E-Discovery Is THE Discovery

In the large majority of cases, electronic evidence discovery is not a "problem." The small minority of very complex cases is probably an exception. In the other 90-95% of our federal cases, it is the way that the search for truth proceeds.

I write this paper to respond to Greg Joseph's observations. His perspective and suggestions, delivered before the empirical surveys were completed, may apply to the 5-10 % of very complex cases. But if they applied to the others, or less broadly put if they applied to the employment cases brought in the federal courts, they would do some harm to the normal employee seeking statutory or common law remedies. Some suggestions might do significant harm.

I propose to follow the format Mr. Joseph utilized, and comment on each section from the perspective of an experienced lawyer representing employees in the federal court.

I. PRE-LITIGATION PRESERVATION

A. Mr. Joseph's Proposals

Mr. Joseph notes the lack of "codified benchmarks" triggering a pre-litigation duty to preserve electronic evidence. He argues that the guideline of "reasonably foreseeable litigation" is not clear enough, in general, to provide a safe harbor if electronic evidence is destroyed. Therefore, even though organizations are uncertain whether they will face litigation, they still must make pre-litigation judgments whether and how to preserve evidence. A variety of "costs" arise, which may eventually include litigation costs. The solution to this part of the "problem" is to promulgate clear and specific rules, as well as to "require subjective bad faith as a prerequisite for pre-

litigation spoliation sanctions." The new rules must also consider cost-shifting when (1) a third party receives a notice to preserve, in which case cost-shifting should be mandatory and (2) whenever a pre-litigation notice is issued.

The new rules also should clarify what constitutes a notice. One suggestion is to create a form with the "essential elements" necessary for notice. Then, both the recipient of a valid notice, and the sender, shoulder the obligation of preservation. Concrete and exhaustive examples, which avoid catch-all phrases, should be part of the rule, even if such examples "may be subject to manipulation."

Clear limits should also be set, even if "effectively arbitrary," that specify "the [pre-litigation] scope of the duty to preserve." If a prospective party wants broader preservation, it should bring suit. In fact, if it does not bring suit within a specific time period after its preservation demand, the duty to preserve should dissolve. Moreover, the duration of the duty to preserve should be "uniform," effective from the date of the preservation demand or other trigger. If contractual, regulatory or statutory duties provide otherwise those limits may apply.

Finally, for pre-litigation activities negligence is the wrong standard. The standard of proof should be "subjective bad faith."

B. Comments

Suppose you counsel a company which classifies a category of employees as exempt from overtime pay. Your company has received no notices of prospective litigation, nor any administrative complaints. But, because you read the newspaper and subscribe to various legal periodicals, you know that there are at least ten other companies which have classified the same categories of employees as exempt that have been sued in class actions in different federal courts. Should you start destroying all of

your electronic evidence that is relevant to the decision to classify these employees? I submit that it is probable that almost any federal judge would find that your company was subject to "reasonably foreseeable litigation."

In the employment relationship, companies are subject to record retention requirements, most of which require retention for more than one year. I have attached a spread sheet showing such requirements. (Attachment 1) These are one important type of "codified benchmarks." The term "reasonably foreseeable litigation" is no less determinable than a host of other important legal terms. How about "negligence?" Or, in the employment context, "similarly situated?" These terms involve questions of fact, which vary from case to case and must be decided after evaluating evidence. The observation that companies must exercise judgment which in hindsight may be found to be wrong is hardly a reason to give such companies a free pass, conditioned only on them making their judgments in other than subjective bad faith. In employment law, those of us representing employees are well acquainted with the "business judgment rule" that preserves all the discretion in the world for companies to make decisions as long as the decisions are not discriminatory or violate the law in some other way. Even with the protection of the "business judgment rule" many companies have, in hindsight, been fund to be wrong.

In West v. Goodyear Tire & Rubber Co., 167 F 3^{d} 776, 779 (2d Cir. 1999) the Second Circuit observed "it has long been the rule that spoliators should not benefit from their wrongdoing, as illustrated by 'that favored maxim of the law, omnia presumuntur contra spoliatorem.' 1 Sir T. Willes Chitty, et al., Smith's Leading Cases 44 (13th ed. 1929). '("Let all be presumed against a spoiler of evidence.")" Moreover, lawyers must obey their obligations under ethical rules. ABA's Model Rule 8.4 (d) prohibits lawyers

from engaging in conduct prejudicial to the administration of justice. More on point, however, is Model Rule 3.4 (a) that specifically prohibits unlawful alteration or destruction of evidence or assisting others to do so.

But what about the "costs" of preservation? Most of Mr. Joseph's listing of "costs" are not "costs" at all - they are just corporate judgments about document retention. Other "costs" are required by federal statutes and regulations, and therefore should not be proposed for sharing by other parties. Finally, large companies that engage in complex litigation can and should get expert assistance to retain and produce electronic evidence. Attachment 2 contains good suggestions of how to control costs by using experts.

One of the biggest almost unexamined weaknesses is, in fact, the willingness of commentators and some courts to reflect the claim that "costs" are so exorbitant in electronic discovery that those "costs" must be limited or shared. Very few list, as to his credit Mr. Joseph did, how those "costs" are defined. I submit that the pre-litigation list of "costs" very starkly shows that most (if not all) are simply normal business judgments which must be made whether or not there may be "reasonably foreseeable litigation." If the Company decides that it should pay its lawyers, whether inside the company or outside, to assist it in determining what to retain and what may be deleted, this also may be a reasonable corporate judgment but this judgment is also made simply in the normal course of business. There is no reason whatsoever why the normal plaintiff in the federal court should be subject to a hindsight decision to share in the cost of corporate legal counseling.

Therefore, there would and should be substantial opposition to any rule limiting or circumscribing the present development of the law, and/or specifying a one-size-fits-

all duration for preservation of electronic evidence. In particular, there is no good policy reason to require a showing of subjective bad faith as a prerequisite to a sanction for pre-litigation spoliation. The party accused of spoliation always can argue that it proceeded in subjective good faith. Perhaps it was subjectively ignorant of all of the case law on spoliation. If it took that position, it is highly doubtful that a court would excuse its conduct, and there is no good policy reason why the court should excuse it. On the other hand, if as discussed below a party diligently tried to follow applicable guidelines, this would be an objective defense to bad faith and spoliation which I suspect most courts would credit.

If a third party argues that it should be allowed to shift certain costs when it receives a pre-litigation notice to preserve but it is not the litigation target, it may have a good point and its position is the most compelling. But, it should be required to detail its "costs" of compliance and those alleged "costs" should be strictly scrutinized. If, for example, the party issuing the notice would be willing to accept a mirror image of the third party's hard drive, the third party would have no real costs. Of course, it may not want to provide all of that information; it may want its lawyers to review all of that information first. That is a reasonable corporate judgment, but it is difficult to understand why the requesting party should be forced to contribute to that review.

Finally, the suggestion that cost-shifting should be considered whenever a preservation notice is issued has little merit. The reason proposed that automatic cost-shifting is not "unfair" is that a party can file suit which would allow a judge to be involved in the preservation notice issue. This reason flies in the face of modern dispute resolution, where the first principle is that a lawsuit, if possible, should be avoided rather than encouraged. In addition, to mandate judicial involvement, increasing the already

heavy workload of our federal judges, is a bad alternative.

If there is a lack of clarity in the term "reasonably foreseeable litigation" one of the suggestions Mr. Joseph makes should help clarify what constitutes notice of such litigation. His proposal for setting forth the "essential elements of a certification" or including a form with those elements is a very good idea, and could reduce litigation over the contents of notice. I also agree with his suggestion that if such a notice is issued, this triggers a duty to preserve on the part of the issuer as well.

His suggestion that the drafters of the new rule must think of every example that triggers a duty to preserve electronic evidence, and that those examples must be conclusive without any "catch-alls" to provide for the unforeseen, should be partially acceptable. It is a good idea to provide concrete examples of when the duty to preserve exists, and it is a good idea that those examples be as exhaustive as possible. I disagree with him that intentional manipulation should be excused because there should be no residual catch-all phrase. It is better to make the examples serve as guidelines, with a residual catch-all, than to encourage those with the specific intent to do wrong to be allowed to manipulate a concrete rule.

Similarly, Mr. Joseph has set out some good guidelines that would assist courts in determining the case-by-case scope of the duty to preserve electronic evidence. There is no need to set specific limits which will be "effectively arbitrary." Given the different lengths of time that electronic evidence is required to be preserved by federal employment law or regulation, it is hard to imagine that an inflexible rule could provide for preservation for any period shorter than the longest statutory or regulatory time presently required, which probably doesn't make very much business sense. I would also support the idea that a guideline could be drafted to allow cessation of preservation

activities if suit is not brought within a specified period following a demand. Again, however, because it would be counterproductive to force lawsuits in circumstances where pre-litigation settlement is possible, any rule which forces lawsuits because an arbitrary time period has passed would not be a good rule.

II. POST-COMMENCEMENT PRESERVATION AND PRODUCTION

A. Mr. Joseph's Proposals

The proposals made in this section again appear to be founded on issues arising in complex cases. Mr. Joseph notes that preliminary motions are common and delay attention to discovery, or even stay discovery. Even without a motion, the initial pretrial conference may take weeks or months to schedule, and there is no assurance of electronic discovery problem-solving at that time. With these uncertainties, evidence conservation is often over-inclusive. As long as discovery is discretionary and wide open, lawyers tend to agree to more discovery to avoid burdening the court with disputes.

It is difficult to define what is "undue burden and cost" even when electronic evidence is "reasonably accessible." The cost of allowing unlimited judicial discretion is too high. Parties need concrete rules. There are options for concrete rules. One is to apply limits to certain categories of electronic evidence, or limits to the number of custodians responsible for gathering the evidence, or limits to the type of data or platforms. Another option is to provide that certain categories of electronic evidence should be allowable only upon exceptional circumstances which would make some categories presumptively exempt from production. Or, alternatively, some categories of electronic evidence may require a showing of likely admissibility before production is ordered. And, when information has been produced in a usable form, a party that wants the same production in a different form should incur the cost.

B. Comments

There is no serious dispute that a mega-case can stop a court cold. The electronic discovery in one case can dwarf the discovery necessary in numerous garden-variety cases. The question is whether solutions should change the Rules. I submit that mega-cases should not control the Rules. There are less drastic remedies to try to deal with the specific issues which surface in large complex cases.

Complex cases may indeed need special case-by-case procedures and "rules" (small r). An immediate motion to designate the case as complex, if granted, could put it on a special track. In the recent Voir Dire magazine published for the American Board of Trial Advocates, Judge Royal Ferguson (N.D. Texas) suggests appointing a special master "with expertise in information technology" in these cases. The parties would divide the cost. Normally, the "special master would meet with the IT representatives of the various parties to determine how their IT systems work and how discovery can be focused to obtain the needed information without excessive expense." The special master could also act as an expert to the court.

Judge Ferguson has made an excellent suggestion. The cost of the special master is probably less than the cost of one associate per party who would otherwise work on the case. I would suggest, however, that appointment should not be automatic, but made only after motion. The moving party could hardly object to the cost. Nor in reality could an opposing party, unless its reason for objection was that the parties contemplated working out solutions to discovery without court intervention. If the solutions were not forthcoming, and the court needed to intervene anyway, it could at that time appoint a special master sua sponte.

The special master appointment process should be like an arbitrator selection process. First, if possible a master could be selected by the parties' mutual consent. If the parties cannot agree, however, thus requiring the court to appoint a master, before the appointment becomes final the master should provide a detailed disclosure of all prior contacts with the parties, witnesses or counsel. After receiving the disclosure, the parties should have a fixed amount of time to object to the appointment, for cause shown by the disclosure.

The special master appointment process should eliminate the need for "concrete rules" setting quantitative limits, undiscoverable categories of electronic evidence or requiring a showing of admissibility before certain electronic evidence is discoverable at all.

III. EARLY MERITS REVIEW

Significant controversy accompanies the proposal that courts should consider the merits of cases before discovery begins. In employment cases, when most employees are escorted from the premises without prior notice, and immediately lose computer access to documents, there is almost always, as Mr. Joseph put it, "a profound imbalance of information.." For such individuals in litigation, early merits review before reasonable discovery feels profoundly unfair.

One reason that federal judges are not that well-qualified to evaluate pleadings by "draw[ing] on... judicial experience and common sense," Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949-50 (2009) is, frankly, that in general their life experience is substantially different from the life experiences of those who might be picked as jurors in the case being evaluated. Most federal judges have never been fired, nor demoted nor suffered any real adversity in their work. They have done extremely well at school. Some judges

come from different, less privileged backgrounds. It is relatively easy to predict that the "common sense" of one federal judge will be quite different than the "common sense" of another federal judge, both of whom are evaluating the same case.

I was recently made aware of how Judge Mark Kravitz (District of Connecticut) evaluates pleadings on a motion to dismiss. He stated that when he reviews pleadings, the distinction between a "conclusory allegation" and "fact" is not particularly helpful. Instead he considers (1) how general is the information in the complaint and (2) who is in possession of the facts. When a plaintiff alleges a hostile work environment, for example, and the complaint states "I was subjected to a hostile work environment," this statement is (1) rather general and (2) made by the person who allegedly endured the environment and should be in possession of more specific facts. Absent amendment that case would be dismissed. In contrast, however, if the plaintiff asserted that two defendants should be regarded as a single employer, because those defendants would be far more likely to be in possession of the facts, he would be more inclined to deny the motion to dismiss.

This is a sensible, or "common sense," way of reviewing pleadings.

In my other paper, I will suggest a mechanism which could speed initial discovery and, in some cases, contribute to cost-effective solutions other than the blunderbuss approach of early dismissals. For now, I only submit that the courts should be slow in dismissing employment cases, for the cogent reasons advanced in Swierkiewicz v. Sorema N.A., 534 U.S. 506 (2002). Although it is hard to argue that Swierkiewicz remains good law, it may at least remain a statement of good "common sense." The complaint at issue "detailed the events leading to his termination, provided relevant dates, and included the ages and nationalities of at least some of the relevant persons involved with his termination. These allegations give respondent fair notice of what

petitioner's claims are and the grounds upon which they rest." Id. at 514. Using Judge Kravitz's rubric, although the allegations are somewhat general, the defendant is in possession of the facts. Therefore, a motion to dismiss should be denied.

ATTACHMENT #1

Record Retention Requirements

Laws	Records/Reports	Retention Requirements
Age Discrimination in Employment Act (ADEA) *Applies to employers with at least 20 employees	Payroll or other records, including those for temporary positions showing employees, names, address, dates of birth, occupations, rates of pay and weekly wage Applications, personnel records relating to promotions, demotions, transfer, selection for training, layoff, recall, or discharge; job advertisement and posting; copies of employee benefit plans, seniority system and merit system **IN MONTANA ALL EMPLOYERS, NO AGE LIMIT, MINIMUM OR MAXIMUM**	**Three years** for payroll or other records showing basic employee information **Two years** for applications and other personnel records Where a charge or lawsuit is filed, all relevant records must be kept until **final disposition** of the charges or lawsuit
Americans with Disabilities Act (ADA) *Applies to employers with at least 15 employees	Applications and other personnel records (e.g. promotions, transfers, demotions, layoffs, terminations) requests for reasonable accommodation. **IN THE STATE OF MONTANA, APPLIES TOO ALL EMPLOYERS WITH AT LEAST 1 EMPLOYEE**	Two years from making the record or taking the personnel action Where a charge or lawsuit is filed, all relevant records must be kept until **final disposition**
Civil Rights Act of 1964, Title VII *Applies to employers with at least 15 employees	Applications and other personnel records (e.g. promotions, transfers, demotions, layoffs, terminations), including records for temporary or seasonal positions. Requires the filing of an annual EEO-1 Report **IN THE STATE OF MONTANA, APPLIES TO ALL EMPLOYERS WITH AT LEAST 1 EMPLOYEE**	**One year from making the record or taking a personnel action** Where a charge or lawsuit is filed, all relevant records must be kept until **final disposition** A copy of the current EEO-1 Report must be retained
Consolidation Omnibus Budget Reconciliation Act (COBRA)	Provide written notice to employees and their dependents of their option to continue group health plan coverage following "qualifying events", such as the employee's termination, layoff or reduction in working hours, entitlement to Medicare, and the death or divorce of the employee (that would cause dependents to lose coverage under the employers' plan	
Davis Bacon Act Service Contract Act Walsh-Healy Public Contracts Act	Records containing the following information for each employee: Basic employee data to include name, address, social security number, gender, date of birth, occupation and job classification Walsh-Healy requires the retention of current work permits for minors Compensation records to include:	**Three years from the end of the contract** Walsh-Healy requires the retention of data with respect to job-related injuries and illnesses, specifically logs with dates and

Laws	Records/Reports	Retention Requirements
Applies to Federal Contractors	▪ Amounts & dates of actual payment ▪ Period of service covered ▪ Daily and weekly hours ▪ Straight time and overtime hours/pay ▪ Fringe benefits paid ▪ Deductions and additions	summaries and details of accidents
Employee Retirement Income Security Act (ERISA)	Maintain, disclose to participants and beneficiaries, and Report to the Department of Labor, IRS, and the Pension Benefit Guaranty Corporation (PBGC) certain reports, documents, information and materials. Except for specific exemptions, ERISA's reporting and disclosure requirements apply to all pension and welfare plans, including: ▪ Summary plan description (updated with changes and modifications) ▪ Annual reports ▪ Notice or reportable events (such as plan amendments that may decrease benefits, a substantial decrease in the number of plan participants, etc.) ▪ Plan Termination	Employers must maintain ERISA-related records for a minimum of **six years**
Employee Polygraph Protection Act	Polygraph test and the reason for administering	**Three years**
Equal Pay Act	Payroll records including time cards, wage rates, additions to and deductions from wages paid, and records explaining sexually based wage differentials	**Three years**
Executive Order 11246 Applies to Federal Contractors	Requires the preparation of an Affirmative Action Plan (AAP) for Minorities and Women Applications and other personnel records that support employment decisions (e.g. hires, promotions, terminations) are considered "support data" and must be maintained for the AAP	AAPs must be updated annually: and documentation of good faith efforts must be retained for **two years**. Personnel or employment records must be retained for **two years**. If there are less than 50 employees or contract is less than $150,00, the retention period is **one year**
Fair Labor Standards Act (FLSA)	Payroll or other records containing the following information for each employee: Employee's name; home address; date of birth (if under 19 years of age); gender; time of day/day of week for beginning of workweek; regular hourly rate of pay or other basis of payment (Hourly, daily, weekly, piece rate, commission on sales, etc); daily hours worked; total hours for each work week; total daily or weekly straight-time earnings (exclusive of overtime premiums); total additions to and deductions from wages for each pay period; total wages per pay period; date of each payment of wage; period covered by the payment.	For at least **three years**

Laws	Records/Reports	Retention Requirements
	For executive, administrative, and professional employees, or those employed in outside sales, employers must maintain records which reflect the basis on which wages are paid in sufficient detail to permit calculations of the employee's total remuneration, perquisites including fringe benefits.	
Family & Medical Leave Act (FMLA)	Records containing basic employee data as required by FSLA and dates of leave taken by eligible employees. Leave must be designated as FMLA leave For intermittent leave taken, the hours of leave Copies of employee notices and documents describing employee benefits or policies and practices regarding paid and unpaid leave Records of premium payments of employee benefits Records of any dispute regarding the designation of leave	**Three Years**
Federal Insurance Contribution Act Federal Unemployment Tax Act Federal Income Tax Withholding	Records containing basic employment data. Compensation records to include: ▪ Amounts & dates of actual payment ▪ Period of service covered ▪ Straight time and overtime hours/pay ▪ Annuity and pension payments ▪ Fringe benefits paid. Tips ▪ Deductions and additions Tax records to include: ▪ Amount of wages subject to withholding ▪ Agreements with employee to withhold additional tax ▪ Actual taxes withheld and dates withheld ▪ Reason for any difference between total tax payments and actual tax payments ▪ Withholding forms (W-4, W4-E)	**Four years** from the date tax is due or tax is paid
Immigration Reform & Control Act (IRCA)	INS Form I-9 (Employee Eligibility Verification Form) signed by each newly hired employee and the employer.	**Three years** after date of hire **or one year** after date of termination, whichever is later.
Occupational Safety & Health Act (OSHA)	A log of occupational injuries and illnesses A supplementary record of injuries and illnesses Post a completed annual summary of injuries and illnesses Maintain medical records and records of exposure to toxic substances for each employee	**Five Years** **Employee's job tenure plus thirty years**
Rehabilitation Act of 1973 Applies to Federal	Personnel employment records (e.g.; requests for reasonable accommodations, results of physical exams, job advertisements and postings, applications, resumes, tests, test results, interview notes and	**Two Years** (Note: If a contractor has fewer than 150 employees or a contract

Laws	Records/Reports	Retention Requirements
Contractors	records regarding hiring, assignment, promotion, demotion, transfer, layoff, terminations, rates of pay or terms of compensation and selection for training apprenticeship) Data on complaints of disability discrimination and action taken. Requires an Affirmative Action Plan for individuals with disabilities	of less than $150,000 the retention period is only **one year**.) Where a charge of lawsuit is filed, all relevant records must be kept **until "final disposition.** AAPs must be updated **annually;** no current requirement to retain expired plans
Uniform Guidelines on Employee Selection Procedures	For employers with 100 or more employees, records showing toe impact of the selection process for each job, maintained by sex for each racial or ethnic group that constitutes at least 2% of the labor force in the relevant labor area or 2% of the applicable workforce. For employer with less than 100 employees, records showing for each year the number or persons, promoted, terminated, applicants hired for each job by sex and where appropriate by race and national origin. Records including applications, tests, and other types of selection procedures used as a basis for employment decisions, such as hiring, promotion, transfer, demotion, training and termination. Adverse impact analysis of selection process must be conducted annually	Where adverse impact is found in the selection process, records must be maintained for **two years** after the adverse impact is eliminated. For federal contractors, during a compliance review from the Department of Labor's Office of Federal Contract Compliance Programs, data for the prior year's analysis must be available, and for the current year if a contractor is six months into its AAP plan year. (See also Executive Order 11246)
Vietnam Era Veterans, Readjustment Assistance Act. Applies to Federal Contractors	Personnel/employment records (see Rehabilitation Act of 1973 above) Affirmative Action Plan for covered veterans. Requires the filing of the annual VETS-100 report. Job openings for positions must be listed with the sate employment service	**Two years** (Note: If a contractor has fewer than 150 employees or a contract of less than $150,000 the retention period is only **one year**) AAPs must be updated **annually**; no current requirements to retain expired plans. A copy of the current VETS-100 report must be retained.

ATTACHMENT #2

Chapter 15: Working with IT Experts
Author: Linda G. Sharp, Esq., MBA
Edotor: Douglas E. Dexter, Esq., Farella Braun & Martell LLP, San Francisco

Many thanks go out by this author to Meridith Socha, Law Clerk, Kroll Ontrack, for her assistance.

I. THE NEED FOR ELECTRONIC WORKPLACE DATA EXPERTS

The past ten to fifeteen years have wrought dramatic changes in the creation, use, and retention of business information. Attorneys litigating employment disputes cannot ignore these changes for the simple reason that workplace data is omnipresent in employment matters, and often a case cannot be won without it.

Accordingly, attorneys must acknowledge these changes and grapple with them. Given the immensity and complexity of information that must be understood for even a run-of-the mill employment matter, attorneys must be prepared to select qualified electronic workplace data experts to guide data retention efforts as well as the identification, collection, processing, and production of responsive electronic data. Remember, *Zubulake* was "just a single plaintiff's employment matter". Something that may seem so simple and and run of the mill, may not be in the world of ESI.

In order to understand the types of experts that an attorney may need to retain to assist with establishing a data retention program to prepare for the inevitable litigation, investigation or regulatory matter that will require locating and producing data, attorneys need first to acknowledge that times have changed.

A. How Data Has Changed

Prior to the dawn of the technological era, end user (custodian) business records/data was largely stored in paper form with some information stored as micro-fiche or micro-film. We might see data stored in large main frames and other computer systems, however, the primary data sought in litigation resided in paper. The majority of such hardcopy records remained in the care, custody and control of the company that created the data or its agents. Such records were maintained in boxes that were strategically labeled, shelved and tagged for destruction pursuant to the company's "records retention" schedule.

In the event of litigation and the corresponding litigation hold, it was customary to have individuals cull through their offices to search for responsive data, which may have resulted in identifying a relatively small, limited set of documents. This would be followed by a visit from outside counsel who would personally inspect the offices to locate and retrieve additional relevent information.

The Federal Rules of Civil Procedure were amended on December 1, 2006 to provide more clarity around producing electronically stored information as discoverable information.[1] Many states have followed the federal example and have either copied or in some way mirrored the federal rules and also explicitly included electronic information in the list of information that is discoverable during litigation.[2] Additionally, many regulatory and investigatory bodies consider this type of information fair game and often seek it during the course of their investigations. In short, the production duty placed on parties and their counsel has not essentially changed under the amendments to the Federal Rules: if data exists, parties are required to identify, preserve, review and produce those pieces of information that are relevent or responsive to discovery requests, absent a claim of privilege or other valid objection.

What has changed, however, is the *volume* and *complexity* of the information subject to the duties now expressly required by the Federal Rules of Civil Procedure. Moreover, corporate America has seen a sea of change in the way it creates data and the form that data takes. Specifically, new technologies have drastically decreased the need for administrative and other clerical staff that once labelled, organized, and managed company records in compliance with corporate policies. In this modern reality, fewer attorneys and company executives employ their own administrative assistant than in yesteryear. Alternatively, many assistants that are employed are supporting multiple professionals. The result is that professionals themselves are doing more clerical work than in the past. Another significant difference between the old and current practices is that in the "old days" documents would often be proofread by an administrative assistant and the professional before a final document was signed and distributed. In sharp contrast, professionals today can be nearly anywhere while preparing a business record typed with their thumbs on a PDA and distributed via e-mail without a second thought, let alone a second pair of eyes. However, these hastily written e-mails are as much a business record as the thoughtfully crafted documents of yesteryear and are avidly sought in the midst of litigation and regulatory investigations.

In addition to altering the practices used to create documents and creating more documents than ever before, the manner in which those documents are

---

[1] Fed.R.Civ.P. 34(a) (2008).

[2] For information on states that have adopted such requirements, see BNA's *Digital Discovery and Electronic Evidence.*

maintained has also drastically changed. Records are no longer organized by color-coded, labeled folders; rather, business records are lumped in with the bits and bytes of communications stored on a computer system somewhere – perhaps a single computer operating system, a network, or any number of portable storage devices or backup environments.

One-size-fits-all retention schedules are impossible to establish for these "business records" that are comprised of such disparate data types. To understand the problems with evaluating these electronic "business records," one need merely look to one's own e-mailbox and note the volume of communications regarding "leftover food in the lunch room" and "pick up the milk on the way home" to realize how intricately our "business records" are comprised of potentially relevant and completely irrelevant data. These types of communications were not labeled business records ten to fifteen years ago because people then relayed such informal, non-business communications bypicking up a phone, and the company-wide memorandums were appropriately filed in "file 13" and summarily destroyed. But changing business practices, often the result of changes in technology, have resulted in problems with today's "business records" that are two-fold. First, there are far too many records. Second, many of the records contain information that in fact does not qualify as a business record.

B. Continuing Preservation Obligations in the New Data Environment

As noted above, although workplace data has changed in many ways over the past ten to fifteen years, parties continue to be under the same stringent duty to preserve relevent information. As explained in the benchmark case, *Zubulake v. UBS Warburg LLC*,[3] once a party reasonably anticipates litigation it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents, including electronically stored information (ESI). In other words, a duty to preserve ESI is triggered when a party reasonably anticipates being sued. Unfortunately, there is no bright-line rule regarding when a situation constitutes a credible threat of litigation as to trigger the preservation duty. Instead, each instance must be evaluated on a case-by-case basis, taking into account the facts and circumstances of the case including the parties' business sophistication and experience with litigation.

The bottom line is that an organization has a legal duty to preserve and produce responsive ESI when a litigation or regulatory investigation matter arises; please refer to chapters seven, eight, and nine of this book for a more exhaustive discussion of workplace data retention laws. These obligations arise long before notice of litigation or an investigation, are technically and legally complex to meet, and are not quick to implement. The knowledge of what must be produced and how to retain, preserve, and collect data for production requires specialized legal and technical expertise.

[3] 220 F.R.D. 212 (S.D.N.Y. 2003).

This chapter is intended to guide companies and the attorneys that represent them on how experts can be utilized to reach a state of litigation readiness and be prepared for the inevitable litigation or investigation that will affect your company or the company you represent. Experts are best utilized in different manners during different stages of working with electronic workplace data. This chapter breaks the use of experts into two overarching stages: (1) The use of experts in counseling and preparation roles prior to notice of litigation or an investigation, and (2) the use of experts in litigation and investigation roles subsequent to notice.

While the discussion of pre-notice litigation focuses on the use of experts from a management perspective, experts are also critically important to the plaintiff's side. The duty to preserve and ultimately produce is a burden shared by all parties to litigation. Plaintiff's duty to preserve attaches before filing of the Summons and Complaint at whatever time one "reasonably anticipates litigation." Arguably, this is likely coincident with the formal retention of counsel, if not before.

ESI experts can advise plaintiffs and their counsel on the types and locations of their client's data, what data a defendant may have available, and the mediums in which that data should be requested. Experts can also help plaintiffs devise programs to search through and identify key data and analyze material where statistics are important. For a further discussion of this topic, see Proving the Case, in *Representing Plaintiffs in Title VII Actions*, by Kent Spriggs,[4] Part IV - in particular see chapters 14 - 16 on "Use of the Defendant's Electronic Records," "Building Electronic Data Bases, and "Expert Witnesses" respectively.

Just as a municipality would not wait until a fire is in full flame before building a firehouse and hiring firemen, a corporation should not wait until the time and emotional pressures of litigation flare to prepare. In litigation, if you fail to prepare, you should prepare to fail – avoid this likelihood by taking the necessary precautions and partnering with the requisite experts.

II. THE USE OF EXPERTS PRE-NOTICE: COUNSELING AND PREPARATION ROLES

The roles of ESI experts prior to notice of litigation can be broken down into three distinct roles: retention, litigation readiness, and preservation/collection. While each role does require unique skills and qualifications to address different aspects of being prepared for litigation, it is important to note that there is some overlap between these roles and the same expert often can efficiently fulfill multiple roles depending on his or her training and experience. On the other hand, retaining multiple experts may be the best course of action depending on the facts and circumstances of your organization to best meet your business needs.

[4] Aspen Publishers.

A. Retention Experts

Retention experts are ESI experts who look at the nature of the business and the potential exposure to litigation on a proactive basis to ensure that business records are maintained in compliance with business needs.

The initial action taken by any retention expert worth his or her salt is an evaluation of what types of documents a particular business or organization is creating. This can be determined in any number of ways including interviews and conducting an inventory of data retained by the organization. Once it is determined what data types an organization retains, a retention expert's role is to create a defensible document retention policy based on the legal and practical retention requirements of certain documents. They need to take into consideration the media on which the data is stored, whether it is paper or electornic. If electronic, where is it and how is it stored?

Retention experts assist corporations in identifying legal and regulatory requirements surrounding various data types. Many documents (such as SEC filings and documents that fall under HIPPA) must be retained for a certain period of time by law. The statutory retention requirements may vary by jurisdiction or for each company depending upon the company's characteristics; a very helpful list of common employment-related statutory retention periods can be found in Appendix C to Chapter 11 of this treatise.

Data that is not governed by a specific law may require various retention periods based on the "useful life" period of the data type. Retention experts have knowledge as to what constitutes the useful life of various data types; knowing what is the useful life of a record is important to make a reasonable decision as to how long the record should be retained, and thus establish a reasonable, defensible retention schedule. For example, accounting records may have an 8-year retention schedule, customer service call logs/recordings a 5-year period, and e-mail a 60-day period. Moreover, a company with many diverse business units may have different retention periods for each; retention experts look at all business types to determine the proper retention period for each particular business unit given all the requirements and circumstances. Attorneys should keep in mind that a company with many diverse business units may have various retention periods for each.

Often times organizations, their attorneys and even inexperienced retention experts who are tasked with developing a retention schedule pay little or no attention to the IT infrastructure of the organization. Ignoring the IT infastructure of the organization can be a major blunder. The following two issues often arise when the retention expert ignores the IT infastructure:

- The retention periods applied to paper documents may not correspond with those for the electronic data. In other words,

simply relying on the buiness record type without taking into consideration the storage medium and its IT infrastructure support needs may result in determining an inappropriate retention schedule for the record type - one which may not hold up to judicial scrutiny for reasonableness.

- The company's IT capabilities may not be able to meet retention requirements established by a reasonable retention schedule.

In the event the second issue arises where the company's IT capabilities are unable to meet reasonable retention requirements, a retention expert can help the organization explore its options to meet its retention obligations. For example, one option is for the company to increase its IT capabilities or to outsource its IT responsibilities. Another option, in some circumstances, is to work with the retention expert to craft a retention policy which allows the organization to meet its responsibilities in a manner that consumes fewer IT resources. For example, many companies run a "brick-layer" backup configuration where data from disparate functional groups is backed up on the same backup tape; thus, e-mail, accounting and customer service data may all reside on the same backup tape. If each type of data has a different retention period, all of the tapes must be maintained for the longest period of time required by the various retention schedules. Therefore, if e-mail is retained with accounting data, both will be maintained for 8 years as opposed to 60 days; this unnecessarily ties up vast amounts of IT resources to retain the e-mail which could be destroyed pursuant to an e-mail's retention schedule 94 months prior to the date it will be destroyed when it is stored with the accounting data.

In considering a retention expert, the company should examine the expert's technical understanding of the company's network infrastructure. While a retention expert may make a recommendation as to optimal retention periods for various types of data, in practice, generally the final decisions are left up to the company itself, often to the decision makers in the IT department. Furthermore, often times the IT department will also determine how the retention requirements will be implemented. Therefore, it is crucial that the retention expert work closely with the IT department in a cooperative fashion, so that IT fully understands and is supportive of the retention policy crafted by the expert. Finally, it is extremely beneficial to also involve the legal department in crafting the policy and making retention decisions to ensure compliance, and executives to consider possible budget issues.

B. Litigation Readiness Experts

A litigation readiness expert plays a related role to that of a retention expert. However, the role is distinct from that of retention insomuch as it is broader and more process-based, requiring an even greater level of technical

expertise. Litigation readiness experts are retained to assist a company's IT department in working through implementation of the retention schedules.

i. Overview of Responsibilities of Litigation Readiness Experts

Litigation readiness experts proactively assist in determining ways to isolate key individuals' data or data types that are predictably to be sought in the event of a litigation or regulatory matter. They are generally hired on a proactive basis to implement processes ensuring that the company and its counsel can locate, preserve and collect data in a timely, cost effective manner. They can work with counsel and the IT department to get a clear understanding of how to best structure the IT environment, taking into consideration the type of organization and type of litigation or regulatory matter that commonly arises. Moreover, ESI experts in the litigation readiness role can assist you in modifying the established retention schedules in order to meet the needs of pending litigation. For example, if data related to certain custodians is commonly implicated in litigation, that data might best be hosted and backed up separately from infrequently-accessed data.

ESI experts in the litigation readiness role are frequently called upon to make judgments requiring both legal and technical expertise, although not usually attorneys. The following list of responsibilities commonly assumed by litigation readiness experts which should be used as a checklist of things an expert you retain has had experience handling:

1) Identify the likelihood that an organization will be named in litigation or a regulatory matter;

2) Determine which data will most likely be sought in the event of litigation or a regulatory matter;

3) Assist in the implementation of an Electronic Discovery Task Force and processes as discussed below in this section;

4) Identify software applications and customized databases;

5) Look at ways to modify the network environment to ensure that data is efficiently maintained when a preservation hold is implemented; and

6) Establish processes and protocals on how data will be handled. This may include:

    a. Preservation holds;

    b. Collection processes, including forensic imaging of data and ensuring that internal IT staff are properly trained;

c. Document review protocals;

d. Selection of a service provider for handling data in the event of a ligitation or regulatory matter, including conducting security audits and negotating contracts; and

e. Identifying which law firms, and which specific individuals within a firm, are prepared to handle electronic information. (The firm that may have served a company well for the last 20 years may not be the right firm to handle the technology of today.)

As can be seen from the above, the responsbilities of litigation readiness experts are different than those of retention experts, although they may be the same individuals operating in another step in a multi-step process that needs to be undertaken, or they may be more technical in their background.

There are many ways that a litigation readiness expert can assist in identifying ways to save money on a proactive basis in the event that such data is needed. It is common in certain network environments to see 50,000 to 100,000 employee e-mails sitting in one e-mail environment. This configuration can increase the costs associated with electronic discovery for many reasons. First, it is common for individuals to have personal, non-business communications in their mailbox. Second, it is common for individuals to work on more than one project during the workday. Additionally, only a fraction of the group's data may be required to be preserved as part of a litigation hold. However, lumping all the data together on a single backup system requires preservation of it all.

Attorneys should keep in mind that retention experts are looking at the nature of the business, the types of documents that are being created, and the retention periods assigned to different document types. In contrast, litigation readiness experts are the next step in the process and are looking at the identified document types, comparing them to defined retention schedules, identifying where the data it physically located, and determining what it will take to retrieve data. Litigation readiness experts are identifying "holes" in the IT infrastructure compared to the retenion schedules that are defined. They work with IT departments to determine what would it take to meet the retenion schedules as well as ensure that "business records" are being retained in a fashion that they can actually be recovered in a cost effective manner.

ii. Creating a Data Inventory

Litigation readiness experts require a complete inventory of what data is stored in what locations in order to fulfill their responsibilities of determing how to effectively retain information. A clear understanding of what data an organization has and *where* it is located is an inherent prerequisite to charting a course of action to preserve that information and retrieve it when necessary.

In an effort to meet regulatory and legislative requirements, many companies have become proactive in their electronic data management, and are beginning to gain an understanding of their corporate network infrastructures and how their business records are maintained. Creating an inventory, also sometimes called a data map, is a critical first step to being prepared for a litigation or investigation involving your organization.

A litigation readiness expert may choose to create either or both an Application Inventory or a Data Map depending on the specific needs and structure of the organization whose data he or she is inventorizing.

A typical **Application Inventory** would record the following about the client's computer applications on which its data is stored:

- ☑ Application name;
- ☑ Implementation/decommission dates;
- ☑ Primary function & business process;
- ☑ Abbreviations and acronyms;
- ☑ Version/patch history;
- ☑ Vendor information;
- ☑ Type of record created;
- ☑ Data storage location;
- ☑ Subject matter expert;
- ☑ Business and application owner;
- ☑ License information;
- ☑ Documentation location; and
- ☑ User information.

A **Data Map**, in contrast, is focused on the data rather than applications. A typical data map would record the following about the client's data:

- ☑ Data type;
- ☑ Application of origin;
- ☑ System location;
- ☑ Media type;
- ☑ Physical location of the data; and
- ☑ Supporting notes (database schemas, data dictionaries, file layouts, etc.).

This important first step of inventoring your organization's current data landscape requires retention of an experienced ESI expert who has technical training in identifying data types and locations. An understanding of the technicalities surrounding that data is crucial to implementing a response plan to make the preservation obligations (both legal and of the company as established in the document retention policy) a reality.

iii. Implementing a Response Plan & Team

Litigation readiness experts, as previously discussed, are responsible for implementing a response plan that make the retention policy actually happen in-fact. This requires that *policies, systems, and processses* should be established for the following:

- Identifying key custodians;
- Discontinuing of destruction and backup tape recycling policies;
- Identifying, storing, and safeguarding relevant active data and backup media;
- Maintaining critical information for accessing and reviewing potentially relevant data;
- Ensuring and documenting proper chain of custody; and
- Educating all employees on the organization's retention and destruction policies.

Litigation readiness experts can also assist an organization in the creation and implementation of an Electronic Discovery Response Team (Response Team). The importance of creating an effective Response Team cannot be stressed enough. The role of a Response Team is forward-looking to ensure future, continuing compliance with data retention and preservation policies. Future compliance with policies can be accomplished by processes such as a system for monitoring compliance and a system of regular trainings for both new and current employees which will educate the employees about retention policies and procedures.

Litigation readiness experts can help you determine who should be on the Response Team given the specific nature of your business and likely disputes. Generally, the Response Team should be comprised of multi-departmental professionals who can work collabortively with key personnel in each department to ensure relevant information is identified, preserved, and produced in the face of pending litigation or reporting requirements. The following is a checklist of personnel you should strongly consider having on your Response Team:

- ☑ Counsel
  - Corporate in-house counsel
  - Discovery counsel
  - Outside firm counsel
- ☑ E-discovery Expert Consultant
- ☑ IT
- ☑ Human Resources
- ☑ Corporate Security
- ☑ Business Line Managers

The Response Team should be authorized to quickly alter a document retention policy in the event of an emergency to ensure compliance with record preservation duties. Litigation readiness experts have first-hand experience and extensive knowledge they can apply to a company's specific situation to intelligently choose: (1) the most appropriate professionals to comprise the Electronic Discovery Task Force, and (2) the best procedures for the Response Team to follow.

C. Technical Assistance in Understanding Data Locations

The experts you retain to guide you through the intracrecies of handling workplace data will need to work closely with the company's Information Technology (IT) departments at each stage of the process from the initial establishment of retention schedules to collection, which will be discussed below. Established IT departments will already have a wealth of knowledge in dealing with an organization's electronic data and are an invaluable resource. IT departments are often referred to as internal experts, as discussed below.

There are two overarching types of IT departments: those that are internal to the organization and those that are outsourced. As noted earlier, in an effort to curtail administrative overhead, many corporations have outsourced their IT departments to one degree or another; again, this could mean as little has been outsourced as the backup environment or help desk, or it could be mean that the entire IT infrastructure has been outsourced.

It is important in any litigation or investigatory action to understand all of the locations of data and this task can become very daunting if the company is unable to find the right people within its employees or consultants to provide that information. Outsourcing this work overseas creates additional difficulties with the difference in timezones, languages, and laws. The use of experts for each type of configuration will be discussed separately below.

i. Internal IT Structure and the Internal Expert

For companies with an internal IT structure, the internal experts are critical to the company's ability to understand and identify locations of information; they are "the keepers of the key to the kingdom."

Some organizations retain qualified staff to handle data collection properly. In this situation, the attorney's job (regardless of the IT configuration of the company) is to understand the nature of the case, the locations of relevent data, the types of data required, and then to work with the IT department to make sure that IT can accurately collect the data. It is wise to personally meet with the IT representatives involved in the matter, since some of the biggest mistakes that can be made in an ESI matter relate to improper identification and collection of data. Attorneys should also be working directly with their client's IT staff whom are involved in collection. It is important to effectively communicate with IT personnel, using language and terminology that both sides can understand and agree on, about the scope of and best practices to use during collection Partnering with a preservation expert (*see* discussion above) can ensure proper preservation, collection, processing, and ultimately production of the data needed for the matter.

Attorneys have a tendency to say, "I want it all." This language, to an IT person, may and can be taken literally. Chances are the attorney doesn't really want everything. What the attorney is really looking for is just that which may be potentially responsive to the matter. To an IT department, however, all, literally means ALL. Thus it is extremely important that the attorney effectively communicate with IT staff to understand what they have, what data actually is needed, what is required to preserve it, and the best process for collection.

It is important to make sure that IT personnel have identified all locations of data, including informal individual-employee sources. It is only then that attorneys should look for problems or issues. For example, if the IT department indicates that there is an auto delete policy for e-mail after 14 days, the attorney's next step would be to identify how employees manipulate their in-boxes to get around this policy. The attorney may find that one person prints out their information, another burns it to a CD, and yet a third may download the data to a USB device and take it home for safe keeping.

After data source identification, the next step is data collection. Part of the function of the IT department is to enable employees to perform their jobs by offering the best available technology. The IT department's responsbilities include maintaining the network, loading updates on desktops and servers, and properly backng up the environment to ensure preparation for potential disaster. Most individuals are not trained on collecting electronic information for a litigation or regulatory matter. Likewise, most IT infrastructures are not equipped to absorb the time that will be needed to assist in the data collection. IT staff have regular, full-time jobs. The IT department may already be understaffed and a litigation or regulatory case only adds to their workload. Often times, corporate executives have come to rely on these individuals and their belief is that they can do anything. Attorneys need to make sure to inquire into the skill set of the IT staff and their time available to assist in collection, based on a careful estimate of the likely time commitment required for anticipated tasks likely to be involved in dealing with the matter.

When it comes to data collection, attorneys should also be sure to inquire into the specifics, rather than assuming that the IT staff knows how to properly collect data. It is very important to walk through the entire data collection process with the staff. If the attorney is not fully educated in adequate data collection procedures, they should bring along their data preservation and collection expert to this meeting to ensure that the process meets industry standards. This is one area in which huge mistakes can be made. Attorneys must constantly remember that electronic workplace data is fundamentally different from the paper data of yesteryear and requires special expertise to properly collect without risk of inadvertent destruction. If the data is improperly collected, an attorney may not be able to use it in a matter, or may be able to do so only at a huge additional cost. All too often there is no going back as was possible in the days of paper records if a scanning job went poorly.

After the attorney has identified the process that will be used to collect the data, it is important to also audit the process. For example, if the IT department has identified a process whereby individuals do a "self-pull" of data and transmit that data to the server, after which the IT department collects the data from the server, what process is going to be used to ensure that metadata isn't changed? Additionally, how does the IT department plan to "bucket" (i.e. organize) this data? Is it going to lump all the data together, or provide each individual with his or her own "bucket" for the information? How is the attorney going to make sure that the individual actually pulled all of the data that was relevent? When collection is done in such an ad hoc fashion without a distinct and established process for every custodian to uniformily follow there is an increased likelihood that future review of the production set will not include all responsive data as required by the preservation duty. Each of these elements needs to be considered to effectuate an efficient and accurate collection.

ii. External IT Structure and the External Expert

As discussed above, in an attempt to reduce costs, many organizations have outsourced some degree of their IT resources, from just the backup environment to the entire IT environment. This adds a huge wrinkle to the task of identifying not only locations of information, but also getting the data collected. The same obstacles discussed above for the internal expert also apply to the external expert. However, depending on what exactly is outsourced and where, the outsourcing can create additional major issues that require expert consideration in your matter. For example, when your IT functions are outsourced who is going to testify as to the manner in which data was stored and preserved and the processes used to collect that data?

The outsourcing scenario is an area where data is often improperly handled. Sources of data can easily be overlooked, and miscommunication may thwart understanding of the collection process. Outsourcing IT functionality does not release the organization from its duties to properly identify, preserve and collect relevent information. In this instance, it may be even more important than ever to engage a preservation expert to ensure that the manner in which data is being collected meets the needs of the matter.

III. The Use of Experts Post-Notice: Litigation and Investigation Roles

A. Preservation/Collection Experts

Preservation and collection experts are usually sought once the organization is on notice that litigation or a regulatory matter is about to ensue. It is advisable to seek these types of experts early on as opposed to late into the matter. They may be the same expert that assisted with the litigation readiness

evaluations, but it need not be. There are generally two scenarios: companies in a litigation readiness position and companies that are not operating in a litigation readiness position.

i. Companies in a Litigation Readiness Position

Some companies have done a great job of retaining retention and litigation readiness experts in advance and implementing the processes identified and maintaining the records in the fashion recommended. These organizations are in a far better position than those that merely spent the money to hire an expert and obtain recommendations but then inadequately implemented the expert's recommendations. In this prepared environment, a preservation expert should meet with the members of the Electronic Discovery Task Force, discussed above, along with the inhouse counsel and the outside counsel. Because of the advanced preperation, the preservation expert can easily be handed the "road map" of the network environment.

The primary responsibilities of a preservation and collection experts include:

1) determining where the relevent data is located;

2) determining the volume of data that is required;

3) recommending a reasonable preservation hold; and

4) when applicable, assisting counsel in creating an argument for a reduction in the amount of data to be preserved and collected.

With regard to creating a legal argument for a reduction in the amount of data to be preserved and collected, such arguments can be based on legal concepts such as relevancy (*see* Chapter 14, section A) and undue burden or cost (*see* Chapter 6, section A). These arguments, which are often highly technical to demonstrate, often require an expert to make convincly. For example, to be successful, an undue burden argument in federal court must show that data is not reasonably accessible; an expert is often needed to objectively and knowledgebly determine what is reasonably accessible in light of the expert's prior experience.

ii. Companies Not Operating in a Litigation Readiness Mode

Unfortunately, this is the scenario that occurs far too often. In an effort to reduce costs, the client may have either established a process for litigation readiness but failed to maintain it or may have failed to establish a process at all. In this scenario, a preservation expert may be retained to assist the client in understanding and implementing many of the things that a litigation readiness

expert would have assisted the client with previously. Had this been undertaken on a proactive basis, it could have been done during a time when individuals were under less stress, had fewer time constraints and were better able to make sound decisions; being in the midst of litigation or a regulatory investigation is not the ideal time to have to start identifying the disparate locations of corporate data. At this point, the expert should be assisting counsel in understanding what data should be preserved for the matter, not scrambling to make up for a failure to establish the groundwork for foreseeable needs for basic information on the corporate IT system.

When the work is done in the haste of impending or ongoing litigation, the preservation expert may recommend that a broader preservation hold be implemented rather than running the risk that relevent data might be overlooked. However, this situtation is not ideal, and may cost the company in several ways. First, data may be lost in the normal course of business during the time in which the preservation hold was being issued. Second, an overly broad preservation hold may result in holding far too much data, which increases the costs of IT resources to create and to store the additional backup tapes as well as increasing the potential costs of searching those backup tapes for responsive data. Lastly, retention of too much data and the resultant additional time required on both sides of the litigation to deal with the overload may increase the likelihood of a spoliation sanction for late production as the preservation experts are attempting to work with counsel under tight time constraints to understand the environment, identify and locate the relevent data, release irrelevent data, and determine the most cost effective manner in which to collect, process, and produce the data. During this time of analysis, counsel may have made good faith representations to the opposition, the court or investigative body that are impossible to carry out during the time agreed, if at all.

iii. International Data Transfer Experts

An emerging issue during collection of data that is growing in both prevelance and complexity is the need for international data transfer experts. The laws overseas regarding handling of data are very different than they are in the United States. For example, as discussed in Chapter 10, many countries in the European Union and Asia have strict data privacy and some have state secrecy laws. These foreign laws must be considered when a matter involves the collection and review of data that is not located within the United States. In the international context, it is important to identify whether the law firm and the service provider even have the legal authority to collect and review the data.

Attorneys should also consider whether the circumstances require a release to be signed by the individuals about whom the data concerns as required by many countries' privacy laws, and if sowhether that release is sufficient to extend to the service provider. For example, the Safe Harbor agreement between

the United States and the European Union[5] allows for the transfer of data in certain circumstances where private data might otherwise be non-transferrable. However, before rushing off to Europe to collect data, it is important to retain an expert that is well versed in the intricacies of the Safe Harbor agreement and is fully able to advise your organization on its particular issues.

These complex issues require knowledge of the foreign laws and how they interact with laws in the United States. Frequently, it is advisable to seek a local expert in the jurisdiction where the data you are seeking resides. Alternatively, ESI experts who have familiarity with international data transfer and knowledge of the local laws of other jurisdictions are recommended.

B. Forensic Experts

Computer forensic experts are crucial to the success of much litigation where data must be recovered that is not accessible to an active user of a computer or computer system. Computer forensics is the forensic recovery, authentication, and analysis of electronic data. The discipline of computer forensics is narrower in scope than electronic discovery, often dealing with the recovery and analysis of information on a single piece of media or a small number of media sources.

Computer forensics is in many ways similar to traditional physical forensics. While detectives dust for fingerprints at a crime scene, forensic experts likewise search for "digital fingerprints." Computer forensic experts endeavor to determine the "who, what, when, where, and how" of computer related conduct.

Forensic experts must follow forensically sound protocols to avoid altering the data. Metadata – data that contains information about data such as formulas, the creation date, and file size – can easily be altered by as little as turning on/off a storage device or searching for data. It is crucial that the forensic expert always make an exact bit-by-bit image of any storage devices prior to performing a forensic analysis, and that that the analysis be conducted on the forensic copy. This ensures there is evidence that the original data was not altered; a forensic expert can also testify at trial as to the protocols used to ensure no data was changed. In other words, a forensic expert can "authenticate" the data.

Forensic experts can often retrieve all or part of "deleted" files as the "delete" action does not physically remove data from a computer system until another file is stored in precisely the same location, thus overwriting the file. Similarly, data can frequently be recovered by a forensics expert from a hard drive that has been physically damaged (e.g. dropped, fire-damaged, or water-damaged).

---

[5] See the discussion in the section on the European Union in Chapter 10.

Moreover, forensic experts also frequently recreate computer conduct including specific chains of events. For example, a forensic expert can frequently determine whether and when a user used a wiping program or other measure to remove data from a computer, which can show bad-faith destruction of evidence and result in severe sanctions including dispositive sanctions such as summary judgment. Forensic experts also perform a myriad of other activities, including data authentication and password breaking.

A real world example of a trade secrets case illustrates the benefits of computer forensics. A company sought assistance in investing several former employees suspected of stealing the company's trade secrets. The night before forensic engineers were to image the hard drives in question, one of the former employees destroyed the computer evidence by deleting the incriminating information and then downloading approximately six gigabytes of MP3 files to the drives, thus overwriting the files. Even though no evidence of the trade secret misappropriation was recoverable, engineers presented their findings, which supported the company's claims that the former employee destroyed incriminating evidence.

Forensic experts are not needed in every case. However, they can be vital resources for both plaintiff and defense sides when it is suspected that a computer may reveal evidence upon a forensic investigation that is otherwise not retrievable; for a further discussion of the uses of forensic experts by plaintiffs, see Proving the Case, in *Representing Plaintiffs in Title VII Actions*, by Kent Spriggs.[6] For both parties, evidence recovered by forensic experts may be the "smoking gun" that proves their theory of the case. Computer forensics can establish facts to support the elements of a claim, refute allegations of computer malfeasance, and reveal evidence of spoliation, discovery misconduct, or data mismanagement committed by another party.

C. Litigation Hold Experts

ESI experts can also assist your company with developing, implementing, and tracking the process of a litigation hold notice. Once a party has been notified of, or can reasonably expect litigation, the party has a duty to preserve all potentially responsive information. According to *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003), a litigant is generally under a duty to preserve what is knows or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, or is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

Litigation holds should take effect *immediately* upon notice, even anticipation, of litigation. Keep in mind that data can always be destroyed later

[6] Aspen Publishers.

pursuant to a re-evaluated document retention plan, but destroyed documents are extremely expensive, and occasionally impossible, to recover.

The first step that should be taken in implementing a litigation hold is to send a preservation letter to all individuals in all locations involved in document destruction practice of potentially relevant information and instruct them to immediately cease destruction. To successfully initiate preservation, a preservation letter must be sent to all potential custodians, administrators, and stewards of relevant information; an ESI expert familiar with who typically retains what type of information will be able to assist organizations identifying custodians of information. A checklist of possible custodians will include:

- ☑ Employees;
- ☑ Independent contractors;
- ☑ Legal opponents;
- ☑ Partners;
- ☑ Websites and other telecommunication service providers;
- ☑ Law firms; and
- ☑ Vendors that are hosting company data externally from the company IT infrastructure.

An ESI expert can also help you draft the preservation letter so that is effectively conveys *what information to preserve* and *how to preserve it.* Providing written instructions on where information physically is located and what it takes to preserve it requires technical expertise given the fragile nature of electronic data (e.g. deleted data can be overwritten merely through normal daily computer operations and metadata can be altered merely by turning on a computer.

A preservation letter should communicate the following information to custodians:

- ☑ Statement of purpose for the hold;
- ☑ Description of the lawsuit or investigation and the pertinent issues;
- ☑ Specific guidelines for determining which documents and data should be maintained; and
- ☑ Statement(s) making it clear that recipients must err on the side of caution if they are not sure whether to preserve under the guidelines.

In addition to issuing a preservation letter to individual custodians, an organization must take organizational wide measures to ensure that data is not lost by suspending routine and automatic destruction practices. An ESI expert can help you identify what systematic actions need to be taken and to implement those actions. There are generally three areas that organizations must make systematic changes with regard to in order to meet preservation obligations: auto-destruct e-mail systems, routine overwriting of tapes, and defragmentation.

- **Auto-Destruct E-mail Systems:** In most organizations, the sheer volume of e-mail messages exchanged daily can be daunting. In order to prevent a system overload, many administrators implement auto-destruction features. If users wish to save a message, they must make a copy and save it to their local hard drive or their remote disk storage space on the file server. Organizations should immediately suspend an auto destruct policy if e-mail evidence needs to be preserved.

- **Routine overwriting of tapes:** System administrators often store backup copies of files and programs on tapes and generally perform "tape rotations." If tape rotation policies are not halted, the amount of available backup data could be significantly reduced or even eliminated all together.

- **Defragmentation:** Defragmentation software it is often used by individuals and organizations to remove files that may not be needed by the computer user. However, the same files that may be unneeded by one person may hold the key to a computer forensic investigation. In order to ensure that this data is preserved, any tools that perform automatic or routine drive "cleanup" must be halted immediately.

Also, because the litigation process can take years to resolve, and the roster of custodians frequently expands, it is a best practice to periodically re-issue litigation hold notices. ESI experts can also help you monitor the preservation efforts to ensure that preservation obligations are indeed being met by creating a tracking system. Increased storage needs can result from the need to preserve information pursuant to a litigation hold.

Parties are often asked to defend their preservation practices, which dictate that documentation and tracking of notices be maintained. A benefit of partnering with an external ESI expert is that he or she is a neutral expert who can testify to what preservation actions were taken. It is also common for simultaneous litigation holds to be in effect and a tracking system will ensure that only the right custodians and data for the correct matter are released from hold.

D. Search Experts

ESI Experts also play an important role in the e-discovery process in the processing, production, and review stages. Perhaps most importantly, an ESI expert is increasingly necessary to formulate and implement search plans. A number of recent cases have made clear that experts are a practical necessity and may be a requirement to meet ethical duties of competent representation.

In a case in early 2008, *Equity Analytics, LLC v. Lundin*, 2008 WL 615528 (D.D.C. Mar. 7, 2008), Magistrate Judge Facciola, in response to a search term dispute for a computer forensics examination, required the plaintiff to submit an affidavit from the forensics expert explaining: the limits of the proposed search, how the search is to be conducted, whether a mirror image would be a perfect copy, and whether there would be some reason to preserve the drive once imaged. This clearly is information requiring expertise to provide.

In *United States v. O'Keefe*, 2008 WL 449729 (D.D.C. Feb. 18, 2008), another opinion by Magistrate Judge Facciola, Facciola suggested that judicial review of search methods may require expert testimony: "Given this complexity, for lawyers and judges to dare opine that a certain search term or terms would be more likely to produce information than the terms that were used is truly to go where angels fear to tread. This topic is clearly beyond the ken of a layman . . . ."

Perhaps the most significant case yet to address the legal requirement of utilizing experts to perform competent searches is *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2008 WL 2221841 (D. Md. May 29, 2008), a case by Magistrate Judge Grimm. In *Victor Stanley*, Magistrate Judge Grimm found privilege waived regarding inadvertently produced documents, determining the defendants' reliance on an insufficient keyword search did not constitute reasonable precautions to prevent disclosure. The court specifically noted, "Selection of the appropriate search and information retrieval technique requires careful advance planning by persons qualified to design effective search methodology."

Victor Stanley also mentioned that, in its analysis why the keyword search was not a reasonable precaution against inadvertent waiver, the producing party failed to provide information about the following to the court:

- The keywords it used when doing privilege keyword search;
- The rationale for keyword selection;
- The qualifications of persons who made keyword selections;
- The sophistication level of the keyword search; and

- Whether any sampling or other quality control was done to ensure the accuracy of the keyword search.

The case law discussion above suggests a clear judicial trend towards requiring search experts to formulate and implement keyword searches in collaboration with parties to litigation. Because courts are also demanding that clients collaborate and attempt to reach agreement on e-discovery issues, it requires that the search expert work with opposing parties as well as their own client. The choice of search terms used determines how relevant the retrieved documents will be as well as how many relevant documents may be missed. This in turn determines the volume of retrieved documents which has a direct and substantial impact on the cost of discovery. Experts can help you craft a search to return the maximum number of responsive documents with least number of irrelevant documents possible. Experts can also assist in the review of these documents and quality control checks to make sure the search was indeed the best possible.

Advanced search technologies such as concept searching are another area where experts are especially useful in crafting search terms to identify responsive documents for review. Conceptual search retrieves documents from a data set without requiring the occurrence of the search term in the retrieved documents; rather, the query will return documents that are conceptually related to the search term. In *Disability Rights Council of Greater Washington v. Washington Metro Transit Authority*, Magistrate Judge Facciola suggested that concept searching is an efficient search method that is likely to produce more comprehensive results than keyword searching. The potential for great advances and cost saving exist with concept searching, but like keyword searching it does require an expert to make the most of by choosing the right words to query.

ESI experts can play additional important roles once the discovery process commences. One role is that experts can provide informed cost estimates to aid counsel and clients in preparing a litigation budget. Another role is in advising as to the best form of production which should be negotiated for by either the requesting or responding party. As the requesting party, it is important to request documents in a form in which all metadata remains intact and unaltered. An ESI expert can advise parties on which forms maintain data integrity as well as some of the advantages and disadvantages of native, TIFF, and other forms of production.

IV. EXPERTS IN COURT

A. Roles of Experts in Court

Experts frequently play a very important role as witnesses at trial. There are many subject matters that experts can testify to at trial, which have been

mentioned throughout this chapter. The following are several common subject matters about which experts provide valuable testimony or advice:

- **Preemptive Argument that the Court Should/Should Not Limit Discovery:** An expert can be used to make a premptive argument that the court should limit discovery under Federal Rule of Civil Procedure 26(b)(2)(B)[7] because the data is "not reasonably accessible because of undue burden or cost." Showing that data is not reasonably accessible for purposes of Rule 26(b)(2)(B) most often requires an expert to objectively and knowledgebly determine what is reasonably accessible in light of the expert's prior experience.

- **The Client's Conduct Was/Was Not Reasonable:** An expert can be used to show the reasonableness of a client's conduct regarding retention, preservation, and **collection** in the event that an adverse party makes a spoliation claim against the client.

- **The Search Techniques Used Were/Were Not Reasonable:** An expert can be used to show the reasonableness of a client's conduct regarding the search terms used to retrieve data. This is particularly important in the context of privilege waiver where searches are meant to retrieve attorney-client privileged and work-product protected documents and the reasonableness of those searches can determine whether privilege over those documents was waived.

- **The Evidence Is/Is Not Authenticated:** An expert can be used to demonstrate whether proposed evidence is authenticated. Authentication is a legal **requirement** that something is probably what it purports to be. Forensic experts can often demonstrate or disprove that data is the original that was created based on the data's metadata and history. Please refer to the section on Forensic Experts above for a more complete discussion.

- **Spolitation Did/Did Not Occur:** A forensic expert can often show whether **spolitation** occurred and often whether that data was intentionally destroyed by recreating a chain of events that show computer conduct. Please refer to the section on Forensic Experts above for a more complete discussion.

[7] Fed.R.Civ.P. 26(b)(2)(B) (2008).

B. Consulting and Testifying Experts

Attorneys must understand that there are two types of experts that can potentially be called to trial, particularly with regard to the second common purpose of using an expert at trial – showing the reasonableness of a client's data practices. The first kind of expert is the consulting expert who has worked with the client as either a retention, litigation readiness or preservation/collection expert. Consulting experts may be called upon at trial to testify regarding their conduct, advice given, and the defensibility or reasonableness of the advice given. Thus, attorneys and companies must take care to select a qualified consulting expert who will also be sufficiently articulate at explaining their conduct to be able to do so under cross-examination in court. Also, one should make sure that whatever consulting expert they hire is rigorous in documentation of their activities and recommendations, as this will greatly strengthen their credibility and persuasiveness at trial.

The second kind of expert is a testifying expert. This title testifying expert simply means that the expert called was not a consuting expert and did not personally involve him or herself in the conduct that is being evaluated. Rather, a testifying expert is meant to provide a more objective analysis. The logic to using a testifying expert rather than a consulting expert to prove the reasonableness of the data retention, preservation or collection conduct is that the consulting expert might be characterized as inherently biased because the conduct that is being evaluated is either the consulting expert's own conduct or conduct that was based, at lease initially, on the expert's advice.

The decision regarding whether to use a consulting expert or a testifying expert is one left to the discretion of the trial attorney based on the particular circumstances surrounding the need to call an expert at trial, as is the best manner to prepare the expert for trial and to present the expert's testimony. Choosing an expert who already has testifying experience will greatly decrease the level of preperation necessary and will also be likely to result in more persuasive testimony.

C. Preparing an Expert for Court

The selection, preparation, and presentation of experts at discovery hearings and trial is the responsibility of the trial lawyer. It is important to remember when preparing experts to testify at trial that ESI experts are technical experts. Accordingly, it is important to coach them to use language and explain concepts in a way that a judge and jury will understand. Selecting an expert with testifying experience is perhaps your best way to ensure you get an expert who will present well in court as he or she has already been through the experience and no doubt learned from it. One of the most challenging areas in the world of ESI is having a technical individual attempt to explain to laypersons how documents are created, stored and ultimately what happened to them during the discovery

process. If there wasn't proper documentation of the overall process, it is even more difficult for the expert to outline step by step the methodology that was used and whether or not such process is in fact valid. Remember, just as indicated above in discussions about the various types of experts, you may need different experts to describe what was done and whether such process/conduct met the minimum standard of care or not.

Federal Rule of Evidence 702, titled *Testimony by Experts*, provides general guidelines for the minimum requirements any ESI expert must meet before testify. Trial attorneys are advised to research the reputation of experts before calling them to testify. A good indicator that an expert is qualified to testify is that they have testified in the past regarding similar matters. Rule 702 reads:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

If your opponent is going to be calling an expert to testify, as with all other witnesses, you will probably depose them in advance of trial. When serving a Federal Rule of Civil Procedure 30(b)(6) deposition notice, the following are a check list of items you will typically want to notify a deponent who is an ESI expert (there will of course be variations depending on what type of experts and the facts and circumstances of the case) to prepare to testify regarding:

- ☑ Number, types, and locations of computers currently in use and no longer in use;
- ☑ Past and present operating system and application software, including dates of use;
- ☑ Name and version of network operating system currently in use and no longer in use but relevant to the subject matter of the action;
- ☑ File-naming and location-saving conventions;
- ☑ Disk or tape labeling conventions;
- ☑ Backup and archival disk or tape inventories or schedules;

- ☑ Most likely locations of electronic records relevant to the subject matter of the action;

- ☑ Backup rotation schedules and archiving procedures, including any backup programs in use at any relevant time;

- ☑ Electronic records management policies and procedures;

- ☑ Corporate policies regarding employee use of company computers and data; andIdentities of all current and former personnel who have or had access to network administration, backup, archiving, or other system operations during any relevant time period.

V. CHOOSING AN EXPERT

Another major obstacle that an attorney faces is ensuring that he or she has selected the right expert for the job. In balancing due diligence in representing a client with the "cost consciousness" of clients, mistakes can be made. Unfortunately, there is not a standard credential or degree that an expert must possess in the areas identified above, although such a credentialing system, may be on the future horizon as the data preservation and collection industry fully matures. However, because there is not currently a uniform credentialling system it is critically important for attorneys to talk to other attorneys in the industry, do their own research, and educate themselves on the reputation and experience of available experts to ensure that they are not selecting an inadequate expert based on poor information.

When a new individual has to be hired, attorneys, needless to say, must interview the experts that they are considering to use. The following are some considerations during the selection process:

- ☑ Does the expert have expierence on the particular subject matter you are dealing with?

- ☑ Does the expert have expierence and references from organizations that are similar to the size of your organization and in a similar industry?

- ☑ Is the expert familiar with the time constraints of the specific litigation or regulatory matter faced by your organization?

- ☑ What are the workflow processes?

- ☑ How well versed are they in a technical understanding not only the client's environment, but the standards in the industry for collection and processing of electronic information?

- ☑ What level of organizational backup support does the expert have in the event that he leaves that employer or is otherwise unavailable during the course of his duties with your matter?

- ☑ Can the organization implement the processes recommended?

- ☑ Do they have trial testimony expierence?

As a final note, in addition to making sure the expert a company chooses is a qualified expert, the company must make sure he or she is the right expert for the job you have; while a client may be able to use the same individual as an expert in multiple aspects as a retention, litigation readiness and preservation/collection expert, often they will need to hire different individuals with expertise in each specific area to meet their needs. For example, the retention expert may not be qualified to work through preservation or collection issues with the company and attorney. Also, this individual may have established policies that the company chose not to follow or simply didn't turn out to be workable given the IT environment. In sum, choosing the right expert for the right job requires a careful match between a company's specific needs and an expert's specific qualifications and expertise at each stage of the data retention, preservation and collection process.

VI. CONCLUSION

Every business is exposed to the possibility of a regulatory or litigation action, and acting proactively will save companies time and money in the long run. Regardless of the company's level of advanced preparation, retention of a skilled preservation expert once notice of litigation or a regulatory investigation is received is key. Companies and the attorneys representing them must make sure that the experts they have selected fully understand the matter, the network environment, and how to best help control costs without jeopardizing the end goal of retaining and preserving responsive data.

It is critical that companies and their attorneys have someone on their team that is adequately trained in the unique issues faced by organizations attempting to deal with data in an electronic format. Mistakes can happen, since no system is perfect, no person infallible. Discovery misconduct, even that stemming from negligence, in dealing with electronic data can lead to a variety of sanctions, including an adverse jury instruction, an adverse inference, monetary sanctions and in extreme cases, default judgement (*see* Chapter six, section B). Since the Federal Rule of Civil Procedure amendments went into effect in December 2006, there have been numerous cases outlining the repercussions that affect legal teams that are either unprepared to deal with ESI or deal with it in an insufficient or inefficient manner. For example, the court in *In re September 11th Liability*

Insurance Coverage Cases[8] imposed a $1.25 million sanction for discovery violations relating to the nonproduction of an essential document.

Some organizations may attempt to rely on the protections of what has been dubbed the "Safe Harbor" clause. Federal Rule of Civil Procedure 37(e) grants a limited amount of protection from sanctions in situations where destruction of information is caused by the routine, good-faith operation of an information management system. However, this provision fails to cast a large net and most courts faced with inadvertent destruction impose sanctions based on the parties' failure to implement a litigition hold and suspend routine destruction upon reasonable notice of litigation. For example, the court in *Doe v. Norwalk Community College*[9] refused to apply the Safe Harbor clause and issued an adverse jury instruction where the party failed to act affirmatively to prevent the operating system from destroying relevant information.

These cases outline the importance of being prepared for litigation or regulatory investigations in the new face of workplace data. It is not expected that every organization will have the knowledge to handle issues involving electronic data overnight, or on its own. However, it is important to be sure that someone on the team does have the requisite knowledge and is able to offer guidance that meets the business needs of the organization, while preparing the team for litigation, both existing and future. As previously mentioned, these experts can defend the reasonableness of a client's preservation efforts against sanctions in court should relevant data inadvertently be destroyed

As a parting thought, ABA Model Rule of Professional Conduct 1.1 requires attorneys to provide competent representation to their clients. The rule defines competent representation as the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. Very few lawyers would be deemed competent in issues of data location and collection, but that is not required by the rule. What is required for adequate preparation is inclusion of someone that is an expert in the areas in which an attorney's representation requires expertise.

---

[8] 2007 WL 1739666 (S.D.N.Y June 18, 2007).
[9] 2007 WL 2066497 (D.Conn. July 16, 2007).