text ▼

Source:

\_Toc12778599 ▼



Link to content

Properties:

Name	Value	Type
☞ Documen...	STATEMEN...	Text

OK

Cancel

Reply Reply All Forward Print Delete Previous Next

**From:** William C. Gleisner, III  
**Date:** Saturday, February 04, 2006 5:18 PM  
**To:** Ruth Simpson  
**Cc:** Jane E. Garrott  
**Subject:** MAIR v. Trollhaugen Ski Resort, Supreme Court Appeal No. 2004AP1252

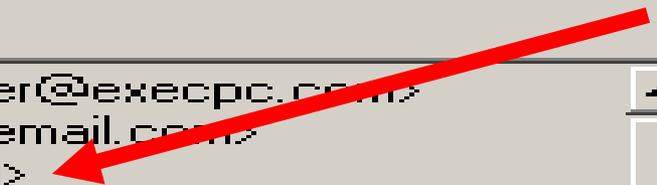
Good Afternoon Ruth,

Should WATL seek to participate in the oral argument of *Mair* as Amicus Curiae, now scheduled for March 14, 2006 at

General Details

headers for this message:

From: "William C. Gleisner, III" <gleisner@execpc.com>  
To: "Ruth Simpson" <ruth@choiceonemail.com>  
Cc: "Jane E. Garrett" <exec@watl.org>  
Bcc: "Robert L. Jaskulski" <rjaskulski@habush.com>,  
"Linda Meagher" <LMeagher@Habush.com>,  
"D. James Weis" <djweis@habush.com>,  
"Rhonda L. Lanford" <rlanford@habush.com>,  
"Mark L. Thomsen" <mthomsen@cannon-dunphy.co  
"Charles Schmidt" <cschmidt@Cannon-Dunphy.com>  
"Lynn Laufenberg" <LRL@lauflaw.com>,  
"Martha Heidt" <ddskow@baldwin-telecom.net>,  
"Lora A. Kaelber" <lkaelber@grayandend.com>,  
"Ruth Simpson" <ruth@choiceonemail.com>  
Subject: MAIR v. Trollhaugen Ski Resort, Supreme Court Appe.  
Date: Sat, 4 Feb 2006 17:18:09 -0600  
MIME-Version: 1.0  
Content-Type: multipart/related;  
boundary="-----\_NextPart\_000\_017A\_01C629AE.F8E  
type="multipart/alternative"



Message Source...

OK

Cancel

- By the way, when it comes to email discovery, to do it right you will need the assistance of a forensic computer expert. But, **if the email is important, don't settle for hardcopy.**
- In order to “capture” the email from an adversary's computer system so that you preserve all of the relevant metadata you need to obtain a copy of the email database which contains the email. In the case of Outlook that's the .pst file; in the case of Outlook Express that's the .dbx file; and in the case of Lotus Notes that's the .nsf file. There are many other email database systems out there, such as Eudora or proprietary systems.

- Favorites
- Add... Organize...
  - GRENIG - WEB SITES
    - Download Stationery for Outlook Express [Int...
  - GRENIG
  - MARCUS THEATERS
  - Distance Education
  - Jane Joseph
  - KERRY
  - Links
  - Media
  - POEMS
  - ABC News Homepage Online news, breaking n...
  - Wisconsin State Law Library - Home Page
  - AltaVista
  - GOOGLE
  - Ask Jeeves - Ask.com
  - ATLA Homepage
  - ATLA Sign-On Page
  - Buderus
  - CHEAP SOFTWARE
  - CNN.com Specials
  - CNN.com
  - DRI Homepage
  - Free AOL & Unlimited Internet
  - HouseCall online virus Scan - Scan Now
  - MSNBC - MSNBC Front Page
  - HP United States - Welcome
  - Internet Explorer Home
  - Manual for Complex Litigation, Fourth
  - MicroLaw - Legal Technology Consultants - Mil...
  - Microsoft Download Center Windows (Security...
  - Netscape ISP Try It! \$9.95
  - Netscape.com
  - Marquette University Law School- 1974 Class ...
  - Merijn.org
  - OnMilwaukee.com - Milwaukee's Daily Magazine
  - Outdoor Life Network - Home - 154045 GMT
  - Outlook Express Support Center
  - Radio Station Guide
  - Roxio - Home
  - Security Updates for Juno

- United States (change) Microsoft.com Home | Site Map
- Microsoft Office Online
- Search: Assistance Go
- Home
  - Assistance**
  - Training
  - Templates
  - Clip Art and Media
  - Downloads
  - Office Marketplace
  - Work Essentials
  - Microsoft Office System
  - Deployment Center

- Things To Do
- [Suggest new content](#)
  - [Get answers from other Office users](#)
  - [Get our newsletter](#)
  - [Contact Us](#)

## Find and remove metadata (hidden information) in your legal documents

Help

Applies to: [PowerPoint](#), [Word](#), [Excel](#)

Legal professionals are familiar with the concept of "discovery" and the requirements set out by the courts for complying with discovery demands. They also understand that they are only required to provide the documents and data set out in the discovery demand. Unfortunately, if you are providing electronic versions of your documents, you may "discover" that you are inadvertently supplying more information than you realize.

### Metadata

Whenever you create, open, or save a document in Microsoft Word, the document may store information — known as metadata — that you had no intention of including or disclosing (this also applies to Microsoft Excel spreadsheets and Microsoft PowerPoint® files). Metadata is used for a variety of legitimate purposes, and it adds functionality to the editing, viewing, filing, and retrieving capabilities of Microsoft Office. However, if some of this information is passed on to inappropriate parties (for example, opposing counsel), that disclosure can create adverse consequences for you and your client. In order to avoid these consequences, you should make yourself familiar with the types of metadata contained in your documents and take steps to remove it whenever necessary.

Some metadata is readily accessible through the user interface of each Office program. Other metadata is only accessible through extraordinary means, such as opening a document in a low-level, binary file editor.

### Some examples of metadata that may be stored in your documents

- Your name
- Your initials
- Your company or organization name
- The name of your computer
- The name of the network server or hard disk where you saved the document
- Other file properties and summary information
- Non-visible portions of embedded OLE objects
- The names of previous document authors
- Document revisions
- Document versions
- Template information
- Hidden text or cells
- Personalized views
- Comments

### Removing metadata

The articles listed below provide information and instructions for removing metadata from your Word documents, Excel spreadsheets, and PowerPoint presentations. Simply click the article number to view the article in the Microsoft Knowledge Base.

- [237361](#) HOW TO: Minimize Metadata in Microsoft Word 2000 Documents
- [290945](#) HOW TO: Minimize Metadata in Microsoft Word 2002
- [223789](#) XL: How to Minimize Metadata in Microsoft Excel Workbooks





# One other point re: Hidden Data

- ***I tell Plaintiffs' counsel: You will certainly miss hidden data if you are not aware of and sensitive to how databases work.*** Be careful for online database may not include all the fields available in that database. The following screen shots demonstrate the phenomena of database "hidden data."

Enter Search Phrase

Fields	Begdoc#	DocTitle	Document Recipients	Docdate
1	RAC990511-18375	RAG DOCUMENT PRODUCTION FILE HEADER GREEN	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	05/12/1999
2	RAC990511-19716	WRITTEN UNANIMOUS CONSENT OF THE BOD AND SOLE SHAREHOLDER OF RAC ADPZONA ET AL	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	05/16/1995
3	RAC-12354	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	01/18/1996
4	RAC-12352	EMPLOYEE PROFIT SHARING PLAN MANAGING COMMITTEE AND EMPLOYEE STOCK OPTION PLAN	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
5	RAC-12348	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	11/21/1995
6	RAC-12346	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
7	RAC-12344	DIRECTORATE COMMITTEE ORGANIZATION: AUDIT AND EXAMINING	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
8	RAC-12342	EXHIBIT B: DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
9	RAC-12333	MINUTES OF THE REGULAR MEETING OF THE BOD OF 05/02/95	KAPLAN, JAMES I.; AND RAG	05/02/1995
10	RAC-12274	PRESENTATION BY THE CHICAGO	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	10/18/1995
11	RAC-12261	SUMMARY OF STRATEGIC ALTERNATIVES POTENTIALLY AVAILABLE TO THE	SPECIAL COMMITTEE OF BOD	10/18/1995
12	RAC-12259	LETTER TO SPECIAL COMMITTEE II EXHIBIT	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
13	RAC-12258	EXHIBIT B: SPECIAL COMMITTEE II RESOLUTIONS	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
14	RAC-12255	-CONSOLIDATED THIRD QUARTER 1995 FINANCIALS	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	10/23/1995
15	RAC-12251	MINUTES OF THE REGULAR MEETING OF THE BOD OF 10/24/95	JEFFREY W.	10/24/1995
16	RAC-11599	RESUME	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
17	RAC-11597	RESUME	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
18	RAC-11596	CONFIRMATION LETTER FOR TELEPHONE	KAPLAN, JAMES I.; CTFG AND RAG	07/13/1995

### RELIANCE LITIGATION MASTER FORM

Category Key #  Category Name

Document Begin #  Document End #  # of Pgs

Unique Main Record #  Unique attachment #  Unique sub-attachment #

Addon Doc  Box#  DocDate  Estimated Date?  Undated?

Document Recipients  DocTitle

Document Authors  Copy Recipients

Names referenced in doc  Work Papers #\_Info

Document Type  Folder of Origin

Privileged?  Confidential?  Is this a Main Document?  Is this an Attachment to a doc?

Complete Main Doc First #  Complete Main Doc Last #

Name of main doc to which this is an attachment

Sub attach?  Complete Sub Main First #  Complete Sub Main Last #

Name of sub-main doc to which this is a sub attachment

Cross Reference to Related Document(s)

Marginalia?  Problems (e.g., missing page)

Issues  Key words

Deponent's Name  Deposition Exhibit No.

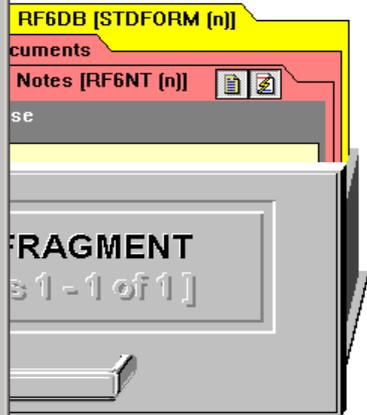
Defendant A Cross-Exhibit #  Def't B Cross-Exhibit #  Def't C Cross-Exhibit #

Comment

STATISTICAL INFORMATION

Has Image  YES Record created by:  Created on  Created at

Record updated on:  Updated at:  Hot Fact



Summation Blaze - Database RF63DB

File Edit Search Summary Field Notes Options Window Help

Enter Search Phrase

Form Column ocrBase

Column STDFORM Edit: Summary 3 of 35

Fields	Begdoc#	DocTitle	Document Recipients	Docdate
1	RAC990511-18375	RAG DOCUMENT PRODUCTION FILE HEADER GREEN	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	05/12/1999
2	RAC990511-19716	WRITTEN UNANIMOUS CONSENT OF THE BOD AND SOLE SHAREHOLDER OF	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	05/16/1995
3	RAC-12354	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	01/18/1996
4	RAC-12352	EMPLOY PROFIT SHARING PLAN MANAGING COMMITTEE AND EMPLOY STOCK OPTION PLAN	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
5	RAC-12348	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	11/21/1995
6	RAC-12346	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
7	RAC-12344	DIRECTORATE COMMITTEE ORGANIZATION: AUDIT AND EXAMINING	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
8	RAC-12342	EXHIBIT B: DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
9	RAC-12333	MINUTES OF THE REGULAR MEETING OF THE BOD OF 05/02/95	KAPLAN, JAMES I.; AND RAG	05/02/1995
10	RAC-12274	PRESENTATION BY THE CHICAGO	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	10/18/1995
11	RAC-12261	SUMMARY OF STRATEGIC ALTERNATIVES POTENTIALLY AVAILABLE TO THE	SPECIAL COMMITTEE OF BOD	10/18/1995
12	RAC-12259	LETTER TO SPECIAL COMMITTEE II EXHIBIT	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
13	RAC-12258	EXHIBIT B: SPECIAL COMMITTEE II RESOLUTIONS	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
14	RAC-12255	-CONSOLIDATED THIRD QUARTER 1995 FINANCIALS	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	10/23/1995
15	RAC-12251	MINUTES OF THE REGULAR MEETING OF THE BOD OF 10/24/95	JEFFREY W.	10/24/1995
16	RAC-11599	RESUME	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
17	RAC-11597	RESUME	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
18	RAC-11596	CONFIRMATION LETTER FOR TELEPHONE	KAPLAN, JAMES I.; CTFG AND RAG	07/13/1995

Begdoc# Note ANKey Template

Editing Zoom

Fields	Begdoc#	DocTitle	Document Recipients	Docdate
1	RAC990511-18375	RAG DOCUMENT PRODUCTION FILE HEADER GREEN	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	05/12/1999
2	RAC990511-19716	WRITTEN UNANIMOUS CONSENT OF THE BOD AND SOLE SHAREHOLDER OF RAC ADI... ET AL	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	05/16/1995
3	RAC-12354	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	01/18/1996
4	RAC-12352	EMPLOY PROFIT SHARING PLAN MANAGING COMMITTEE AND EMPLOY STOCK OPTION PLAN	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
5	RAC-12348	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	11/21/1995
6	RAC-12346	DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
7	RAC-12344	DIRECTORATE COMMITTEE ORGANIZATION: AUDIT AND EXAMINING	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
8	RAC-12342	EXHIBIT B: DIRECTORATE COMMITTEE ORGANIZATION:	SEE MAIN DOCUMENT SEE BATE STAMP # RAC-12333	04/19/1994
9	RAC-12333	MINUTES OF THE REGULAR MEETING OF THE BOD OF 05/02/95	KAPLAN, JAMES I.; AND RAG	05/02/1995
10	RAC-12274	PRESENTATION BY THE CHICAGO	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	10/18/1995
11	RAC-12261	SUMMARY OF STRATEGIC ALTERNATIVES POTENTIALLY AVAILABLE TO THE	SPECIAL COMMITTEE OF BOD	10/18/1995
12	RAC-12259	LETTER TO SPECIAL COMMITTEE II EXHIBIT	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
13	RAC-12258	EXHIBIT B: SPECIAL COMMITTEE II RESOLUTIONS	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
14	RAC-12255	-CONSOLIDATED THIRD QUARTER 1995 FINANCIALS	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	10/23/1995
15	RAC-12251	MINUTES OF THE REGULAR MEETING OF THE BOD OF 10/24/95	JEFFREY W.	10/24/1995
16	RAC-11599	RESUME	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
17	RAC-11597	RESUME	NOT SPECIFICALLY REFERENCED IN THIS PARTICULAR DOCUMENT	
18	RAC-11596	CONFIRMATION LETTER FOR TELEPHONE	KAPLAN, JAMES I.; CTFG AND RAG	07/13/1995

██████████ FINANCIAL GROUP, INC.  
 DIRECTORATE COMMITTEE ORGANIZATION

Nominating Committee

██████████, Chairman

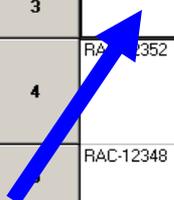
██████████

██████████

Jeffrey ██████████

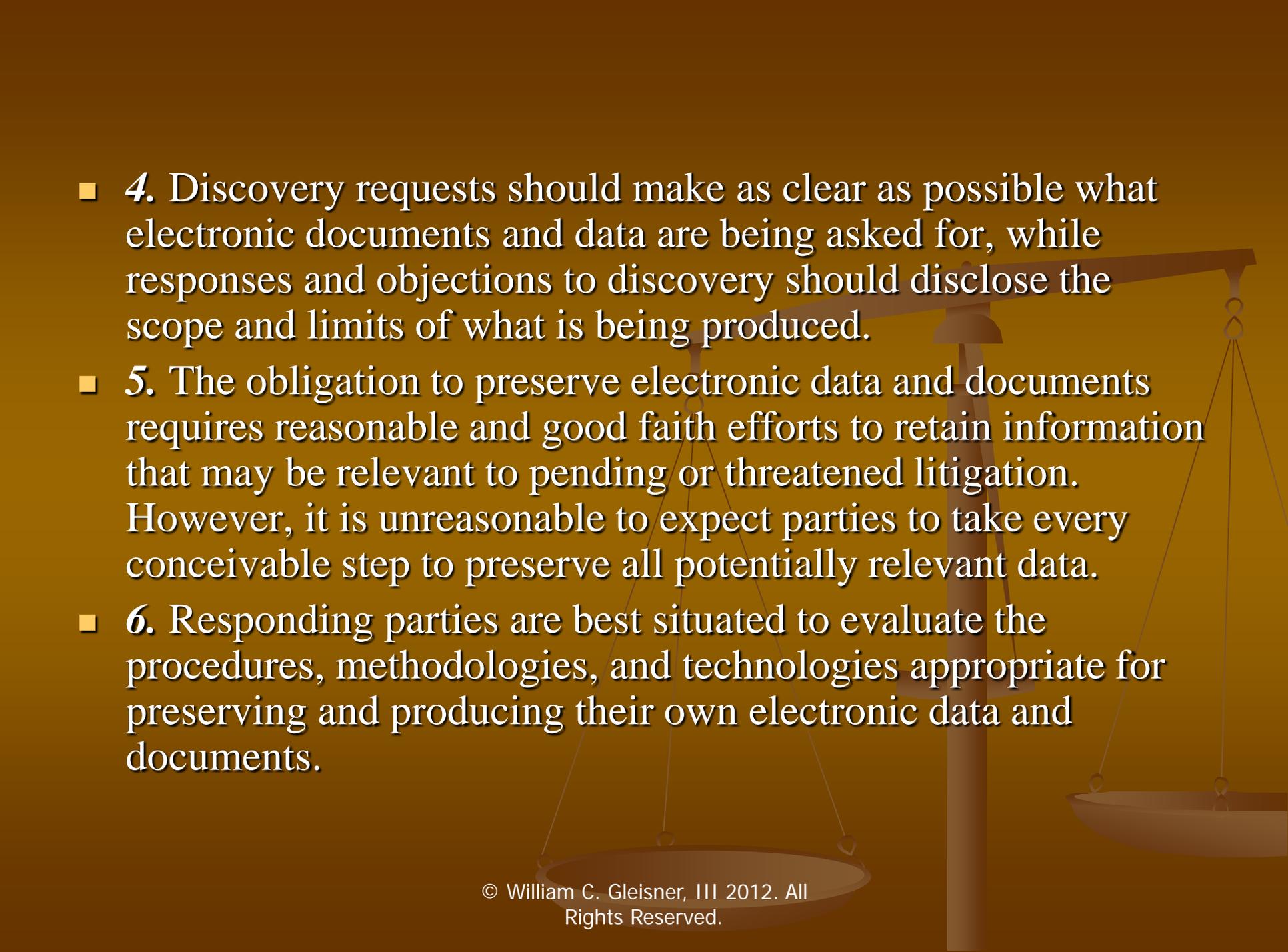
James ██████████, Secretary

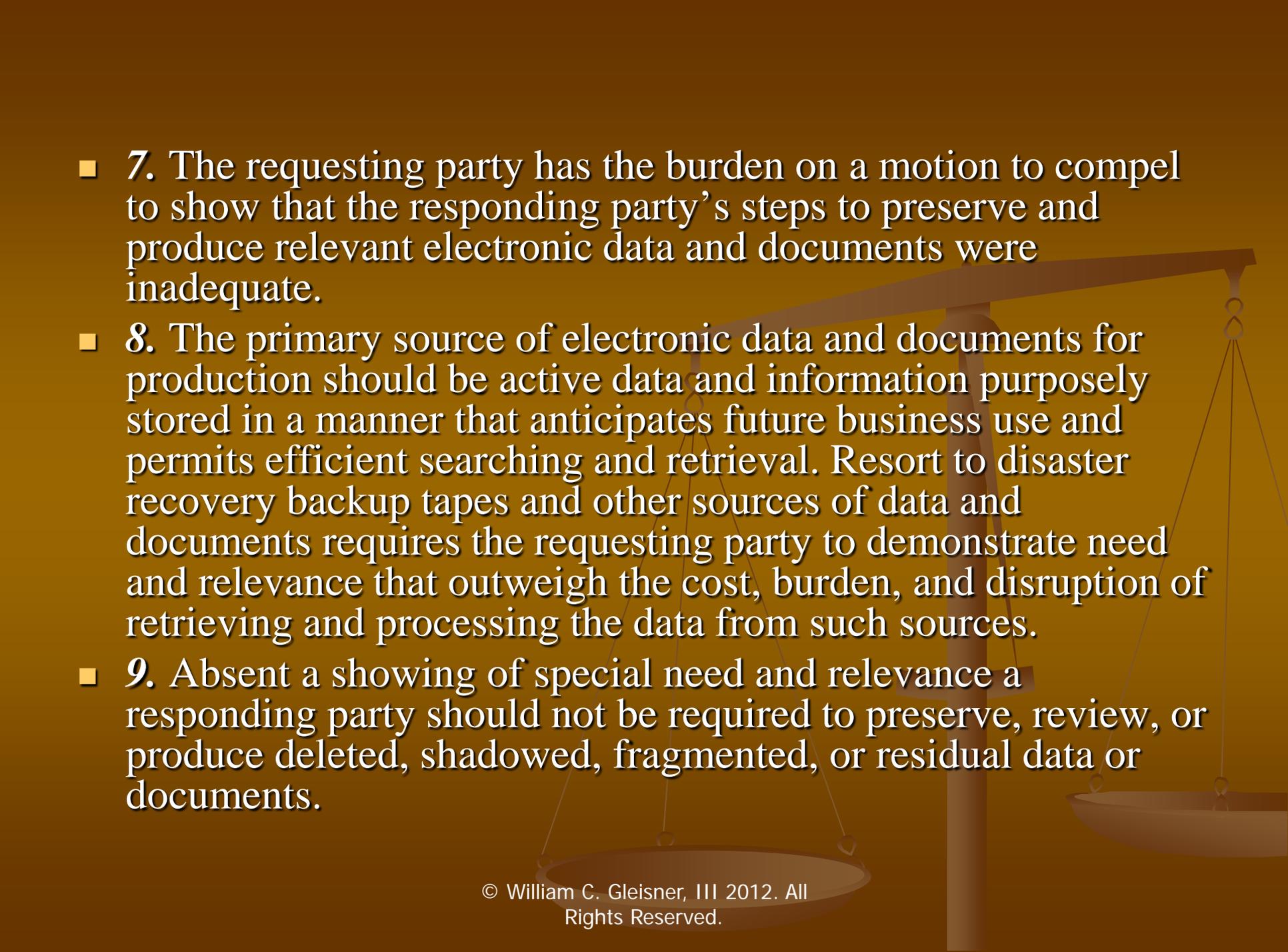
01-18-96

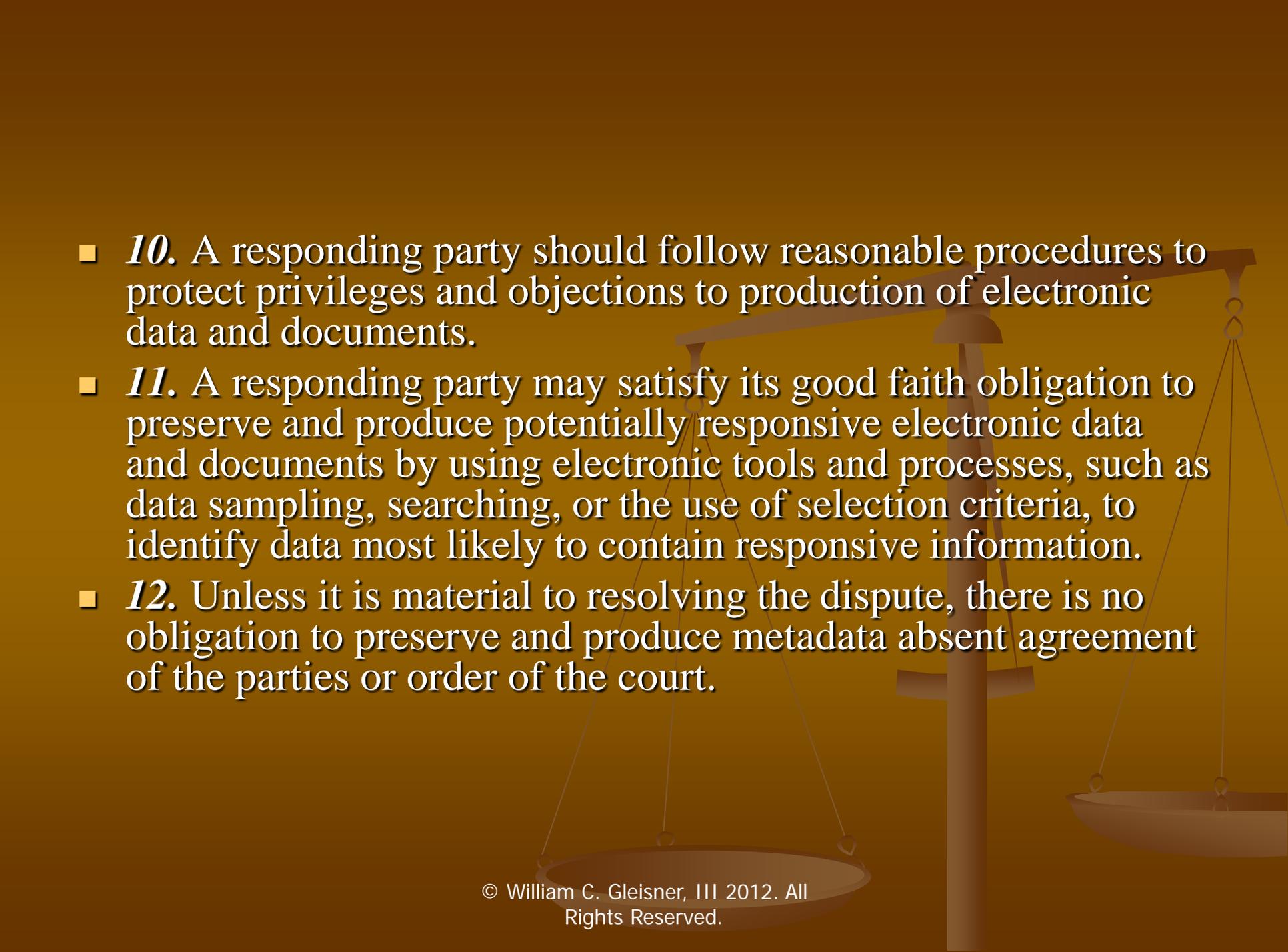


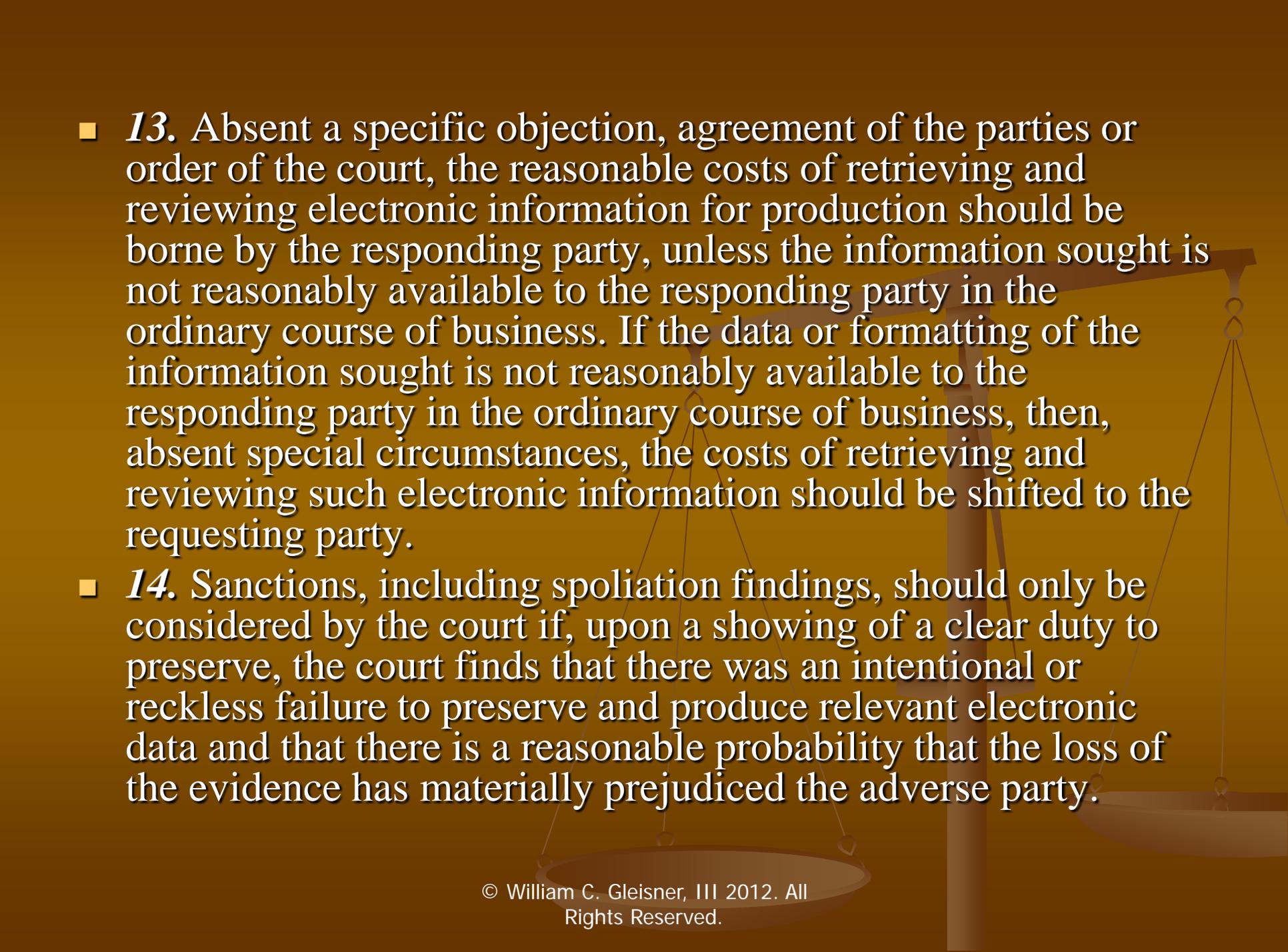
# THE SEDONA PRINCIPLES

- **1.** Electronic data and documents are potentially discoverable under FED. R. CIV. P. 34 or its state law equivalents [in Wisconsin, Wis. Stats. §804.09(1)]. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.
- **2.** When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in FED. R. CIV. P. 26(b)(2) and its state law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.
- **3.** Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.

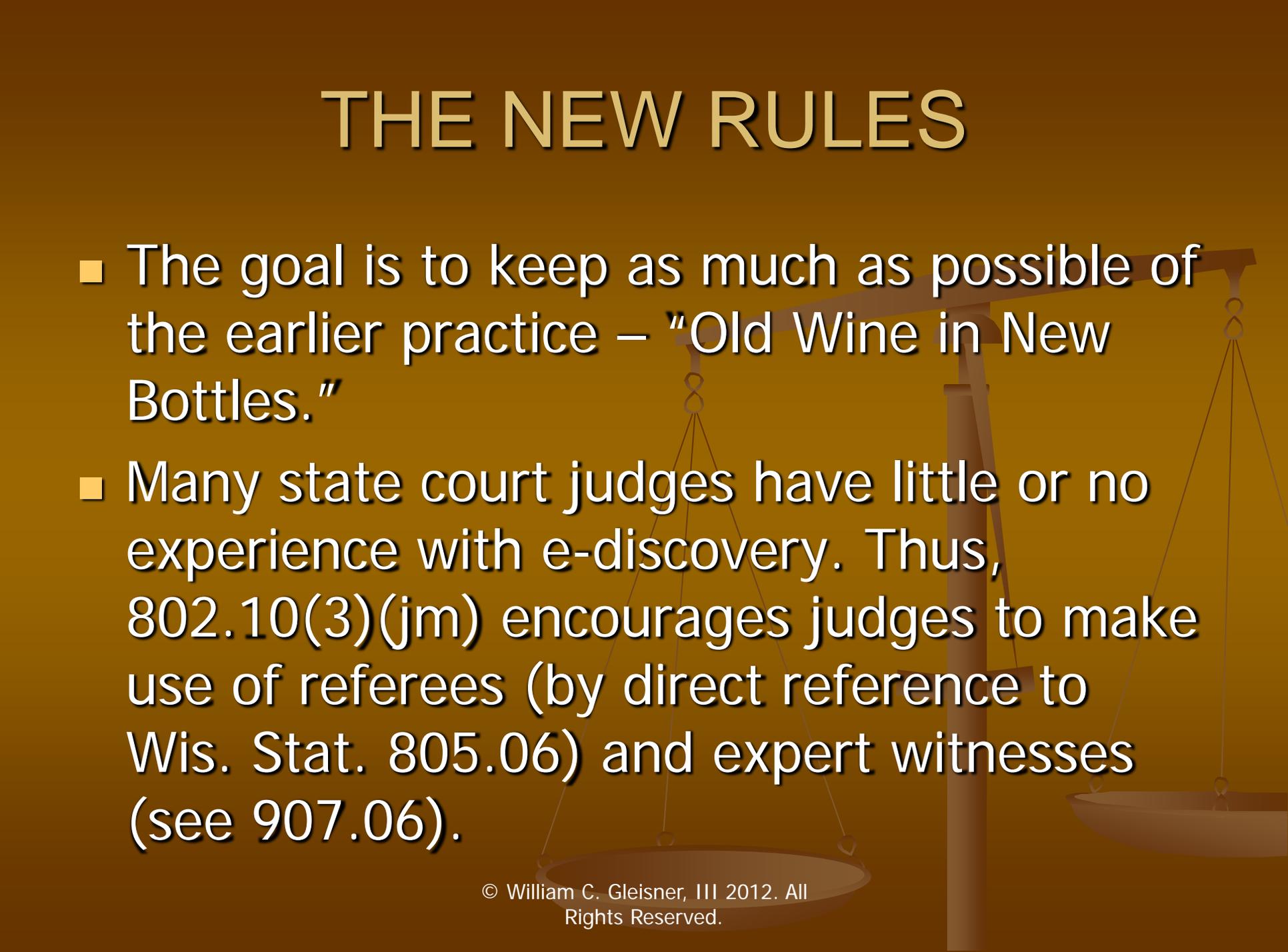
- 
- 4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.
  - 5. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.
  - 6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.

- 
- 7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.
  - 8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.
  - 9. Absent a showing of special need and relevance a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents.

- 
- **10.** A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.
  - **11.** A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.
  - **12.** Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.

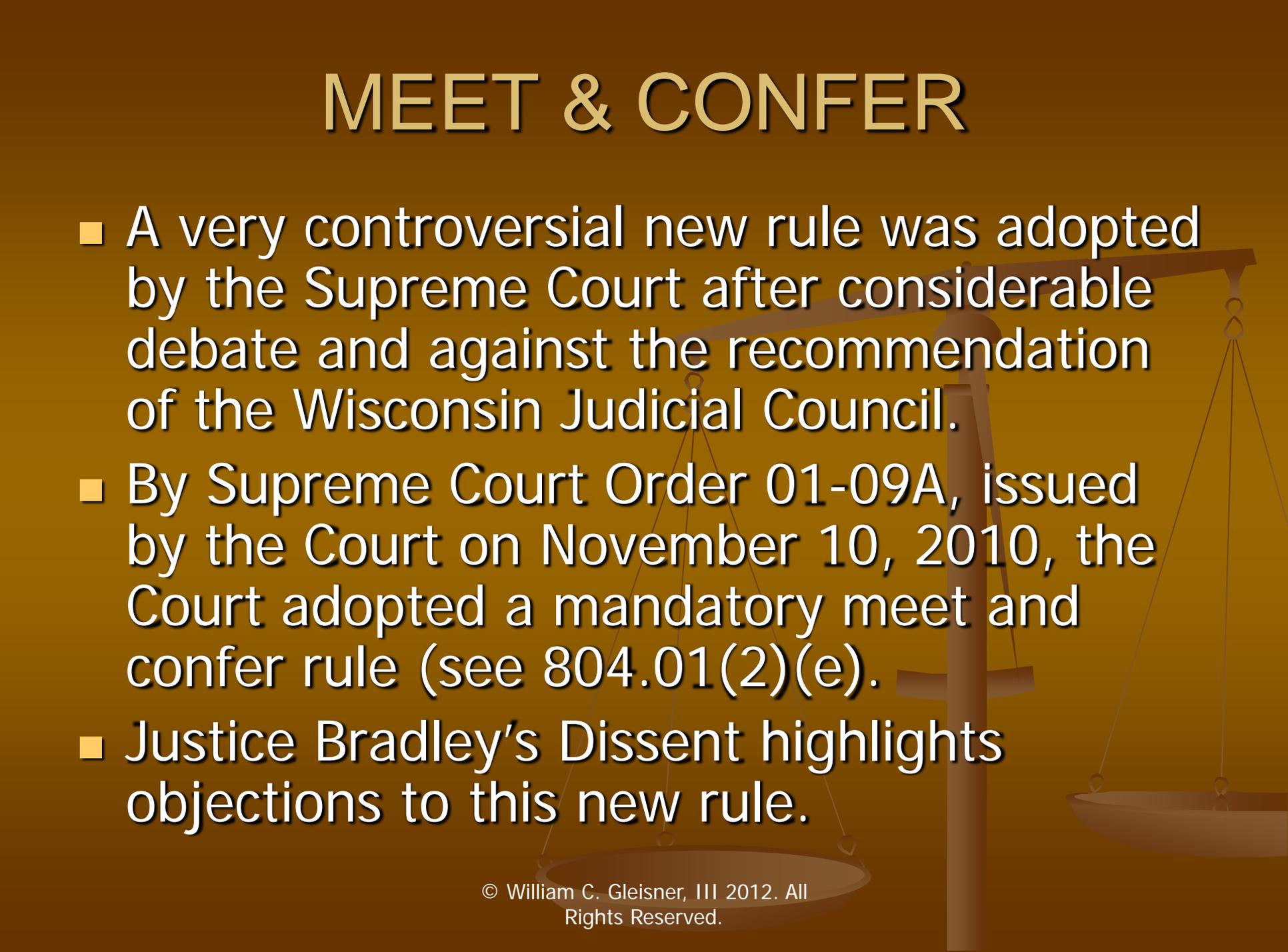
- 
- **13.** Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.
  - **14.** Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

# THE NEW RULES



- The goal is to keep as much as possible of the earlier practice – “Old Wine in New Bottles.”
- Many state court judges have little or no experience with e-discovery. Thus, 802.10(3)(jm) encourages judges to make use of referees (by direct reference to Wis. Stat. 805.06) and expert witnesses (see 907.06).

# MEET & CONFER



- A very controversial new rule was adopted by the Supreme Court after considerable debate and against the recommendation of the Wisconsin Judicial Council.
- By Supreme Court Order 01-09A, issued by the Court on November 10, 2010, the Court adopted a mandatory meet and confer rule (see 804.01(2)(e)).
- Justice Bradley's Dissent highlights objections to this new rule.

# OPTION TO PRODUCE BUSINESS RECORDS IN LIEU OF ANSWERING INTERROGATORIES

- "804.08 (3) OPTION TO PRODUCE BUSINESS RECORDS. The Judicial Council Note states: "Section 804.08 (3) is taken from F.R.C.P. 33(d). Portions of the Committee Note of the federal Advisory Committee on Civil Rules are pertinent to the scope and purpose of s. 804.08 (3): Special difficulties may arise in using electronically stored information, either due to its form or because it is dependent on a particular computer system. Rule 33(d) allows a responding party to substitute access to documents or electronically stored information for an answer only if the burden of deriving the answer will be substantially the same for either party."
- **Very dangerous**. A corporation that opts for this apparently attractive option may be required to supply technical support to the discovering party. **Worse**, selection of this option may require a discovering party to prove the ease by which information supplied can be used and this can open the door to direct access to a defendant's system.

- Federal Commentary: Rule 33(d) allows a party to produce electronic records in response to an interrogatory. The Commentary to new Rule 33(d) provides: "Rule 33(d) allows a responding party to substitute access to documents or electronically stored information for an answer only if the burden of deriving the answer will be substantially the same for either party. ... Satisfying these provisions with regard to electronically stored information may require the responding party to provide some combination of technical support, information on application software, or other assistance. ... [and may involve direct access to a computer system]."

- HEART OF THE NEW WISCONSIN RULES IS 804.09, BASED ON FRCP 34. SO, LET'S TALK A LITTLE ABOUT THE FEDERAL RULES
- New Rule 34(b) permits the requesting party to designate the format in which it wants electronically stored information produced. Under Rule 34 (b) (ii), even if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable." One consolation for the defense bar is the fact that under Rule 34(b)(iii) a party need only produce information in one format, thus preventing an interrogating party from returning to the well because the information that is supplied proves difficult to use.

- One of the great challenges for businesses is to avoid being required to search through disaster recovery tapes or seek out hidden system or metadata. This problem has been addressed in new Rule 26(b)(2)(B), which specifies that *a party does not have to provide discovery of electronically stored information that a party identifies as not reasonably accessible because of undue burden or cost. If challenged, an interrogated party must prove the evidence's inaccessibility.*

# Digital Evidence

How to Preserve, Discover and Use it.

***ATTORNEY WILLIAM C. GLEISNER, III***

Hartland, Wisconsin 53029

Telephone: 262-367-1222

Fax: 262-367-1236

Email: [wgleisner@sbcglobal.net](mailto:wgleisner@sbcglobal.net)