MIMOSA™
SYSTEMS

the know-IT-all's guide to eDiscovery

...because even the smartest, coolest IT experts will have to deal with it sooner or later.

BY BILL TOLSON

ACME
WORLDWIDE, INC.

MEMO: IT DEPARTMENT

PLEASE CIRCULATE:

~~Bob Jones~~
Jeff Ayers
~~Todd McKay~~
~~Mike Hurt~~
John Simon
Paul Blechschmidt
Cindy Meyers

This is great — worth a read. — T

Please review the attached book; Acme is considering options on how to better prepare for potential litigation. Make any notes and pass on to the rest of the department. Thanks.

WITH THE RULES REGARDING E-DISCOVERY CHANGING, WE ALL NEED TO READ THIS — IT'S A GOOD, NO-BS GUIDE.

the know-IT-all's guide to eDiscovery

Look Paul - it's you!

Which Know-IT-All are you?

NAH, THIS IS PAUL, AND MAYBE TODD.

CHECK ALL THAT APPLY.

☐

fig. 1: JOE COOL

The resident wunderkind—you can close most trouble tickets with 10 simple keystrokes and a smug smile. Chicks really dig that.

☐

fig. 2: MR. FIX IT

Hero of the helpdesk—your techie obsession has paid off. Look who needs your geeky know-how now. It's the revenge of the nerds.

☐

fig. 3: TH E ALL NIGHTER

No 9-to-5'er, and it shows—it looks like you slept in your clothes because you did, at your desk. Whatever it takes, man.

☐

fig. 4: THE CONNOISSEUR

No school like the old school--you know what ports and protocols all systems use to talk AND you can synch the berry. You are Morpheus to their Neo.

☐

fig. 5: THE SMARTY PANTS

A promising new recruit—you know the coolest trends, the latest tech, and the big buzz words. No one understands a word you say.

☐

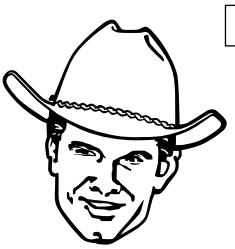


fig. 6: THE RENEGADE

Standard procedures are for chumps—you've learned some problems are fixed with paperclips and chewing gum. Giddyup, who's next?

The Know-IT-All Quiz
Question 1:

eDiscovery is defined as:

A) Online speed dating.

B) Getting to know that hot chick on Second Life®

C) Touring the world on Google Earth™

D) A panicked last-minute request from your corporate legal department requiring you to wade through endless terabytes of ESI, on top of your already-full workload.

Sorry, no – eDiscovery is not online speed dating

Electronic discovery (also called e-Discovery or eDiscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. eDiscovery can be carried out offline on a particular computer or it can be done on the network.[1]

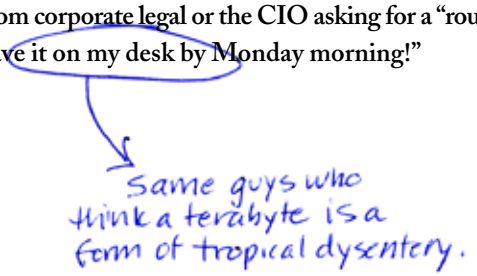
Recent amendments to the Federal Rules of Civil Procedure (FRCP) highlighted that electronically stored information (ESI) is a discoverable record type and should be treated as any other type of evidence (see Chapter Two). In civil eDiscovery, all ESI that could pertain to a case must be found, protected, and turned over to opposing counsel when requested.

It is usually the party being discovered that pays the cost of the discovery.

What does this mean for IT?

It means you may be directed to find specific files (including SharePoint records, emails and metadata) containing specific content, from or to specific employees, sent between specific dates. It can be pretty specific! If your company is like most companies, you will have to search through terabytes of ESI to find this information. To make matters worse, you'll likely have mere days or—at best—a couple of weeks to do so. If you cannot fully comply with opposing counsel's request, your company could lose the case before it ever gets to trial. And losing will cost you—huge fines, punitive damages, and opposing counsel's fees.

Corporate management often doesn't appreciate what's required to adequately respond to discovery requests—especially if they have not been through the process before. Many IT administrators know this pain— the Friday afternoon phone call from corporate legal or the CIO asking for a "round-up" of all ESI detailed in a new discovery request. "Have it on my desk by Monday morning!"

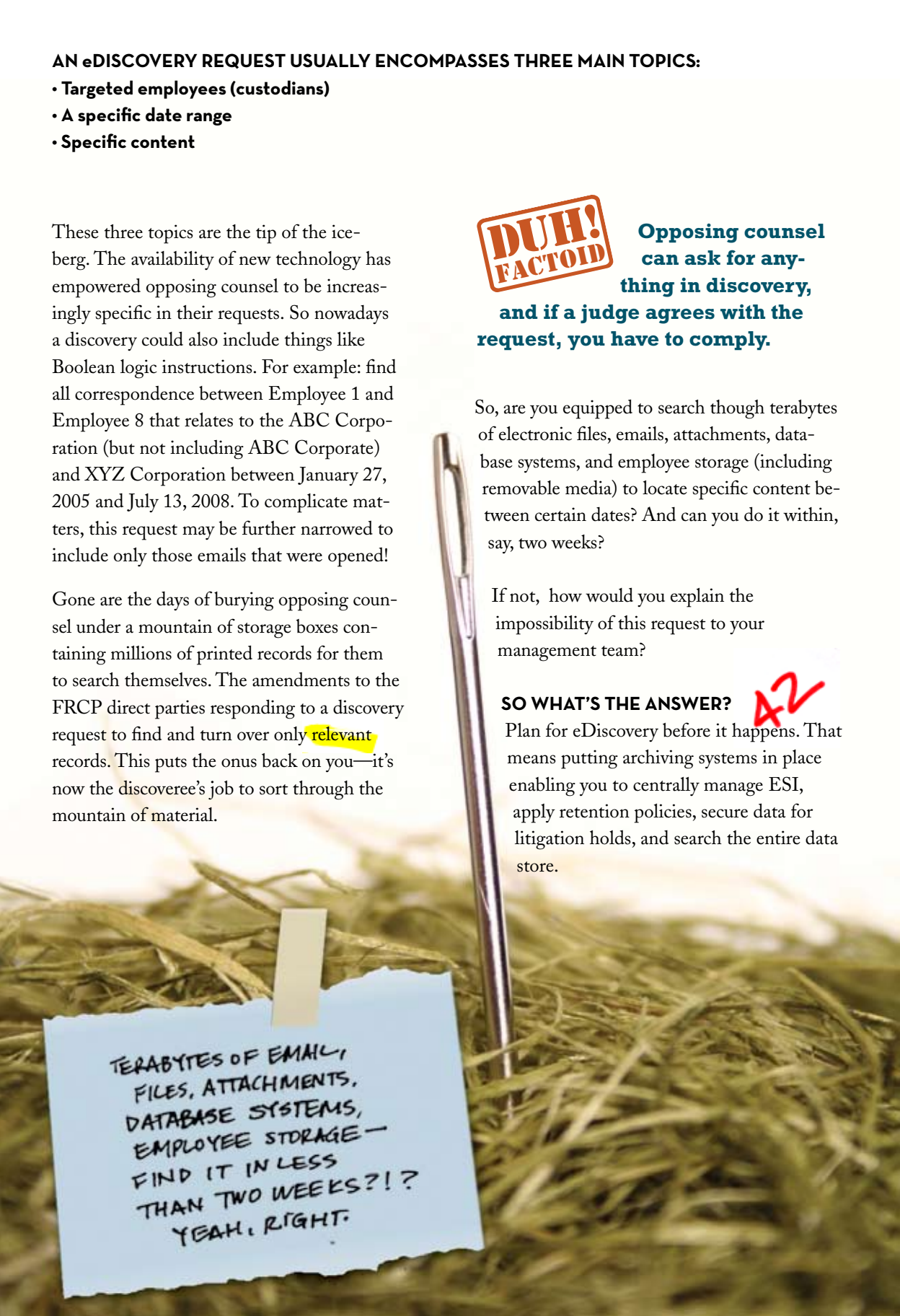


AN eDISCOVERY REQUEST USUALLY ENCOMPASSES THREE MAIN TOPICS:

- **Targeted employees (custodians)**
- **A specific date range**
- **Specific content**

These three topics are the tip of the iceberg. The availability of new technology has empowered opposing counsel to be increasingly specific in their requests. So nowadays a discovery could also include things like Boolean logic instructions. For example: find all correspondence between Employee 1 and Employee 8 that relates to the ABC Corporation (but not including ABC Corporate) and XYZ Corporation between January 27, 2005 and July 13, 2008. To complicate matters, this request may be further narrowed to include only those emails that were opened!

Gone are the days of burying opposing counsel under a mountain of storage boxes containing millions of printed records for them to search themselves. The amendments to the FRCP direct parties responding to a discovery request to find and turn over only relevant records. This puts the onus back on you—it's now the discoveree's job to sort through the mountain of material.



Opposing counsel can ask for anything in discovery, and if a judge agrees with the request, you have to comply.

So, are you equipped to search though terabytes of electronic files, emails, attachments, database systems, and employee storage (including removable media) to locate specific content between certain dates? And can you do it within, say, two weeks?

If not, how would you explain the impossibility of this request to your management team?

SO WHAT'S THE ANSWER? 42

Plan for eDiscovery before it happens. That means putting archiving systems in place enabling you to centrally manage ESI, apply retention policies, secure data for litigation holds, and search the entire data store.

My CIO wants me to come up to speed and follow the new federal rules of civil procedure.
I told him to quit telling me how to treat my wife.

The Know-IT-All Quiz Question 2:

What are the Federal Rules of Civil Procedure?

A) Lie. Deny. Then Jerry Springer.

B) Why I divorced my third wife.

C) Do not talk about the Federal Rules of Civil Procedure. There are no Federal Rules of Civil Procedure.

D) The legal playbook governing court procedures for civil suits in the United States district courts—recently amended to make life a whole lot easier for lawyers and a whole lot harder for the IT crew.

It's all geek to me (Reviewing the new FRCP amendments)

All employees—and especially IT folk—need to understand their responsibilities under both their state's rules of civil procedure and the new Federal Rules of Civil Procedure (FRCP). That's because, under certain circumstances, any employee can be held personally responsible for the destruction of evidence by deleting electronically stored information (ESI). Knowing how to manage ESI substantially lowers everyone's risk.

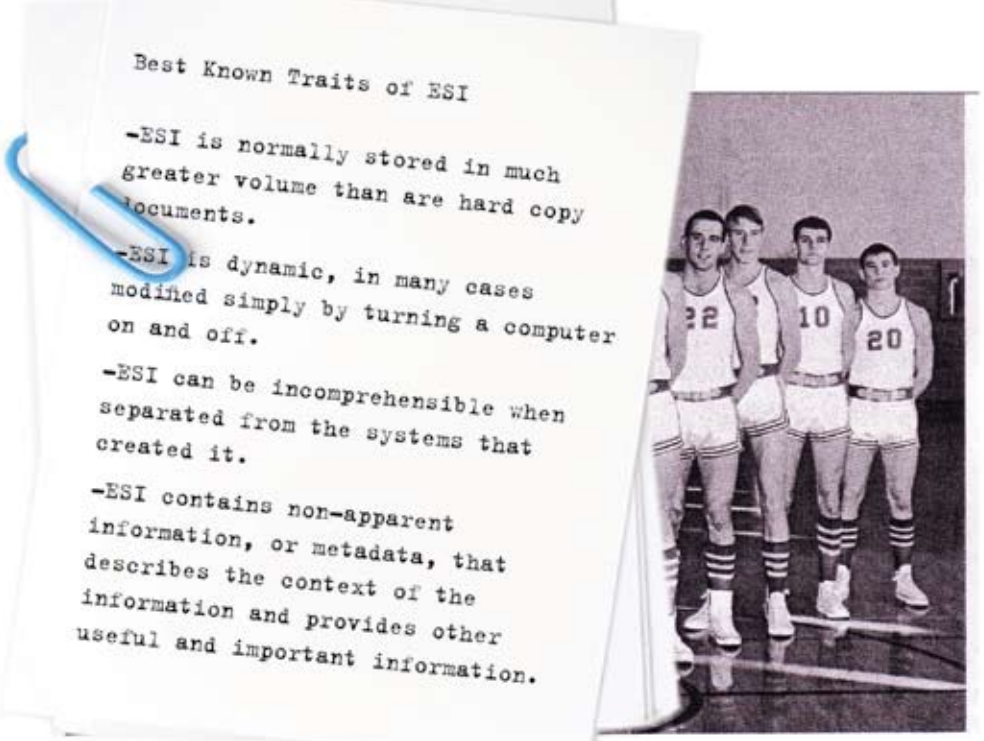
WHAT ARE THE FEDERAL RULES OF CIVIL PROCEDURE?

The FRCP, established in 1938, govern federal court procedures for civil suits in the United States district courts. Put forth by the United States Supreme Court pursuant to the Rules Enabling Act, they were then approved by the United States Congress. The Court's modifications to the rules are usually based on recommendations from the Judicial Conference of the United States, the federal judiciary's internal policy-making body. Although federal courts are required to apply the substantive law of the states as rules of decision in cases where state law is in question, the federal courts almost always use the FRCP as their rules of procedure. States make their own rules that apply in their own courts, but most states have adopted rules based on the FRCP.

The most recent revision to the FRCP, which took effect in December 2006, included practical changes to discovery rules to make it easier for courts and litigating parties to manage electronic records. These new amendments continue to have a major effect on how companies retain, store, and produce ESI for litigation—especially email, SharePoint, and file system data.

The FRCP does not specify or even suggest any technologies be used for record archiving or eDiscovery processes, but rather makes clear the obligation to quickly secure, hold, and produce all pertinent data for litigation when directed.

In many companies, the IT staff is in charge of collecting ESI and applying litigation holds. So, to reduce your personal risk, you'd better understand your company's legal responsibilites.



TEAM ESI: THE NEW AMENDMENTS

The new amendments define what ESI is, what ESI must be disclosed, and when. They also place new requirements on the parties' knowledge of their own electronic infrastructure—what ESI they have, where it's kept, how it's retained, and how it's deleted. The FRCP also reiterates the parties' obligations for preserving potential electronic evidence. The new amendments to FRCP rules 16, 26, 33, 34, and 37 are aimed directly at ESI.

DUH! FACTOID

The fact that your company has never had a civil lawsuit against it does not mean it never will. Chances are your company will either be a direct target of litigation or a third-party to discovery sooner or later.

The changes reflect the reality that discovery of email and other ESI is now a routine—yet critical—aspect of every litigated case. First, the amendments treat ESI differently. Second, they require early discussion of and attention to electronic discovery. Third, they address inadvertent production of privileged or protected materials. Fourth, they encourage a two-tiered approach to discovery—deal with reasonably accessible information and then later with inaccessible data. Finally, they provide a safe harbor from sanctions by imposing a good faith requirement.[2]

Any organization that can be sued in federal court is affected by these amendments. So all organizations need to proactively manage all aspects of their electronic infrastructure, including litigation hold capability and ESI retention policies.

That means us, dude! Yikes!

Rule 26

This rule clarifies a responding party's duty to include ESI in its initial disclosures. It also requires the party to describe where, in what form, and the accessibility of all ESI they have in their possession. It reads, in part: "A copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment." [3]

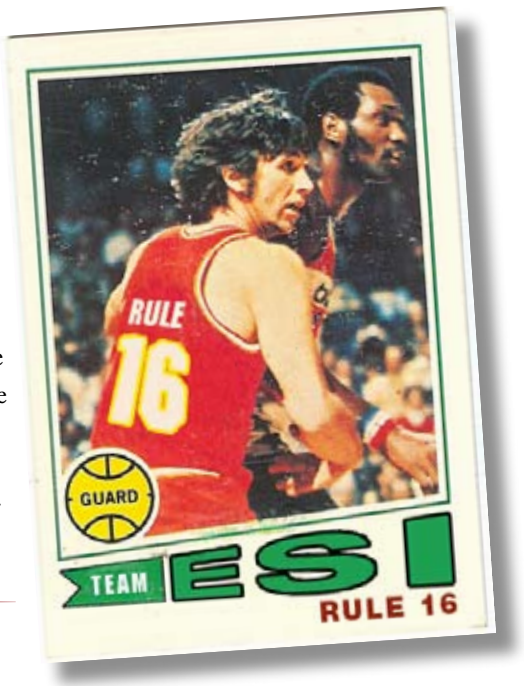
Rule 26(a)(1)

Rule 26(a)(1) specifies that the organization must have a location and high-level inventory of all electronic data ready at the pre-trial conference. This rule removes any maneuvering room around producing instant messages, SMS messages, voicemail, or other forms of electronic data stored in less accessible locations, such as removable storage devices, USB thumb drives, digital camera memory, etc.

What does this mean for IT? IT will be called upon to quickly produce this detailed data mapping or inventory. Be proactive! Create the data map or inventory ahead of time and keep it up to date. Otherwise, your weekend could be appropriated for this last minute exercise.

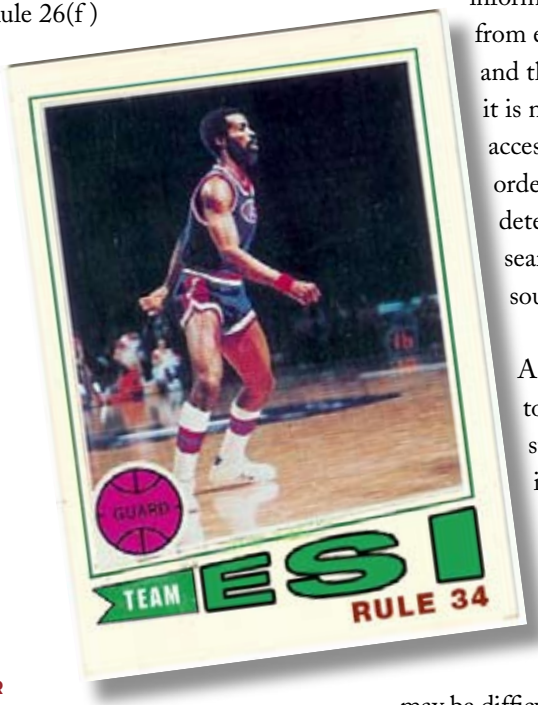
Rule 16(b)

This rule alerts the court and litigants to the possible need to address the handling of discovery of ESI early in the litigation process. Rule 16(b) is amended to invite the court to address disclosure or discovery of ESI in the Rule 16 scheduling order and gives the court discretion to enter an order adopting any agreements the parties reach for asserting claims of privilege or protection after inadvertent production in discovery.



Rule 26(a)(1)(C)

Rule 26(a)(1)(C) removes the long periods of time to respond that were commonplace before the new amendments were issued. Now, a party must make the initial disclosures at or within 14 days after the parties' Rule 26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in this action and states the objection in the proposed discovery plan. In ruling on the objection, the court must determine what disclosures, if any, are to be made and must set the time for disclosure.



What does this mean for IT? You must have your data map or data inventory ready up front. If you wait until you are asked for it, your chances of finding all responsive data are very low.

Rule 26(b)(2)(B)

Rule 26(b)(2)(B) clarifies the obligations of a responding party to provide discovery of ESI that is not reasonably accessible (deleted information, information kept on some backup tape systems, and legacy data from systems no longer in use). The amendment requires the responding party to identify the sources of potentially responsive information it has not searched or produced because of the costs and burdens of accessing the information. If the requesting party moves for production of such information, the responding party has the burden of showing the information is not reasonably accessible. If the responding party makes this showing, a court may order discovery for good cause and may impose conditions.

Any organization should first obtain and examine information that can be provided from easily accessible sources and then determine whether it is necessary to search less accessible sources (a court can order a sampling technique to determine the usefulness of searching the less accessible sources).

A party might be obligated to preserve information stored on sources it has identified as not reasonably accessible.

Rule 26(b)(2)(B) requires companies to know early on what ESI discovery may be difficult to produce, or expensive to produce, why, and identify it to other parties, with reasonable specificity.

Company representatives, including the corporate legal team, must now be knowledgeable of their corporate data infrastructure at the pre-trial meeting to discuss the eDiscovery plan.

What does this mean for IT?

To the court "inaccessible" does not mean "nevermind!" The term refers instead to the priority of data discovery. Data stores that are considered "accessible" are searched first. However, those deemed "inaccessible" could be discovered later. If that happens and your executives insist that "inaccessible" means can't be accessed, get them to put it in writing.

See CYA, page 34

Rule 34

Rule 34 explicitly recognizes ESI as a category of discoverable data. It also allows the requesting party to specify the form or format of data production—hard copy, native format, PDF, etc. A key provision of Rule 34 is to produce data in "a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."

Rule 34 allows for an agreement at the initial meet-and-confer between the parties regarding what form or format the responsive data will be produced. This agreement replaces the past practice providing requested ESI in formats difficult to use, such as hundreds of boxes of printed email.

What does this mean for IT?

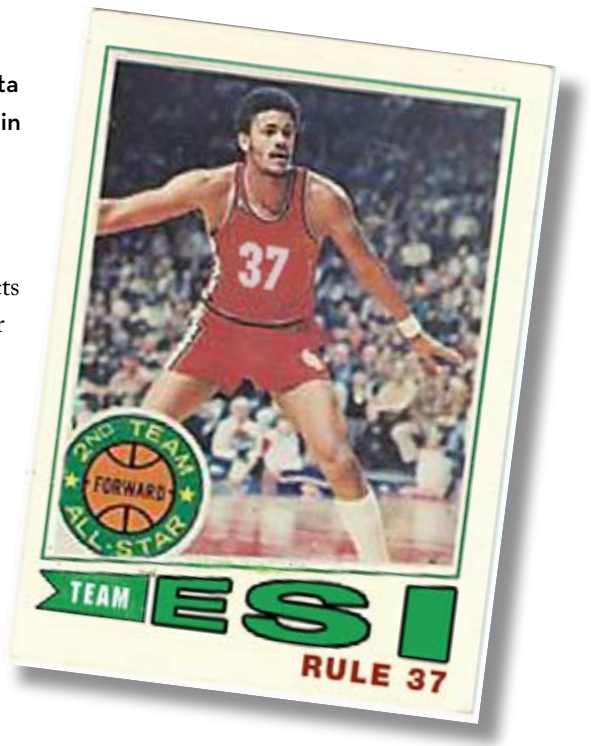
Simply put, secure and turn over all email, SharePoint, and file system and custodian data in the format you find it, wherever you find it in your infrastructure, including all metadata.

Rule 37(e)

Rule 37(e) creates a "safe harbor" which protects the discovered party from adverse sanctions for failing to provide ESI because of inadvertent loss due to "good faith" operation of the company's electronic infrastructure. For example, if the company initiates a litigation hold and takes other measures to preserve all potentially responsive ESI after it's been made aware of possible litigation, then it could claim safe harbor if responsive data is inadvertently lost or deleted. The key to claiming safe harbor is being able to show the court the company took several steps to ensure responsive data was not deleted or lost. This proof can take the form of existing data retention policies, formal litigation hold and discovery procedures, employee awareness campaigns, etc. In essence, Rule 37(e) obligates businesses to have a compliant records management program and litigation hold procedures, among other things, to show "good faith" and intent to be responsive to any discovery order.

What does this mean for IT?

Upon learning of possible litigation, IT has to be able to stop all deletions of responsive data immediately. This means preventing all employee deletions as well as automated system deletions of all potentially responsive records within minutes, if not seconds.



Order NOW!

As seen on TV!

Amaze your friends & colleagues!

LITIGATION DETECTOR!

Sally got fired on Friday?
Simply turn on the ALL-NEW LITIGATION DETECTOR and find out if she plans to sue your company… great fun at parties and corporate events!

- **Adjustable volume control**
- **Minimally invasive**
- **Available in black, silver, or red**

The Know-IT-All Quiz Question 3:

Which of the following constitutes notice of possible litigation?

A) The execs all suddenly move to Switzerland.

B) The janitor urinating on the copier.

C) The guy who got fired last week sues the company.

D) All of the above—and much, much more.

"I have to stop all ESI deletions when?" (When or what is considered notice of possible litigation?)

Amendment 37(e) is much debated in the legal community as a whole and dangerously misunderstood in the corporate legal community in particular. The FRCP Advisory Committee's comments to amended Rule 37(e) make it clear that any automatic deletion feature should be turned off and a litigation hold imposed once litigation can be reasonably anticipated. This begs the question: when can litigation be reasonably anticipated?

The answer is important. Recognizing possible impending litigation triggers your responsibility to secure and protect all potentially responsive records, both electronic and hard copy. The inadvertent destruction of such evidence would not be not be looked upon kindly by the court.

So, when is notice of a possible lawsuit given to a business entity? Say several employees are standing around the department coffee machine. Bob says to Jim; "Did you hear they fired Sally?" Jim responds; "Yeah, I spoke to her on Saturday, and she said she is thinking of hiring a lawyer." Is this notice of possible litigation for the company? Many lawyers and judges would say yes. This conversation should trigger the company's obligation to start protecting data for the possible discovery request.

Written documents are not the only notice of potential litigation. Notice can be verbal or even based on circumstances.

FCRP Rule 26(b) states: Every organization has "a duty to disclose all potentially relevant sources of information" to the courts as soon as they "reasonably anticipate" litigation, unless these sources are "not reasonably accessible because of undue burden or cost." This requirement puts the legal department between a server rack and a hard place. While not necessarily a problem for the IT organization, it is a good idea to at least be aware of the company's legal responsibilities.

The Testa v. Wal-Mart case provides another example of an unconventional form of notice. While delivering a shipment of live tropical fish to a Wal-Mart store, Louis Testa slipped on some ice on the loading dock and hurt himself. As he picked himself up, he spied a young "associate" near the loading dock door and yelled "I'm going to sue you guys!"

Case Study: Testa v. Wal-Mart

In the winter of 1993, Louis Testa, a truck driver for a tropical fish wholesaler, Heavenly Fish, drove his van up to a loading dock in the rear of a newly opened Wal-Mart store in Hinsdale, New Hampshire. Mr. Testa alerted Wal-Mart to his arrival, unloaded his shipment of tropical fish, and proceeded up Wal-Mart's delivery ramp. The ramp was coated with snow and ice, causing Mr. Testa to fall and hurt himself. As Mr. Testa was leaving, he threatened to sue Wal-Mart for his injuries. A Wal-Mart employee, presumably present on the loading dock, heard Mr. Testa's threat and made note of it in an internal report of the incident. In addition, Wal-Mart noted that an invoice clerk had put a hold on the order placed with Heavenly Fish for that day, which was the day of the store's grand opening. Wal-Mart had informed all vendors that it would not accept deliveries on that day, which is why Wal-Mart did not bother to clear the ramp of snow and ice that day. The invoice clerk also followed up with a phone call to Heavenly Fish confirming that deliveries were cancelled for that day.

Wal-Mart had a written record of the purchase order and phone call to Heavenly Fish. Wal-Mart had a two-year document retention policy, which it faithfully followed. Accordingly, two years after the incident involving Mr. Testa, Wal-Mart destroyed all its records relating to the incident, including the purchase order and phone record. Unfortunately for Wal-Mart, the statute of limitations in New Hampshire for personal injury exceeded two years. Shortly after Wal-Mart had destroyed its records consistent with its destruction policy, Mr. Testa filed suit. Wal-Mart defended against the suit by claiming Mr. Testa ignored Wal-Mart's explicit direction not to make deliveries that day.

During discovery, Wal-Mart was unable to produce either the purchase order to Heavenly Fish or the telephone records for the day Wal-Mart claimed it had cancelled the delivery. Wal-Mart testified that it had destroyed the records a few months before the lawsuit was filed but more than two years after the incident in accordance with a standard record retention policy.

During the trial of the matter, the court provided the following instruction to the jury regarding the documents Wal-Mart could not produce:

A reasonable inference is a deduction which common sense and reason lead you to draw from the evidence. An example is one inference that the plaintiff seeks to have you draw here is to the effect that the defendant, having known that a lawsuit was pending, destroyed certain records and did so because defendant knew the records to be harmful to its own case. But the law holds that such an inference can be drawn only if the plaintiff proves by a preponderance of the evidence that [the defendant] not only knew of the potential claim of the plaintiff, but also knew of the potential relevance of the destroyed documents. And even where plaintiff satisfies this burden of proof, any inference that may be drawn is permissive and may or may not be drawn by the jury.

After the jury awarded a verdict for the plaintiff, Wal-Mart appealed challenging the trial court's adverse inference instruction as improper. The Court of Appeals concluded that a rational jury

could have concluded that Wal-Mart was on notice of the plaintiff's claim because it had conducted an investigation and generated an internal accident report, which noted Testa's threat to sue, immediately after the accident occurred. The court also concluded that a rational jury could conclude that Wal-Mart was on notice of the relevance of the destroyed documents. In response to Wal-Mart's argument that there was no evidence that the Wal-Mart employee who discarded the records had any notice of Testa's claim or the relevance of the records to it, the court explained that only institutional notice – "the aggregate knowledge possessed by the party and its agents, servants, and employees"– was required for purposes of the adverse inference instruction Testa v. Wal-Mart Stores, Inc., 144 F.3d 173 (1st Cir. 1998).

The Testa case spotlights the perils of relying on a broad-based, general retention policy. Consistent application of Wal-Mart's two-year document retention policy was of no avail to Wal-Mart in the face of Testa's threat to sue and the three-year statute of limitations. Testa also underscores the need for companies to devise and implement early detection measures for potential lawsuits. A properly implemented record retention policy, which considers extended retention requirements due to potential lawsuits, will provide protection against sanctions for a business accused of destroying documents in the face of litigation. However, the policy must be consistently and universally implemented and may not be used merely as an excuse for the destruction of pertinent records.

(Excerpted from the paper: E-mail Retention: How Much Risk Can You Afford? *by William F. Savarino, Esq. of Cohen Mohr LLP, 2003.)*

Is that threat notice to the Wal-Mart corporate entity? The judge in New Hampshire thought so. It should have triggered Wal-Mart's duty to apply a litigation hold (which they didn't do) on all records, including emails, video surveillance, employee access card records, etc. that could become evidence in the upcoming litigation. Other examples of "reasonable anticipation" include situations where a reasonable person would conclude litigation is a possibility sometime in the future. Take the following situation: Due to the current economic crises, a company of 98 employees decides it needs to lay off 20 percent of its workforce. Should the company assume and plan for potential litigation from these layoffs? Absolutely. Generally speaking, litigation should be anticipated in the wake of employee layoffs.

What does it mean for IT?

Once your corporate legal department acknowledges pending litigation, it will direct IT to start collecting and securing data. The gap between when a company should have reasonably anticipated litigation and when they actually do can (and often is) used by opposing counsel to charge companies with destruction of evidence.

The Know-IT-All Quiz Question 4:

Locating specific ESI is like trying to find:

A) Kickboxing on the Lifetime Channel.

B) Meaning at the bottom of the next bottle.

C) A girlfriend on craigslist.

D) Your lunch in the office fridge—somewhere behind the birthday cake and Jim's Hot Pocket™ from last week.

Searching for ESI is like looking through the office fridge: There's more in there than you'd expect

Rule 34, in the new Federal Rules of Civil Procedure (FRCP), specifies electronically stored information (ESI) is a discoverable format in the litigation process. Since approximately 95 percent of the information generated and received in a company's day-to-day business is electronic, this amendment created a gigantic increase in data sources that must be searched and protected in litigation.

The average 1 GB USB thumb drive can hold upwards of 75,000 pages of data. The average email box (including PSTs) could be hiding hundreds of thousands—even millions—of individual emails and attachments.

Do you know how much data you have sitting in your email system, in your SharePoint system, on your file and print servers, on backup tapes, on employee hard disks, on CD/DVDs, on USB thumb drives, etc.?

A company's responsibility to fully respond to a discovery request is absolute. There must be a good faith attempt to find all requested data. If the discovery process is incomplete or suspect, a company can lose a case before it even gets to court. If you have never been through the process, you may not be aware of the systems and areas that could be subject to a discovery search.

TO BE CONSIDERED A FULLY-RESPONSIVE SEARCH CONDUCTED IN GOOD FAITH, YOUR LIST MAY INCLUDE THE FOLLOWING:

- Email servers and attached storage
- SharePoint servers and attached storage
- File and print servers and attached storage
- Share drives
- Server log files
- Server RAM
- Backup tapes or backup targets
- External storage facilities
- Failover sites
- Hosted archive sites
- Employee workstations
- Employee external hard disks
- Employee CDs
- Employee DVDs
- Employee USB thumb drives
- Digital camera memory
- iPods/PDA
- Cell phones
- Corporate blogs
- Corporate web sites
- 3rd party infrastructure
- Employee personal computers
- Employee external email accounts

Not common, but sometimes these need to be searched too.

Consider that list and ask yourself if you could perform a thorough search and then certify to the court that you have retrieved all records and data relevant to a specific discovery request…in a matter of weeks. Some corporate General Counsels (GCs) argue that only the most obvious repositories need to be searched to satisfy an ESI discovery request. Legally speaking, this is absolutely false. Failing to search all possible repositories can greatly increase a company's risk of being charged with destruction of evidence.

When performing an eDiscovery search or placing a litigation hold, it's a good idea to pair a member of your legal staff with an IT employee to insure procedures are followed. This measure will also protect both employees should they be called into court to explain how the discovery was accomplished. Even better, the legal department can perform the discovery themselves if your company has a centralized archiving system. Not surprisingly, IT prefers this solution, in part because it reduces the chance of their employees being subpoenaed.

Ensure your backup tape recycling period is shorter than your published retention policies. This practice removes backup tapes as a discoverable target.

PLANNING FOR eDISCOVERY

To improve your response time and reduce your company's legal risk, you need to be fully prepared for eDiscovery. There are two main ways to achieve this. The most comprehensive strategy is to put proactive ESI archiving solutions in place to capture all potentially responsive data in real time, apply retention policies to it, and index it for easy search and retrieval.

An extreme example of not finding all requested data after a company had certified complete compliance to the court is the Colman v. Morgan Stanley case.

In this case, Morgan Stanley time and time again told the court they had found all responsive emails on their backup tapes, even though they kept finding more backup tapes in closets, under desks, and so on. The judge finally tired of this and issued an adverse inference instruction to the jury—meaning the jury can assume that Morgan Stanley either destroyed or refused to turn over the requested records because it would have had a negative impact on their defense. Morgan Stanley lost the case to the tune of $1.45 billion dollars.

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005)

If an investment in capital equipment is not feasible, a second strategy is for IT to create and manage an enterprise-wide data map. A data map is essentially an inventory of all of the company's ESI records. It should describe the records—by business unit and custodian, if appropriate—and specify the various types of electronic media on which the records are maintained.

WHAT DOES THIS MEAN FOR IT?

eDiscovery and/or a litigation hold will throw an unprepared IT department into complete chaos. You may have to search through your entire infrastructure—including employees' local hardware—in a very short time. Planning for this eventuality will greatly reduce your risk as well as reduce your response time. Install a fully indexed and searchable ESI archive or create a data map.

THE USUAL SUSPECTS

The Know-IT-All Quiz Question 5:

Which employees should be included on the cross-departmental eDiscovery team?

A) Tim, for sure. He always brings donuts.

B) The accountants, even though I've heard they eat paste.

C) Anyone with a C_O in their title, because they pay our salaries.

D) Legal, IT, Finance, Accounting, HR, and the CFO.

Now it's a party.

A CEO, a marketing manager, and an email admin walk into a bar… (eDiscovery involves many departments, not just IT)

Corporate civil litigation rarely affects only the legal department. A discovery request can and does affect many, if not all, departments. The most obvious department in the crosshairs is IT, mainly because legal assumes that IT controls and has immediate access to all stores of buried information. This, of course, is often not the case. IT usually has a general idea of the data stores they manage within the corporate infrastructure. But a huge amount of potentially discoverable data is controlled by employees directly. Asking IT personnel alone to search for and retrieve all responsive data places an undue burden on that department.

A team approach to eDiscovery will lower your discovery costs as well as your legal risk. Much of the cost of discovery is directly related to finding all the requested data, wherever it may be. Unprepared companies perform inefficient searches—disrupting employee productivity, searching the same data store many times, and looking at employee data not part of the discovery request. Such inefficiency increases a company's risk of not finding all data requested or adversely turning over too much data.

Proactively creating and training an eDiscovery team will greatly reduce costs and risks as well as help IT when unexpected litigation arises. Let's start with these:

THE FOLLOWING ROLES ARE IMPERATIVE TO HAVE ON THE TEAM:

- **A "C" level sponsor, such as the General Counsel, Chief Information Officer, or Chief Financial Officer.** This key executive has a direct line of communication to the Board of Directors, the executive committee, or the CEO and can therefore secure buy-in from senior management and get budgets approved.
- **A senior member of the legal staff** who represents the legal priorities of the team and insures all legal responsibilities are followed.
- **A senior IT representative** with in-depth knowledge of the corporate network's protocol and procedures, a thorough understanding of the corporation's IT infrastructure, and historical knowledge of how the network was constructed and maintained (or is at least privy to the history and able to access it conveniently and quickly).

• A member of the finance department who can track discovery expenses and help build financial business cases when new technology and services are required.

Depending on your circumstances and the size of your organization, you may chose to add team members from the following functions. If you do not add these members, be sure that these functions are nevertheless covered by the existing team.

- **Investor relations**
- **Human resources**
- **Records management**
- **Accounting**
- **Risk management**
- **Purchasing**
- **Engineering**

Create a cross-departmental eDiscovery team to take some of the burden off the IT group.

Creating the eDiscovery Team (from the IT point of view)

STEP 1: Get buy-in for the creation of the team from the CEO or Board of Directors. If needed, have the CEO appoint an executive-level sponsor.

STEP 2: Find a member of the legal department who is knowledgeable about the amended Federal Rules of Civil Procedure (FRCP). This may be more challenging than you might expect. Many companies employ outside law firms to handle actual litigation, so legal staff members may not be conversant on the subject. If none are available, consider hiring an eDiscovery consultant.

STEP 3: If you are not the right IT representative, find an IT resource who can and wants to work closely with the legal representative, is knowledgeable about the IT infrastructure, and understands legal points.

STEP 4: Have the legal team member educate the team on the basics of eDiscovery, the company's legal obligations, and the company's current litigation hold process and discovery procedures.

STEP 5: Have the IT member educate the team on the corporate data infrastructure.

STEP 6: Have the IT team member and the records management team member create a corporate infrastructure data map—an inventory of all of the corporate data-producing hardware, applications, storage repositories, files, number of copies, applications that automatically delete files, etc.

STEP 7: Have the records management member insure that the existing records retention policies have been updated and are being followed—or, if the policies don't already exist, begin the process of creating them with help from legal.

STEP 8: Have the team develop or update the company's litigation hold and eDiscovery procedures, including forms, chain of custody, and documentation instructions for every step of the process. Train all employees on these procedures.

STEP 9: The legal team member needs to keep up to date on new legal requirements, new case laws and so on, and communicate this information to the team.

Your unemployed brother-in-law is probably not the best choice for this

eDiscovery Team Building in NINE EASY STEPS

What does this mean for IT?

Building a cross-departmental eDiscovery team will relieve much of the burden from IT, while also creating the opportunity for all affected departments to share ideas and address requirements. In fact, IT's own requirements—for automated systems to better respond to discovery requests, for instance—will become apparent across the board and reach senior levels through these conduits. An effective eDiscovery team can lead your company smoothly through the nightmare of civil litigation and help avoid significant hardships in the form of fines, bad press, and other penalties.

The Know-IT-All Quiz Question 6:

Applying a litigation hold is:

A) A sure-fire way to win a professional wrestling match.

B) Like suffering through your niece's violin recital.

C) A persistent ache, like adolescence with acne.

D) A debilitating condition, like a workday hangovers.

A litigation hold is like being hungover at work– you just can't focus on anything else

One of the principal rules of the amended Federal Rules of Civil Procedure (FRCP) is whenever litigation is reasonably anticipated, threatened, or pending against an organization, that organization has an immediate duty to preserve relevant information.

This duty to immediately preserve potentially responsive data includes the obligation to identify, locate, and secure all data potentially relevant to the case. When preservation of electronically stored information (ESI) is required, most of the time this duty to preserve obviously overrides any records management policies that would otherwise result in the deletion of ESI. Always be aware this duty also pertains to any systems automatically deleting data without human intervention.

A litigation hold duty triggers immediately when litigation can be reasonably anticipated.

Under Rule 37 of the amended (FRCP), a party that violates a litigation hold or otherwise fails to produce requested data will be exposed to a range of sanctions, including a spoliation/destruction of evidence judgment. However, FRCP Rule 37 also provides that a court may not impose sanctions on a party for failing to provide ESI lost as a result of the routine, good-faith operation of an electronic information system. This is known as the "Safe Harbor" rule (see Chapter 9).

Litigation Hold Guidelines: (from the Sedona Conference Commentary on Legal Holds 2007)

1. Reasonable anticipation of litigation arises when an organization is on notice of a credible threat that it will become involved in litigation or anticipates taking action to initiate litigation. Having a data map to reference will help in determining what items exist, where they are, etc. for a litigation hold. It also shows "good faith intent" for the "Safe Harbor" defense.

So what qualifies as "reasonable anticipation"? Here's an example: A Chief Financial Officer of a company reads a news story about the Securities Exchange Commission launching an investigation into specific industries in regards to the backdating of employee options…and your company's industry is on the list. Under these circumstances, a government investigation (and possibly litigation) can reasonably be anticipated and a preservation obligation has arisen.

Another example in which reasonable anticipation would apply is when your company lays off a substantial number of employees. Most HR managers would foresee potential wrongful termination litigation on the horizon.

2. One factor demonstrating reasonableness and good faith in meeting preservation obligations is the adoption and consistent implementation of a litigation hold policy defining a document retention decision-making process.

An interesting example of how a litigation hold policy can reduce your risk of spoliation would be if your Investor Relations VP receives an anonymous threat to sue with little or no support accusations. The Investor Relations VP consults your existing and updated litigation hold policy, which has very specific descriptions of issues that would result in a litigation hold. Based on the policy, the VP concludes that the company should not reasonably anticipate litigation. In this example, the company is able demonstrate it had a policy which it followed in accessing the potential threat. Even if later litigation arises, a spoliation claim by the plaintiff should be dismissed by the court based on Rule 37.

3.Another factor demonstrating reasonableness and good faith in meeting preservation obligations is the use of established, tested procedures for the reporting of information relating to a potential threat of litigation to a responsible decision maker.

Simply put, your company should train all employees to contact the legal department when they read or hear anything that could point to anticipated litigation.

4. The determination of whether litigation is reasonably anticipated should be based on good faith, reasonableness, a reasonable investigation, and an evaluation of the relevant facts and circumstances.

5. When a duty to preserve arises, reasonable steps should be taken to identify and preserve relevant information as soon as is feasible. Depending on the circumstances (e.g. do you have the ability to find all responsive data centrally via a real-time archive?) a written legal hold should be issued, which includes a preservation notice to persons likely to have relevant information.

6. To determine what data should be placed on litigation hold, consider the nature of the issues raised, previous experience in similar circumstances, and the amount in controversy.

7. To be effective, a manual litigation hold must identify the persons who are likely to have relevant information.

• Issue a written communication to those persons clearly defining what information is to be preserved and how the preservation is to be undertaken.
• Be reviewed periodically and, when necessary, reissued in either its original or amended form.

8. The litigation hold policy and its implementation process should be documented because both the policy and process may be subject to scrutiny by the opposing party and review by the court.

9. The implementation of a litigation hold should be regularly monitored to ensure compliance.

10. The litigation hold process should include provisions for the release of the hold upon the termination of the matter at issue. Ideally, a manager should be identified for each process who can answer all parties' questions and communicate periodic updates, including—finally—the termination announcement.

The Know-IT-All Quiz Question 7:

Spoliation is a term used to describe what happens when:

A) The moment you realize your prom date is actually a man. No wonder she was taller than you.

B) Your recently-rehabbed best friend brings "Near Beer" to the Superbowl party.

C) Wednesday's Chinese food converts to a two-hour trip to the toilet.

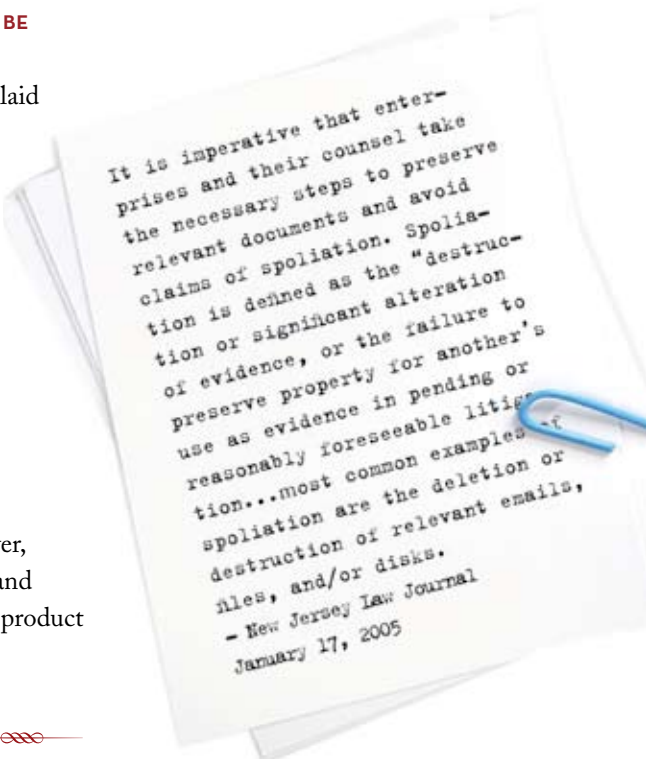
D) A party in a legal proceeding intentionally or negligently withholds, hides, alters, or destroys relevant evidence.

Spoliation is not what happens to last week's Chinese food.

Spoliation is the intentional or inadvertent destruction, mutilation, concealment, or alteration of evidence. A misplaced record, either electronic or hard copy, can affect the outcome of litigation and redirect liability. That's because a spoliation decision can result in an "adverse inference" instruction to the jury, who are free to conclude that the missing evidence was detrimental to the party responsible for it. Some consider being found guilty of spoliation to be the last nail in the coffin. If this happens to you, you can stop worrying about whether or not you'll lose the case and start wondering what it's going to cost you.

SPOLIATION IS THE INTENTIONAL OR ACCIDENTAL DESTRUCTION OF RECORDS THAT MAY REASONABLY BE REQUESTED BY OPPOSING COUNSEL.

Here are a few quick examples spoliation charges laid against defendants in actual court cases:

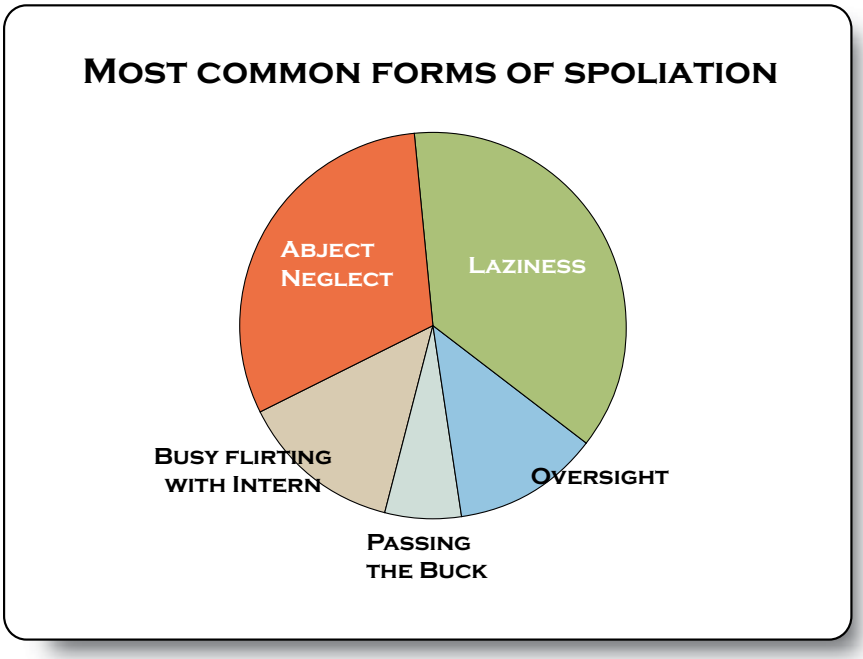


Case 1: An Intellectual Property Theft Case

Defendant was ordered not to alter any information on the company's computers. However, numerous files containing relevant information were subsequently deleted and later recovered from the Windows recycle bin.

Case 2: A Product Liability Case

Defendant was ordered to preserve emails related to the product in question. Within a week, however, emails exchanged between product development and senior management discussing the dangers of the product were deleted.



Case 3: An Insurance Fraud Investigation

Defendant loses the case when investigators recovered a deleted internet browser history revealing that Google searches had been performed on such incriminating topics as "how to burn a house" and "how long to collect insurance money."

The only way to guarantee ESI will not be deleted is to take the control away from the employees.

Given how easy it is to accidentally delete records and how difficult it is to convince the court you are not responsible for spoliation, the importance of having a tested litigation hold procedure is abundantly clear. That's the only way to quickly stop ESI deletions by your infrastructure as well as by your employees.

A spoliation of electronically stored information (ESI) decision can result from a number of routine actions and automated processes in your day-to-day business:

- Re-use of backup tapes
- Continued use of applications that automatically delete data after a litigation hold has been applied
- Deletion of email by employees
- Deletion of SharePoint files
- Practice of writing over files on a USB thumb drive
- Disposal of data CDs or DVDs

What does this mean for IT?

The most obvious way to control deletions of ESI is to capture all potentially discoverable data in a centrally-managed archive in near real time. If such a system were in place, employees would not be able to delete archived data. By capturing and managing ESI centrally, you can have a single point of eDiscovery.

The Know-IT-All Quiz Question 8:

The phrase "Safe Harbor" refers to:

A) A movie starring Gregory Harrison about a widowed sheriff and his three sons living with his mother in a motel she owns.

B) A financial consulting firm, specializing in the sale of life insurance annuities.

C) An exemption, in patent law, to the rights conferred by patents, which is especially relevant to drugs.

D) A provision of a statute or regulation that reduces or eliminates a party's liability under the law, on the condition that the party performed its actions in good faith.

E) All of the above, technically, but (A) to (C) are way off topic.

cover your ass

Safe Harbor is the truest form of CYA: Understanding FRCP Rule 37(e)

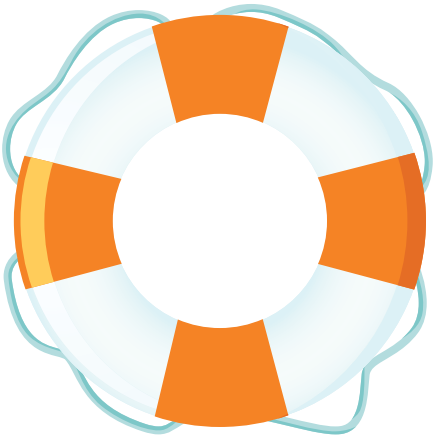
Having a top-notch CYA process is, as Martha Stewart says, "a good thing." (Shame this book was not circulating in time to save her some hard time!) Buried in the new Federal Rules of Civil Procedures (FRCP) amendments is Rule 37(e), otherwise known as the "Safe Harbor" amendment. This new rule protects parties in litigation from sanctions if potentially responsive data (evidence) is inadvertently altered or deleted. Rule 37(e) states:

Absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

Before considering what qualifies as a "routine, good faith operation," you should be aware of the discretionary controls (those which are not centrally controlled) within your infrastructure. For example, most corporate computer applications are not designed to archive data —that is, to store it for extended periods of time. It follows, then, that corporate email systems generally do not control what employees do with the data in their mailboxes, so employees can move it out of the email system or delete it at will. This makes data preservation difficult, if not impossible.

To effectively utilize a CYA strategy, your organization must be able to document that they have taken all reasonable steps to insure potential evidence is not lost. This means that your organization needs to put policies, procedures, data maps, training, and automation in place in order to have a prayer of getting protection under the Safe Harbor amendment.

It is important to note the new rules do not necessarily impose additional obligations to save that which cannot reasonably be saved without disrupting or crippling business operations. That's where the "routine, good faith" standard comes in. Many corporate data systems operate under settings chosen by the user or administrator to govern time periods and volume thresholds—such as mailbox limits that prompt users to delete, overwrite, or store email and attachments. This discretionary process is reflected in the language of Rule 37. These settings, and how they are treated, are potentially subject



to hindsight analysis by the court to determine whether the party allowed deletion to occur in the "good faith operation of an electronic information system" or whether something is amiss under the circumstances. In most cases, the court will presume that, as the owner and administrator of your applications, you are expert in their operation and should know when data deletions need to be suspended. Therefore, to claim Safe Harbor, you must demonstrate you have taken all necessary steps to insure data loss doesn't happen. This way, if potential evidence is lost or deleted, you are far less likely to be held responsible.

What's needed for 37(e)

First of all, to accurately evaluate your risk, you need to understand how the data in your infrastructure is generated, managed, and expired. Answering the following questions can help the IT department create and routinely update a comprehensive data map:

- **What systems are in place?**
- **What applications are running?**
- **What types of data are generated?**
- **How many copies are produced?**
- **Where are the copies stored?**
- **Is there automatic deletion of some data?**
- **How are automatic deletions halted?**
- **What applications and data are controlled by employees?**
- **Where can employees store data?**

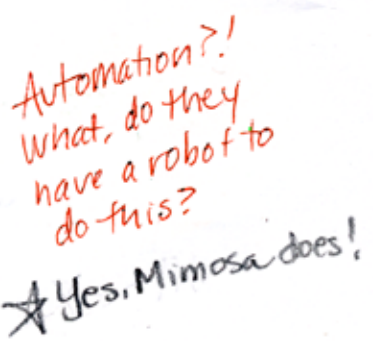
Secondly, you need to create a litigation hold procedure that defines what should happen once your legal department alerts you to potential or pending litigation. When it comes to using the Safe Harbor defense, it goes a long way to have a documented litigation hold procedure that has been approved by your legal department.

Thirdly, you need to make your employees fully aware of your litigation hold procedure and train them on their related responsibilities. This means more than simply adding a paragraph to the new employee "warm welcome" packet. In fact, to meet the Safe Harbour requirements, you should offer in-person or web-based training sessions and periodic refresher sessions—all of which should be fully documented.

Finally, you need to consider litigation support automation—an archive system that captures, indexes, single instances, applies retention policies, and secures all or most discoverable ESI. Automating these functions will dramatically reduce your risk of spoliation and the costs associated with applying litigation holds and complying with eDiscovery requests.

What does this mean for IT?

You must have a deep and comprehensive understanding of your corporate infrastructure and the data it generates and manages. This includes data that employees have direct control over.



STARGATE
Season 1 (1997-1998)
101 Children of the Gods (1 & 2)
102 The Enemy Within
103 Emancipation
104 The Broca Divide
105 First Commandment
106 Cold Lazarus
107 The Nox
108 Brief Candle
109 Thor's Hammer
110 The Torment of Tantalus
111 Bloodlines
112 Fire and Water
113 Hathor
114 Singularity
115 Cor-Ai
116 Enigma
117 Solitudes
118 Tin Man
119 There but for the Grace of God
120 Politics (1)
121 Within the Serpent's Grasp (2)

Season 2 (1998-1999)
201 The Serpent's Lair
202 In the Line of Duty
203 Prisoners
204 The Gamekeeper
205 Need
206 Thor's Chariot
207 Message in a Bottle
208 Family
209 Secrets
210 Bane
211 The Tok'ra (1)
212 The Tok'ra (2)
213 Spirits
214 Touchstone
215 (217) A Matter of Time
216 The Fifth Race

The Know-IT-All Quiz Question 9:

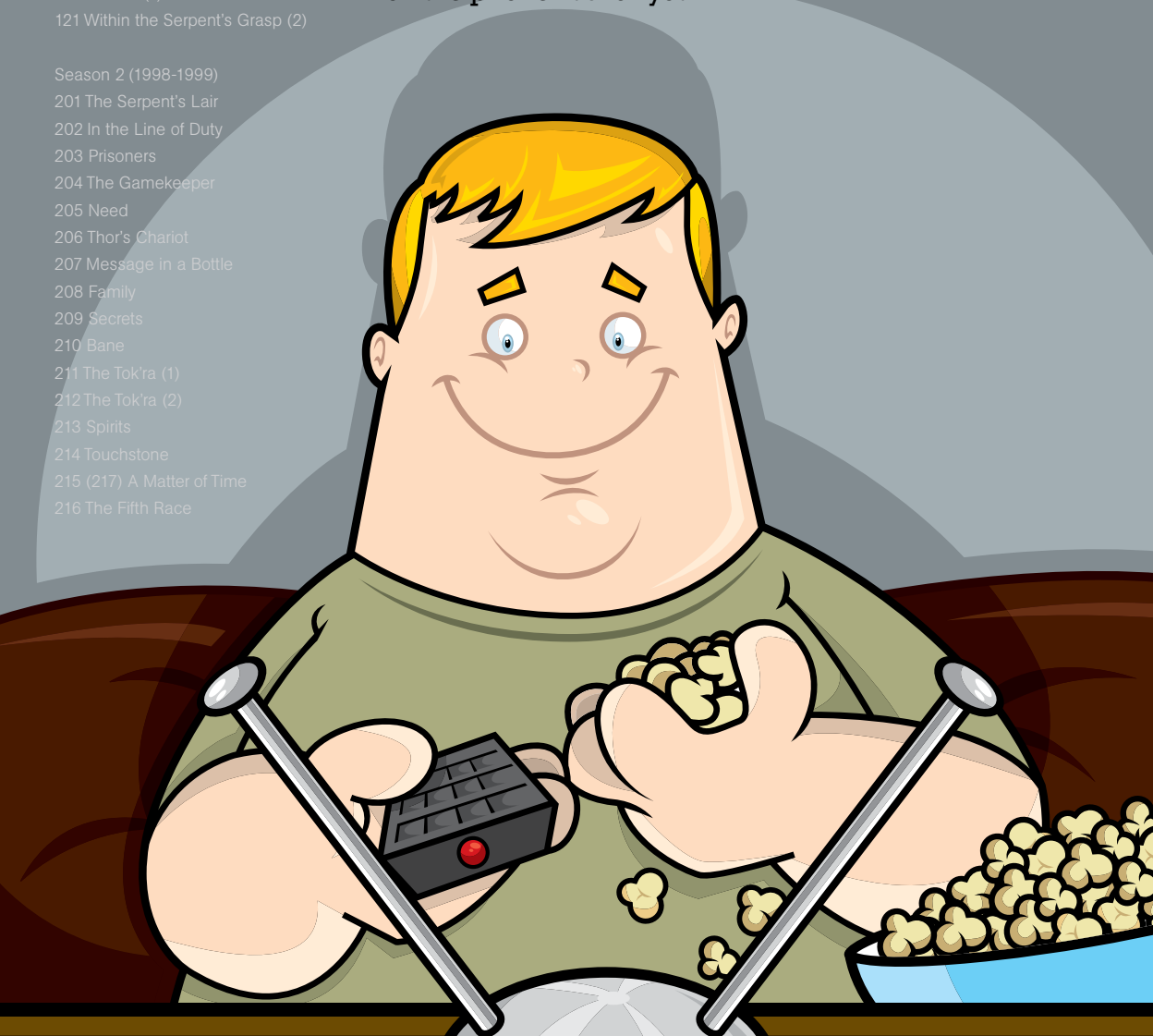
Which of the following "Stargate" trivia questions is too easy to submit to the fan site?

A) In the 1994 movie *Stargate*, who played the role of Dr. Daniel Jackson—a brilliant Egyptologist whose farfetched theories about pyramids led to his participation in the original mission?

B) Who left his home planet of Langara after witnessing Dr. Jackson's deadly sacrifice and the resulting celebration of his planet's leaders?

C) The season 8 episode "Citizen Joe" features a guest appearance by which actor? (Hint: he voices a character in *The Simpsons*)

D) Funny you think you have time for this. Legal's on the phone. It's for you.



Proactive planning for eDiscovery ensures you won't miss the Stargate SG1 weekend marathon

Planning for eDiscovery is essential. If you are unprepared, a request can certainly ruin your weekend. And the weekend after that. And so on. The most onerous task for IT is finding and securing all potentially responsive data. You'll be guided in this task by an interrogatory. Never heard of it? It's the stuff nightmares are made of. Read on.

You or your co-workers can and probably will be questioned by opposing counsel about your infrastructure…be prepared.

Interrogatories

Interrogatories are written questions asked by the opposing counsel to discover key facts about your party's case. IT, in particular, can expect detailed questions about the corporate infrastructure. The following list includes general topics and related questions IT may have to answer in responding to an interrogatory.

Topic 1: Information Technology (IT) & Information System (IS) Personnel

1. List all IT and IS personnel and technical staff that is or has been responsible for managing and maintaining the technology infrastructure of [Plaintiff / Defendant] for the period _____ to _____, including, but not limited to desktop computers, servers, personal digital assistants (PDAs), portable computers, laptop computers, and other electronic devices. Include contact information such as full name, job position, job description, and list of duties.
2. List employees formally or loosely assigned to subgroups within the IT and IS departments, such as network engineering, software development, emergency response, quality assurance, and troubleshooting.

Topic 2: Network Architecture

1. Describe any and all groups of connected computer systems that permit users to share information and transfer data, including, but not limited to local area networks (LANs), wide area networks (WANs), client-server networks, virtual private networks (VPNs), and storage area networks (SANs).
2. List any and all components and network resources that establish and maintain the network environment, including, but not limited to, routers, switches, hubs, bridges, firewalls, and proxies.
3. Describe any and all third-party connectivity between the computer systems and network environment of [Plaintiff / Defendant], including the type of information shared, manner in which information is transferred, and contact lists of internal and external individuals who have authorization to transfer information into or out of [Plaintiff / Defendant] network environment.

Topic 3: Computer Hardware

1. Identify each computer system that is or has been used by employees for the period _____ to _____, including, but not limited to, desktop computers, servers, personal digital assistants (PDAs), portable computers, laptop computers, and other electronic devices. Include descriptions of equipment and any peripheral technology attached to the computer system.
2. Describe the Internet and intranet connectivity of each computer system, including, but not limited to, client-server communications and client-client communications facilitated through modem, network, or direct connection.
3. List all hardware or software modifications made to computer systems in use during the period _____ to _____, including, but not limited to, dates of modifications, software and hardware titles, version numbers, contact information of IT or IS personnel performing the modification, and location of data backups taken prior to modification.
4. Identify any and all specific computer systems that have been used to create, modify, or store electronic information relevant to this legal matter.

Topic 4: Computer Software

1. List all operating systems installed on all computer systems in use by [Plaintiff / Defendant], including, but not limited to, Microsoft Windows, Linux, UNIX, DOS, etc.
2. List the title and version number of any and all software installed or executed on the computer systems used by [Plaintiff / Defendant] during the period ____ to _____.

Topic 5: Electronic Mail Communication

1. Describe all server- and workstation-based software in use or used to facilitate the transmission of email during the period ____ to _____.
2. Identify all hardware in use or used to facilitate the transmission or storage of email during the period ____ to _____.
3. List all email accounts in use during the period ____ to _____.
4. Describe the policies, procedures, and technology employed to backup and archive email messages during the period ____ to _____.
5. Describe any email-based encryption algorithms in place.
6. List all emails, senders, and recipients of email currently known to be relevant to this legal matter.

Topic 6: Data Backups, Archives, and Removable Media

1. Describe the policies and procedures governing the use of removable media, such as CD-ROMs, zip disks, floppy disks, tape drives, removable hard drives, etc., associated with [Plaintiffs / Defendants] computer systems or network.
2. Describe the policies and procedures for performing data backups on all computer systems as well as the hardware and software employed during the period ____ to _____.
3. List any and all removable media utilized to store data during the period ____ to _____.
4. List all IT and IS personnel responsible for conducting data backups and the archiving of electronic information during the period ____ to _____.
5. Identify all removable media known to contain information relevant to this legal matter.

Topic 7: Telephone System

1. Describe the elements of your telephone and voice messaging system, including all hardware, software, and third-party service providers.
2. Identify any and all voice messaging records for [Name] during the period ____ to _____, including, but not limited to, caller message recordings, voice recordings, computer voice mail files, outgoing voice recordings, unified messaging files, etc.
3. Identify any and all telephone use records for [Name] during the period ____ to _____, including logs of outgoing and incoming calls.

Topic 8: Miscellaneous Sources for Electronic Evidence

1. Describe any and all network, server, and workstation-based log files generated during the period ____ to _____.
2. Describe the policies and procedures governing employee use of Internet newsgroups, chat rooms, or instant messaging on [Plaintiffs /Defendants] computer systems.
3. List any and all portable electronic devices owned and operated by [Name] but used in the performance of his/her employment with [Plaintiffs / Defendants].

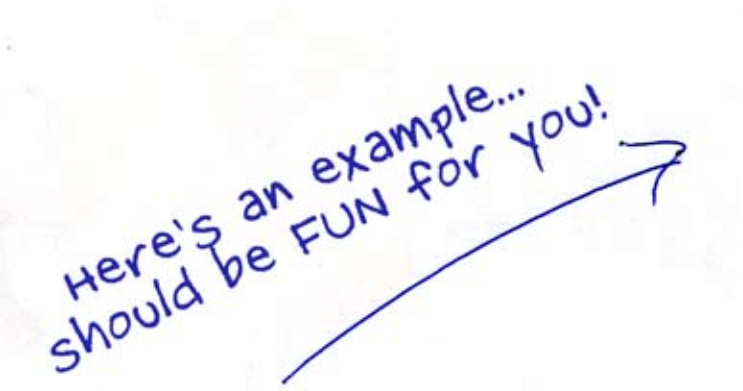
Topic 9: Destruction of Information

1. Describe the policies and procedures pertaining to data retention and list all information scheduled for deletion during the period ____ to _____.
2. Describe all hardware or software utilized to facilitate the deletion of data subject to data retention policies and procedures.
3. List any and all servers, workstations, or electronic devices that have had their hard drives reformatted or replaced during the period ____to _____.
4. Identify any and all information deleted, physically destroyed, corrupted, damaged, lost, or overwritten, either pursuant to the data retainer policies and procedures or not, relevant to this legal matter.
5. Identify any and all information deleted, physically destroyed, corrupted, damaged, lost, or overwritten, either pursuant to the data retainer policies and procedures or not, that took place since the initiation of this legal matter.[4]

Interrogatories are part of the pre-trial discovery stage of a lawsuit and must be answered under penalty of perjury. Court rules tightly regulate how, when and how many interrogatories can be asked. Lawyers can write their own sets of questions or can use form interrogatories designed to cover typical issues in common lawsuits.

eDiscovery requests usually target three main areas:

- **Specific employees**
- **Specific date ranges**
- **Specific content**



URGENT

To: You, our IT guy
From: Legal, on behalf of evil litigators
Date: Today
RE: eDiscovery Request: URGENT. Cancel all social engagements you may have in the near future

1. Produce all documents and electronically stored information that you referred to, relied upon, consulted, or used in any way in answering each interrogatory set forth in [party name] Interrogatories dated _____.

2. Produce organization charts for all of your Information Technology or Information Services departments or divisions during the period of [date] to the present time.

3. Produce all written policies, procedures, guidelines, or records developed by or used by you for your computers, computer systems, electronic data, or electronic media, during the period of [date] to the present time.

4. Produce all written policies, procedures, guidelines, or records developed by or used by you for backup or emergency restoration of electronic data, including backup tape rotation schedules, during the period of [date] to the present time.

5. Produce all written policies, procedures, guidelines, or records developed by or used by you for electronic data retention, preservation, and destruction, including any schedules relating to those procedures, during the period of [date] to the present time.

6. Produce all employee-use policies developed by or used by you for company computers, data, and other technology, during the period of [date] to the present time.

7. Produce all written policies, procedures, guidelines, or records developed by or used by you for file naming conventions and standards, during the period of [date] to the present time.

8. Produce all written policies, procedures, guidelines, or records developed by or used by you for password, encryption, or other security protocols, during the period of [date] to the present time.

9. Produce all written policies, procedures, guidelines, or records developed by or used by you for labeling standards for diskette, CD, DVD, or other removable media.

10. Produce all written policies, procedures, guidelines, or records developed by or used by you for email storage conventions (e.g., limitations on mailbox sizes/storage locations; schedule and logs for storage) during the period of [date] to the present time.

URGENT

11. Produce all written policies, procedures, guidelines, or records developed by or used by you for electronic media deployment, allocation, and maintenance procedures for new employees, current employees, or departed employees, during the period of [date] to the present time.

12. Produce all written policies, procedures, guidelines, or records developed by or used by you for software and hardware upgrades, including patches, during the period of [date] to the present time.

13. Produce all written policies, procedures, guidelines, or records developed by or used by you for personal or home computer usage for work-related activities during the period of [date] to the present time.

14. Produce all backup tapes containing email and other electronically stored information related to this action during the period of [date] to the present time.

15. Produce exact copies (i.e., bit-by-bit copies) of all hard drives on the desktop computers, laptop computers, notebook computers, personal digital assistant computers, servers, and other electronic media related to this action, used by [name], during the period of [date] to the present time.

16. Produce exact copies (i.e., bit-by-bit copies) of all relevant disks, CDs, DVDs, or other removable media containing electronically stored information created, reviewed, or received by [name] related to this action during the period of [date] to the present time.

17. Produce copies of all database files, email, or other files maintained on servers or mainframe or minicomputers, containing electronically stored information created, reviewed, or received by [name] related to this action during the period of [date] to the present time.

18. Produce exact copies (i.e., bit-by-bit copies) of all data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [name] related to this action during the period of [date] to the present time.

19. Produce all documents relating to costs and fees billed to you by any computer forensic examiner or other third-party technology provider with respect to the data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [name] related to this action during the period of [date] to the present time.

URGENT

eDiscovery Request. Page 3/3

20. Produce all documents relating to the terms of any agreement to provide services by any computer forensic examiner or other third-party technology provider with respect to the data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [name] related to this action during the period of [date] to the present time.

21. Produce all documents relating to the hash of any drive image created by any computer forensic examiner or other third-party technology provider with respect to the data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [date] related to this action during the period of [date] to the present time.

22. Produce all documents relating to the original drive hash with respect to any drive image created by any computer forensic examiner or other third-party technology provider with respect to the data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [name] related to this action during the period of [date] to the present time.

23. Produce all documents relating to the chain of custody with respect to any computer drive examined or copied by any computer forensic examiner or other third-party technology provider with respect to the data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [name] related to this action during the period of [date] to the present time.

24. Produce all documents, reports, and conclusions relating to the forensic analysis of any computer drive examined or copied by any computer forensic examiner or other third-party technology provider with respect to the data that was stored, retrieved, downloaded, restored, reconstructed, removed, deleted, salvaged, regenerated, and/or forensically extracted from the computer devices used by [name] related to this action during the period of [date] to the present time.

The above eDiscovery request is an example of a standard form published by the ABA and found in the book: The Electronic Evidence and Discovery Handbook *written by Sharon D. Nelson, Bruce A. Olson, and John W. Simek.*

Imagine how long and hard your IT department would have to work to respond to a similar eDiscovery request (to the satisfaction of the courts) within the tight timeframes usually allotted.

The only way to respond to this type of eDiscovery request, as shown previously, is to have proactively planned for answering these types of questions.

PROACTIVE PLANNING FOR eDISCOVERY:

To be fully prepared for eDiscovery requests, you'll need a two-pronged approach.

First, create or update the appropriate policies and procedures. These include:

- **Electronically stored information (ESI) retention policies**
- **An employee ESI use policy**
- **A litigation hold policy**
- **A tested eDiscovery procedure**

Second, install an automated, centrally-controlled archive system that performs the following functions:

- **Captures (at the very least) all email, SharePoint, and file system data, the three most discovered data types**
- **Indexes data**
- **Single instances data**
- **Applies retention policies**
- **Allows for immediate litigation holds**
- **Searches archived data quickly**
- **Provides on-going data inventory (data map) of all archived discoverable data**

BUILDING A PROACTIVE ESI ARCHIVE

The key to building an effective ESI archive is to use a solution that preserves the types of data you are generating and captures all discoverable data. If you choose a solution that captures only email messages and attachments but not calendar entries, task lists, contact lists, or object attributes, then you will still need to restore backup tapes and image employee's hard disks 24 hours a day. Unfortunately, opposing counsel will often request data that you can't or will have a hard time producing. So your best strategy is to purchase a solution that captures everything they could ask for.

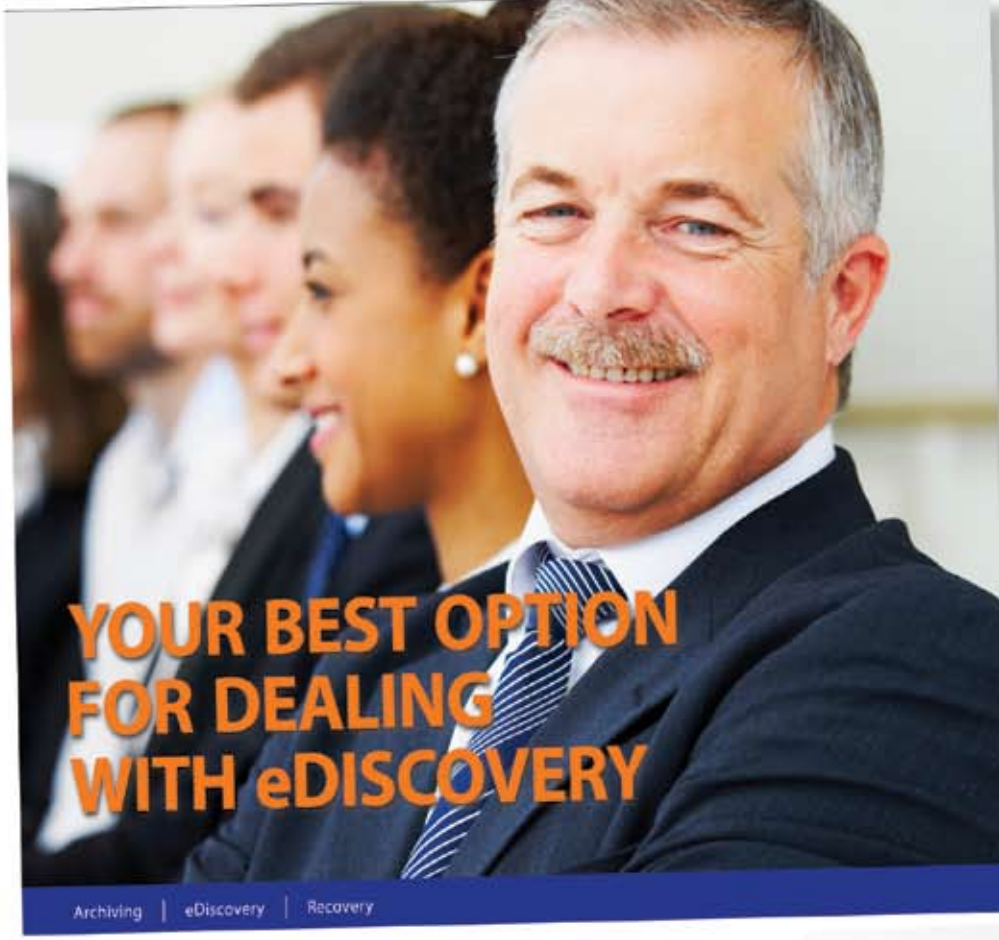
WARNING: BLATANT PRODUCT PLUG AHEAD!

As you've no doubt seen in the headlines, ESI including SharePoint records, work files, and email data are playing an important role in high-profile legal proceedings. ESG reports that 80 percent of organizations in litigation have been asked to produce emails and attachments in response to discovery requests. What is not as widely publicized is that 60 percent of them have also been asked to produce unmanaged general office documents, including SharePoint documents. There is only one ESI archive solution that captures all discoverable data in the SharePoint, Exchange, and Windows file system.

The Mimosa Systems NearPoint™ Content archive captures data in near real time. NearPoint provides an integrated archive for Microsoft SharePoint systems, emails, attachments, instant messages, and file system data. Unlike other archive products that store content in multiple archive locations, NearPoint is the next generation single repository—all content is stored in one highly-scalable archive. NearPoint ends reactive eDiscovery fire drills by providing a unified repository for SharePoint, messaging, and file content with a single search experience for eDiscovery.

WHAT DOES THIS MEAN FOR IT?

Being able to respond to eDiscovery requests quickly (within minutes or hours, rather than days or weeks) will impress the hell out of your General Counsel and maybe even your CEO. Planning for eDiscovery includes putting the right automation in place—it'll always save your company time, dollars, and risk.



All–

Check out this brochure on Mimosa NearPoint. Seems like our best bet.

(Click here to view)

MIMOSA SYSTEMS

DATE OF REQUEST

TIME OF REQUEST

FORM ID-10T

Request for IT Services

NAME

DEPARTMENT

EMAIL

PHONE

DESCRIBE, IN DETAIL, THE NATURE OF YOUR PROBLEM

NOW PLEASE EXPLAIN THE FEEBLE ATTEMPTS YOU HAVE MADE TO REMEDY THE SITUATION

IT SERVICES USE ONLY:

Cut out, make copies, and distribute to irritating colleagues for your continued amusement.

Form ID-10T Summary

To wrap up all the thoughts and suggestions laid out in the preceding chapters, it suffices to say that your company's legal responsibilities related to eDiscovery and electronically stored information (ESI) are absolute … and they are also an absolute pain in the butt. Still, for the sake of appearances, here is a summary of the salient points.

What is eDiscovery?

eDiscovery refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. It can be carried out offline on a particular computer, or it can be done on a network, or both.

How do the new FRCP Amendments relate to eDiscovery?

The new amendments to the Federal Rules of Civil Procedure (FRCP) highlight the fact that ESI is a discoverable record type and should be treated as any other type of evidence. In fact, these amendments are aimed directly at ESI. They define what ESI is, and what ESI must be disclosed and when. They also place new requirements on the parties' knowledge of their own electronic infrastructure; that is, they oblige parties to know what ESI they have, where it's kept, how it's retained, and how it's deleted.

There is a lot to consider. For example:

- **ESI is normally stored in much greater volume than are hard copy documents.**
- **ESI is dynamic—in many cases modified simply by turning a computer on and off.**
- **ESI can be incomprehensible when separated from the systems which created it.**
- **ESI contains non-apparent information, or metadata, that describes the context of the information and provides other useful and important information.**

Litigation holds—what, when, how?

In civil eDiscovery, all ESI that could pertain to a case must be found and protected—that's called a litigation hold—and turned over to opposing counsel when requested. The FRCP's amended Rule 37(e) make it clear that any automatic deletion feature should be turned off and a litigation hold imposed once litigation can be reasonably anticipated.

So what qualifies as "reasonable anticipation"? In short, any situations in which a reasonable person would conclude that litigation is a possibility sometime in the future. Unfortunately, the gap between when a company should have reasonably anticipated litigation and when they actually do, can be (and often is) used by opposing counsel to charge companies with spoliation.

What is spoliation?

Simply put, spoliation is the intentional or inadvertent destruction, mutilation, concealment, or alteration of evidence.

A spoliation of ESI decision against your company can result from a number of routine actions and automated processes, including the re-use of backup tapes, the continued use of applications that automatically delete data after a litigation hold has been applied, the deletion of email by employees, the practice of writing over files on a USB thumb drive, and the disposal of data CDs or DVDs.

A spoliation decision can prompt the judge to issue an "adverse inference" instruction to the jury, who may then conclude that your evidence is "missing" because you decided it was incriminating and tried to get rid of it. In short, spoliation will often lose you the case—perhaps even before you get your day in court. Unless you're lucky enough to find a "safe harbor" in this storm.

Where is the Safe Harbor?

Rule 37(e), otherwise known as the Safe Harbor amendment, is a new FRCP rule protecting parties in litigation from sanctions if potentially responsive data (evidence) is inadvertently altered or deleted. The rule states that, "Absent exceptional circumstances, a court may not impose sanctions ... on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

In most cases, the court will presume you are an expert in your IT operations and should know when data deletions need to be suspended. To claim Safe Harbor, an organization must demonstrate it has made all the right moves to insure potential evidence is not lost or deleted. If your company mishandles ESI, it's highly unlikely that a judge will consider a defence of "we don't have the automated processes in place to handle this!" Chances are your company will lose and be subject to sanctions and fines.

How about a Team Approach?

Good idea. Much of the cost of discovery is directly related to finding all the requested data, wherever it may be. Unprepared companies perform inefficient searches—disrupting employee productivity, searching the same data store many times, and looking at employee data not part of the discovery request. Such inefficiency increases a company's risk of not finding all data requested or adversely turning over too much data.

To make it through an eDiscovery process successfully, IT will have to cooperate with representatives from a number of other departments. Proactively creating and training a well-informed and active cross-departmental eDiscovery team will greatly reduce costs and risks, as well as help IT when unexpected litigation arises. In addition, this measure will also help protect your employees should someone be called into court to explain how the discovery was accomplished. (If the court suspects spoliation, you should expect subpoenas.)

What Does This Mean for a Company Facing Litigation (and for its IT department)?

Any organization can be sued in federal court (it happens to the best of us), so we are all impacted by the FRCP amendments. To prepare for litigation, organizations need to proactively plan all aspects of their electronic infrastructure—including litigation hold capability and ESI retention policies.

If your company finds itself facing civil litigation (and statistics suggest the better lead here is "When your company finds itself facing civil litigation"), you may be directed to locate and protect specific files—including ESI and metadata—having specific content, sent from or to specific employees, and issued between any number of specific dates. But it gets a lot more complicated from there. These days, a discovery request can also include conversation threads, Boolean logic instructions ("this" but not "that"), proximity searches (the word "Tolson" within seven words of the word "Mimosa," for instance), and even such attributes as whether an email was opened, when, and by whom. Two additional things to consider: first, your company will have to guess at what data opposing counsel will want to see and secure it; and second, opposing counsel can ask for anything—if the judge approves their request, you'd better have made sure the responsive data was not deleted after you should have thought to secure it.

Finally, if your company is like most, you'll have to search through terabytes of ESI to find the information being asked for by opposing counsel. And you will likely have a few weeks—perhaps even just a few days—to do so.

What does this mean for IT?

It means that eDiscovery can be your worst nightmare.

The Bottom Line

The only way to greatly lower your risk and cost in eDiscovery is to proactively plan for it. This includes putting systems in place that will automate many of your requirements. There's no denying it: planning for eDiscovery now will pay off big later.

The Know-IT-All's Guide to eDiscovery was brought to you by

Mimosa Systems provides information immediacy, discovery, and continuity for the new generation of critical enterprise information. It enables fingertip access to vast information by users, powerful and rapid search and retrieval of corporate historical information by auditors, and uninterrupted access to corporate information in the midst of failures and errors. Mimosa is focused on information management of unstructured and semi-structured data, including SharePoint, email and attachments, instant messages, files and documents, and other new data types. Mimosa NearPoint™ Content Archiving Solution provides fine-grained and immediate recovery, with self-service archival access to enterprise information. Mimosa NearPoint is the industry's only comprehensive information management solution for SharePoint, Exchange, and file system data, unifying archiving, recovery, and storage management. NearPoint assures content continuity and regulatory compliance, while leveraging cost-effective disk technologies to optimize Exchange storage growth.

SOURCES:

[1] Electronic Discovery definition from the website: http://searchfinancialsecurity.techtarget.com/sDefinition/0,,sid185_gci1150017,00.html

[2] From "The Impact of the New FRCP Amendments on Your Business" by Osterman Research

[3] From the Cornell Law School FRCP site: http://www.law.cornell.edu/rules/frcp/Rule26.htm

[4] From the SETEC Investigations website: http://www.setecinvestigations.com/resources/legaltools/legaltool2.php

---

MIMOSA SYSTEMS HEADQUARTERS
3200 Coronado Drive
Santa Clara, CA 95054
T +1 (408) 970 9070
F +1 (408) 970 9041
Email: info@mimosasystems.com

WORLDWIDE OFFICES
Australia +61 (2) 9089 8603
Canada +1 (613) 797 2952
China +86 (21) 6103 7361
France +33 1 55 60 23 62
Germany +49 (89) 904 7551-0
India +91 (20) 4048596
United Kingdom +44 (0) 118 963 7860
www.mimosasystems.com

MIMOSA™
SYSTEMS

ADVANCED PRAISE FOR

the know-IT-all's guide to eDiscovery

In a world of e-Everything, it's the complexities of eDiscovery that should have us sitting up and taking notice. Thanks for taking this message of hope to the people.

— *The Wally Street Journal*

Droll and eloquent, this is the eDiscovery story of the decade. Bill Tolson is at the top of his craft. (Bill, if you're hiring, call me!)

— *Marty, ACME Worldwide, Inc.*

I laughed. I cried. I hurled. — *Wayne*

With this guide in my back pocket, I'm almost hoping we're sued! We're ready—bring it on!

— *Employee 8, ABC Corporation*

MIMOSA™ SYSTEMS