



Tuesday, October 20
11:00 am–12:30 pm

906 Ediscovery Tool Kit 2: Search Alternatives, Review Alternatives and Discovery in the European Union

Cathy L. Clark
Corporate Discovery Counsel
IE Discovery, Inc.

John H. Hempfling
Global Litigation Management Counsel
Whole Foods Market, Inc.

Richard Munisteri
Vice President and Associate General Counsel
Live Nation, Inc.

Faculty Biographies

Cathy L. Clark

Cathy Clark joined IE Discovery, Inc. as corporate discovery counsel and has served in that capacity since. She has worked with numerous corporate legal departments providing guidance on issues surrounding discovery in litigation matters, and creating corporate-wide discovery management programs. She has worked directly with in-house and outside counsel in charge of cases to provide strategic guidance and expert assistance. She has worked with counsel on several complex litigation matters involving antitrust, patent, employment and contract disputes guiding in-house and outside counsel through complex discovery requests involving terabytes of data.

Prior to her tenure with IE Discovery, Inc., Ms. Clark worked as a prosecutor for the City of Houston and for a computer forensics firm based in Chantilly, VA.

Ms. Clark is a member of both the Houston Bar Association and ACC.

She received her undergraduate and law school degrees from the University of Houston.

John H. Hempfling

Global Litigation Management Counsel
Whole Foods Market, Inc.

Richard Munisteri

Richard Munisteri is vice president and associate general counsel for Live Nation, the world's leading concert promoter, at its headquarters in Beverly Hills, California. He serves as head of litigation, managing the company's docket of lawsuits, arbitrations, administrative proceedings, and regulatory and governmental affairs matters globally.

Previously, Mr. Munisteri was general counsel to the State Comptroller of Texas at the capital in Austin. Before then, Mr. Munisteri was in private practice as a civil trial attorney – as a shareholder in the Houston law firm of Munisteri, Sprott, Rigby, Newsom & Vincent, P.C., and formerly as an associate in the Houston office of Griggs & Harrison, P.C.

Mr. Munisteri holds a JD from the University of Houston Law Center and a bachelors from the University of Texas at Austin.

ACC Association of Corporate Counsel

E-Discovery Tool Kit, Part 2

Discovery in the European Union

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Background of EU Restrictions

In WWII, a person's private data was often the source used to identify and segregate "undesirables."

European attitudes toward privacy were born of the misuse of such private information.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Introduction: Governing Bodies

- The Hague Convention
- European Union Privacy Directive
- Individual Countries' Laws/Regulations
- Master Contracts
- US Department of Commerce Safe Harbor

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Introduction: Other Examples of Privacy Concerns

- Radio Frequency Identification Tags
- Surveillance Systems
- GPS Monitoring Systems

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Time & Cost of EU Discovery

- More time to **assess** requirements
- More time to **collect** consent from custodians
- Additional cost of **processing in the host country** prior to transferring data
- Be prepared to **demonstrate** these to opponent and court

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

European Union Privacy Directive

Data Protection Directive (95/46/EC)

Provides guidance to what corporations can and cannot do with private data.

Does not apply to corporate data (policy manuals, templates, corporate financial documents, etc.)

Must also consult local country's laws or regulations

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

European Union Countries

Austria	Germany	Netherlands
Belgium	Greece	Poland
Bulgaria	Hungary	Portugal
Cyprus	Ireland	Romania
Czech Republic	Italy	Slovakia
Denmark	Latvia	Slovenia
Estonia	Lithuania	Spain
Finland	Luxembourg	Sweden
France	Malta	United Kingdom

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Data Protection Directive

Two Restrictions:

- Restricts "Processing" of private data
- Restricts "Transferring" of private data outside the EU

Determination:

- Does the target data contain private data?
- If so, determine if what you intend to do with the data would trigger either or both restrictions

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

"Personal Data"

- > Personal Data is any data that describes or relates to a particular person
- > Interpreted VERY BROADLY
- > Not just identification numbers, medical information, but any document that provides a name or other personal information – includes email
- > Contracts can have signatures, user manuals and sales material can have contact information, etc.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

“Processing”

- Not defined in similar manner
- Any collection, storage, alteration, retrieval, or transmission of data
- Thus, any movement or purposeful retention constitutes “processing”

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

Lawful “Processing” of EU Data

Must satisfy one of the following requirements:

Consent
Legal Obligation
Legitimate Interest

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel


Consent 1

Defined as “any freely given specific and informed indication of his [the data subject’s] wishes by which the data subject signifies his agreement to personal data relating to him being processed.”

General consent via corporate policy, as part of employment or not particular to a pending matter is insufficient.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




Consent 2

Must be:

- Specific to the reason for "processing"
- Given freely by the data subject (more on that)
- In writing (more on that)
- Revocable at any time without repercussion to the employee (if collecting from an employee)
- Cannot "reuse" or "repurpose" consent

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




Tip #1

3rd Party or Customer Data

If you have databases with customer data, work with your IT staff or discovery vendor to replace sensitive information with place holders. This will eliminate the need to contact each and every customer whose information you need to collect for a litigation matter.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




Legal Obligation

Processing must be necessary to comply with a legal obligation.

- "An obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation . . ."
- Some EU Data Protection Authorities have said this only applies to legal obligations from other EU countries.
- And notice should still be provided to the data subjects regardless of a legal obligation

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




Legitimate Interest

Processing must be necessary for the purposes of a legitimate interest.

- “Against these aims have to be weighed the rights and freedoms of the data subject who has no direct involvement in the litigation process . . .”
- Balancing Test: “take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject.”

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!




“Transferring” Data

Personal Data cannot be transferred outside the EU to a non-EU country unless there is adequate data protection.

- Articles 25 and 26 apply
- The Directive prefers application and approval by The Hague – very cumbersome and time consuming
- Other avenues: US Dept. of Commerce’s Safe Harbor (www.export.gov/safeharbor) or participating in Model Contracts (not covered here)
- Some countries have instituted “blocking” statutes specifically to thwart US-style discovery (i.e. France)

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!



France’s Blocking Statute

Prohibits virtually anyone connected with a French company from transferring data related to economic, commercial, industrial, financial or technical information to any foreign public authority.

Instituted in 1980 to specifically to stop US-style discovery.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

**Societe Nationale Industrielle
Aerospatiale vs. U.S. Dist. Court**

US Supreme Court Case 482 U.S. 522 (1987)

1. The importance to the litigation of the documents or other information requested
2. The degree of specificity of the request
3. Whether the information originated in the US
4. The availability of alternate means to secure the info.
5. The extent to which noncompliance with the request would undermine important American interests or compliance with the request would undermine important interests of the state where the information is located

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

ACC Association of Corporate Counsel

**Cour de Cassation Chambre
Criminelle**

December 12, 2007, the Cour de Cassation fined a French attorney \$10,000 euros for attempting to informally collect information from MAAF, a French mutual insurance company, for a lawsuit pending in California in violation of the French blocking statute.

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!


ACC Association of Corporate Counsel

Other considerations (not exhaustive)

- **Collection:** you cannot repurpose data. Means data collected for one reason cannot be reused for any other purpose.
- **Filtering:** filter irrelevant data out of the collection while data still resides in host country; export only relevant data. Means hiring a local, trusted data vendor to filter prior to transferring data.
- **Access:** any data subject whose information has been collected or preserved must be allowed access to that information in order to "check its accuracy and rectify it if it is inaccurate, incomplete or outdated." Do we see any problem with altering the data collected?

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!



Steps to Take Now

1. Discuss w/Opposing Counsel & Court Early	4. Plan for Consent
2. Understand your IT Architecture Abroad and Map the Data along corp vs. personal lines	5. Educate Overseas Employees and Internal/ External counsel
3. Understand How your Document Retention Policies Affect Data in the EU	6. Identify Discovery Vendors who understand EU restrictions
	7. Investigate Safe Harbor Designation
	8. Consider the Location of your IT Hubs

2009 Annual Meeting
October 18-21 Boston

Don't just survive. Thrive!

Primer on Discovery in the European Union:

By Cathy Clark, Corporate Discovery Counsel, IE Discovery, Inc.

Discovery is a tricky subject in the European Union as the laws in the EU vary by country and are far more restrictive regarding the use of personal information. It is believed that the difference in viewpoints dates back to World War II and the use of private information to identify particular people by religion, ethnic origin or by other indicators. When viewed in that light, the protective attitude toward privacy and private data is much more understandable. Because of the proliferation of electronic data and the broad nature of US discovery, the differing viewpoints were destined to collide. This document does not seek to explain every directive required of a corporation for compliance with data privacy or even discovery in the EU. Rather it gives insight into some of the many laws that are required when completing discovery efforts in the EU. When faced with a specific litigation request that touches data in the EU, you will need to research that particular country's laws as well as other regulations before conducting discovery.

Also, understand that conducting discovery in the EU will add time and cost to your schedule and budget. If you are faced with discovery in the EU, begin talking early with opposing counsel and the court in order to apprise each of the challenges you will face with discovery. Be prepared to cite to specific laws in the target country and back up your statements with a schedule or time table for expected compliance or why you believe that you cannot lawfully comply and seek another solution. Discovery in the EU is largely based upon consent, and the type of consent required will mean more time in the collection effort. The more specific you can be in your explanation, the more likely you will gain the sympathies of your court.

European Union Privacy Directive

The European Union's Data Privacy Directive provides guidance as to what corporations can and cannot do with private data. In the European Union, a corporation must consult the European Union's Data Protection Directive (95/46/EC) and the particular country's privacy laws and/or blocking statutes for potential additional restrictions.

Data Protection Directive

In simplistic language, the Data Protection Directive places two primary restrictions on entities in discovery. First, it restricts "processing" of personal data and restricts when this can occur. And it limits the "transfer" private data to another country by a corporation. Therefore, if you

find yourself needing to handle data in the European Union, you must determine if it is or contains “personal data,” if so, then you must determine if what you intend to do with the data would trigger either or both of the above mentioned restrictions.

“Personal Data”

“Personal Data” is generally considered to be any data that relates to a particular person. In the EU, that definition is interpreted very broadly. It not only includes such personal information as identification numbers, addresses, familial information or medical information, but also includes any document or data point that is likely to disclose personal information such as a person’s name displayed in their email address. In the US, it is generally accepted that there is no expectation of privacy in corporate email, but in the EU, because email reveals a person’s name and potentially other personal information, it is considered “personal” and therefore private. Because of this broad interpretation, essentially any data that is not generic to the corporation will likely be considered personal data. Personal data has two restrictions placed upon it: how you can process it and how you can transfer it – both of which typically occur in US-style discovery.

“Processing”

“Processing” is not defined by the EU in the typical fashion that lawyers in the US define it. “Processing” is broadly defined as any collection, storage, alteration, retrieval, or transmission of data.¹ In other words, virtually any movement or purposeful retention of data can constitute “processing” under the directive. This *includes litigation holds* as recently stated by the Data Protection Working Party in their Working Document of January 2009.² In order to lawfully process data under Article 7 of the Directive, “processing” of private data must meet one of three criteria:

- **Consent:** The data subject’s consent is defined as “any freely given specific and informed indication of his [the data subject’s] wishes by which the data subject signifies his agreement to personal data relating to him being processed”³ However, general consent such as part of corporate policy or as part of the hiring process is insufficient. Consent must be specify the categories of data to be collected and the purpose of collection, be in writing and revocable at any time. Considering the above statement that the Data Protection Working Party considers purposeful retention under a litigation hold policy as “processing,” you can quickly see how gaining “consent” from each

¹ EU Data Protection Directive 95/46/EC

² WP 158, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted February 2009, pg. 8.

³ Ibid.

custodian might immediately impact your ability to comply with applicable laws while also complying with discovery responsibilities in the US.

- **Legal Obligation:** Processing must be necessary to comply with a legal obligation, however, “An obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation” under the Directive.⁴ Some EU data protection authorities have further interpreted this exception to apply only to legal obligations from other EU countries and not legal obligations from countries outside the EU. Additionally, EU authorities evaluating this exception have stressed that notice should always be provided to the data subject regardless of whether or not there exists a proper legal obligation. Thus, it seems to point back to gaining the consent of each custodian.
- **Legitimate Interest:** Processing must be necessary for the purposes of a legitimate interest. “Against these aims have to be weighed the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating parties and is deemed relevant to the issues in hand, e.g. employees and customers.”⁵ The Directive does provide a balancing test for compliance, it must: “take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject.”⁶ Again, the Directive seems to point back to the impact to the individual custodian and seems to stress again the importance of notice and consent.

It becomes apparent that compliance with any of these criteria will be very challenging. Each one of the above criteria requires specific compliance that may be difficult to achieve. While adoption of the directive’s viewpoint varies from country to country, the Data Protection Working Party compounds the problem by throwing considerable doubt on whether or not a data subject who is an employee of a corporation can ever freely give consent due to the implied threat that non-consent might have upon that employee’s employment and certainly doubts whether customer information can ever be exported without gaining the express consent of the customer or 3rd party.⁷ Therefore, while consent seems the most obvious choice of the above options, “consent” must be given explicitly, must relate only to the pending litigation matter in question, be in writing, and be revocable at any time and without repercussion to the employee.⁸ And if you are in France, it must be written in French.

⁴ Ibid, pg. 9.

⁵ Ibid.

⁶ Ibid, pg. 10

⁷ Ibid pg. 8; “The main argument underlying the US jurisprudence since the Aérospatiale case is that if a company has chosen to do business in the United States or involving US counterparts it has to follow the US Rules on Civil Procedure. However, very often the data subjects such as customers and employees of this company do not have this choice or have not been involved in the decision to do business in or relating to the United States.”

⁸ Ibid.

Transferring Data

When considering transferring data outside the EU, Articles 25 and 26 of the Directive apply. These Articles prohibit transferring private data to a non-EU country unless that country has instituted adequate data protection laws, participates in the US Department of Commerce's Safe Harbor program or participates in Model Contracts. The EU Commission has designated only a few countries as having "adequate levels of protection." They are: Argentina, Canada, Guernsey, Isle of Man and Switzerland.

In addition, many countries have adopted what are referred to as "blocking statutes" that pile on additional restrictions. Unfortunately, many of these blocking statutes were designed specifically to thwart US-style discovery. For example, in France, the statute prohibits virtually anyone connected with a French company from transferring data related to economic, commercial, industrial, financial or technical information to any foreign public authority.⁹

In 1987, the US Supreme Court ruled in *Societe Nationale Industrielle Aerospatiale vs. United States District Court*¹⁰ that the Hague Evidence Convention does not pre-empt a US Court's jurisdiction over the litigants present in its court whether or not those litigants are foreign entities. Therefore, the Convention does not pre-empt the discovery rules present in the Federal Rules of Civil Procedure.¹¹ When evaluating a discovery request in light of EU data restrictions, the test created by the Supreme Court includes five factors:¹²

- the importance to the litigation of the documents or other information requested
- the degree of specificity of the request
- whether the information originated in the United States
- the availability of alternate means to secure the information
- the extent to which noncompliance with the request would undermine important American interests or compliance with the request would undermine important interests of the state where the information is located

In the past, most litigants have cited foreign laws as their reasoning for an inability to comply with a discovery request stating that to comply would put the company or its counsel in jeopardy of prosecution. However, until recently, no foreign court had sought to enforce their data protection statutes. Thus, most US courts, over the years, had determined that the threat of prosecution was a hollow one and, therefore, justified the court in ordering discovery in

⁹ Law No. 80-538 of July 16, 1980, Journal Officiel de la Republique Francaise, July 17, 1980, p. 1799.

¹⁰ 482 U.S. 522 (1987).

¹¹ *Aerospatiale*, 482 U.S. at 544 n. 28 & 29.

¹² *Aerospatiale*, 482 U.S. at 544 n.28

defiance of the blocking statutes.¹³ That reasoning changed on December 12, 2007 when the Cour de Cassation Chambre Criminelle fined a French attorney \$10,000 Euros for attempting to informally collect information from MAAF, a French mutual insurance company, for a lawsuit pending in California in violation of the blocking statute.¹⁴

Now litigants, at least French litigants, will have proof that criminal prosecution is no longer an idle threat. It also stands to reason that other European and non-European countries will follow the French lead and begin to enforce their privacy laws and blocking statutes in order to force American courts to at least consider foreign laws in discovery. In fact, just such views were stated at the European Commission's Data Protection Conference held on May 19-20, 2009. During the conference, data protection authorities emphasized that they intended to put more effort into enforcement.¹⁵ Not good news for US corporations with operations in the EU.

Brief Discussion of Collection, Filtering & Access

Under Article 6, the Directive states that only information relevant to the specific litigation matter should be collected or preserved. Additionally, data collected for one purpose, such as another litigation matter or for another purpose such as Human Resources, cannot be repurposed for the instant litigation. Each individual collection effort must adhere to the above cited rules and be able to stand independently from another collection effort.¹⁶ Therefore, even if you have specific consent to collect and process private data for one litigation matter, you would need to gain the consent again if the same data were relevant to a different litigation matter.

The Directive also addresses filtering and collection specifically and advises corporations to filter their collections in the Member state prior to transferring the data to a non-member state. The Directive reasons that any collection effort will likely encompass information that will not be relevant to the specific litigation. And, in order to protect that information from disclosure, the corporation should filter out irrelevant information before it transfers information, thus exporting only that information that is truly relevant to the present litigation.¹⁷

¹³ See *In re Vivendi Universal, S.A. Secs. Litig.*, No. 02 Civ. 5571(RJH) (HBP), 2006 WL 3378115 (S.D.N.Y. Nov. 16, 2006), *Bodner v. Banque Paribas*, 202 F.R.D. 370 (E.D.N.Y. 2000), *Strauss v. Credit Lyonnais SA*, 242 F.R.D. 199 (E.D.N.Y. 2007).

¹⁴ Statute No. 80-538 Collection of certain business data for foreign litigation matters can only be accomplished via The Hague Convention.

¹⁵ <http://webcast.ec.europa.eu/eutv/portal/archive.html?viewConference=7334> for complete recording of the Conference.

¹⁶ WP 158, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted February 2009, pg. 10.

¹⁷ *Ibid*, pg. 11.

Finally, any person whose information is collected or targeted for collection must be allowed access to that information in order to “check its accuracy and rectify it if it is inaccurate, incomplete or outdated.”¹⁸

Steps to Take for Compliance and Readiness

Corporations in the US can take several steps to help ready them for discovery in the EU. Of course, these steps are much more easily accomplished in advance of litigation, yet we all understand that budget constraints make accomplishing this goal elusive.

1. Discuss with Opposing Counsel Early: as stated at the beginning, discussion of your challenges with both the court and opposing counsel will go a long way toward mitigating issues further down the road. Gather all the information you can about the laws and regulations that you must comply with, the anticipated amount of time to gather consent or satisfy another requirement for collection, any particular challenges with the data architecture, and the amount of time to filter in the host country, etc. Proving your challenges rather than simply stating them will greatly aid in your efforts.
2. Understand Your IT Architecture Abroad: mapping your data architecture overseas before litigation strikes will greatly assist you in your efforts to identify data that falls under the aegis of the European Commission’s Data Privacy Directive. Identify IT personnel responsible for data overseas and tap their knowledge of what steps would be involved in extracting relevant data from those systems and hardware. Once you have a data map, begin to amass knowledge of those particular countries’ data protection laws and familiarize yourself with the level of effort that will be necessary in the event of US discovery.
3. Understand How Your Document Retention Policies Affect Data in the EU: review your policies regarding document retention in the EU and consider any impact or implications these policies may have upon your ability to comply with US discovery. Policies may need to be altered in order to adequately comply.
4. Plan for Consent: the safest avenue to collect data in the EU, absent a Safe Harbor designation, is to gain consent from the employees that you are targeting for collection. Because the Directive is so specific as to the requirements of consent, plan now for how you will gain consent from employees. Remember, consent must be specific to the current litigation, be freely given, be in writing and be revocable at any time and without repercussion to the employee. Drafting language to that effect now will save you time and effort in the future.

¹⁸ Ibid, pg. 12

5. Employee Education and Internal/External Attorney Education: employees abroad are not often familiar with US-style litigation. When requesting data from such employees, US attorneys often find that these employees do not understand the nature or the extent of the request. Companies who take the time to educate their EU workforce as to US discovery requests and litigation holds will find that their compliance and collection efforts are much more accurate and smooth. Also, keep in mind that many Europeans take extended seasonal holidays, therefore, planning for discovery timetables may need to encompass such periods when a large percentage of the workforce may be unavailable.
6. Identify Discovery Vendors in your EU countries: if you have data in the EU, likely at some point you will need to extract data for a pending matter. Identifying credible, reliable and knowledgeable vendors will help you avoid legal pitfalls. The Directive favors the filtering of data prior to export, so having a list of vendors at the ready will aid in your ability to both comply with US discovery and also comply with local regulations.
7. Investigate Safe Harbor Designation from the Department of Commerce: in lieu of gaining consent from each individual custodian, you might be able to attain Safe Harbor designation in advance from the Department of Commerce. Investigate if your company can participate and what steps you would need to achieve in order to satisfy the requirements. See www.export.gov/safeharbor for more information.
8. Consider Altering the Location of Your Data Stores: the location of custodians and where they create data is controlling in determining what laws govern, but choosing a less restrictive central location for the overall storage of data from several European countries may reduce the amount of effort you have to expend in collection. Meaning that you may save yourself effort if your data storage is in country whose laws are not as restrictive as others. While this would not negate the effect of restrictive laws upon those custodians working in the restrictive countries, it might eliminate unnecessarily subjecting custodians who reside in less restrictive countries to more restrictive laws.

John H. Hempfling, II
Global Litigation Counsel
Whole Foods Market

I. Biographical Information

II. Introduction

Let me begin this paper by pointing out that it is with no small degree of trepidation that I dare to instruct other lawyers in avoiding the numerous dangers inherent in the world of e-discovery. With that said, I have now engaged in several large-scale electronically stored information (“ESI”) collection efforts and I have sat through more than my fair share of seminars, webinars, and barroom discussions covering the topic. I have found that while there are many litigators who can cite line and verse on the rules of discovery and court opinions covering this topic, there are *very few* who can actually bridge the gap between the law and the technology—which is the very heart of the issue.

E-discovery is one of the most important (and expensive) stages of the litigation process, and in order to do it correctly it is vitally important to build a team of lawyers and technology experts who can communicate with one another and the opposition in order to make the process go as smoothly as possible. (Note that I say “as smoothly as possible”; this process is frustrating and rife with complicated problems that will appear just when you think you have the situation well in hand—no matter how good your assembled team may be.)

To underscore the complexity involved in devising a thorough e-discovery plan, I offer the following quote from a recent court opinion:

‘Whether search terms or ‘keywords’ will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics, and linguistics. *Given the 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 and requires that any such conclusion be based on evidence that, for example, meets the criteria of Rule 702 of the Federal Rules of Evidence . . .’ It is time that the Bar—even those lawyers who did not come of age in the computer era—understand this.

William A. Gross Constr. Assoc., Inc. v. Am. Mfr. Mut. Ins. Co., 256 F.R.D. 134, 135-36 (S.D.N.Y. 2009) (citing, in part, *United States v. O’Keefe*, 537 F.Supp. 2d 14, 24 (D.D.C. 2008) (emphasis added).

I have also found that, while there are a number of CLEs covering e-discovery, it is difficult to find one that uses plain English to instruct those who are unfamiliar with the technology side of things. As a result, many technology-challenged lawyers (and I include myself in that group) become hopelessly lost and end up walking away from the lecture with more questions than answers—and inevitably awakening sweat soaked and terrified in the middle of the night from a recurring nightmare in which the judge (played by the Grim Reaper) drops his gavel (actually a scythe in the dream) and issues draconian sanctions followed by a skewering written opinion that highlights for the world how woefully inadequate their e-discovery plan turned out to be.

For that reason, while I would be remiss in not including recent opinions discussing e-discovery, I have tried to impart to the reader the practical lessons from each case. I have also studiously avoided using technical terms (such as “terabyte”—the knuckle-dragger definition of which is “a passel of electronic stuff”) wherever possible in order to keep you hooked in with my keen wit rather than blinding you (or more likely boring you) with my mastery of all things technical (a lightning bolt actually struck my house as I wrote that). For those technical terms that I do use I try to include a non-technical definition; although, the reader should consult a real e-geek to confirm whether my definitions have any basis in fact.

III. Creating and Implementing a Defensible E-Discovery Plan.

ESI is found in a variety of different formats and in an increasingly mushrooming assortment of locations. Parties to litigation have both the right and the duty to seek out this information, produce the relevant information to the opposition, obtain relevant information from the opposition, and, ultimately, to use it as evidence to prove their claims or defenses.

There was a time in the not-too-distant past when judges and lawyers alike shied away from the mere attempt to use ESI as evidence. One former federal judge disparaged an attorney for relying on evidence discovered on the internet stating: “So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion . . . Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form . . .” *St. Claire v. Johnny's Oyster and Shrimp, Inc.*, 76 F.Supp. 2nd 773, 774-75 (S.D.Tex 1999).

The judge who wrote that particular opinion is no longer on the bench (for reasons wholly unrelated to his views on ESI) and ESI has become a major component of many cases. Today, judges in both federal and state courts are becoming increasingly savvy with regard to ESI, and are also becoming increasingly intolerant of lawyers' failures to properly craft discovery plans addressing ESI.

Two areas rife with danger in the e-discovery arena are the preservation and collection of relevant ESI in order to avoid allegations of spoliation, and protecting privileged documents through the implementation of a sound discovery plan *coupled with a judicial order incorporating the plan*. Because of the massive amount of ESI that is often subject to discovery, conducting a document-by-document privilege review prior to producing ESI is both prohibitively expensive and impossibly time consuming. Lawyers should *not* rely on “claw-back” agreements with opposing counsel unless they have not only incorporated *reasonable* steps to maintain the confidentiality of privileged material, but also sought incorporation of those steps into a judicial order.

Judge Grimm, a United States Magistrate Judge for the District of Maryland, has written extensively (and eloquently) on the topic of e-discovery. In 2005 (before the adoption of the new Federal Rules governing e-discovery), Judge Grimm addressed a discovery dispute involving the proper method for conducting a privilege review involving voluminous ESI in *Hopson v. Mayor of Baltimore*, 232 F.R.D. 228, 230 (D. Md. 2005). In *Hopson*, Judge Grimm pointed out that there are three positions taken by courts in determining whether a party has waived the attorney-client privilege: 1) the “strict-accountability” approach in which the privilege is waived in almost every circumstance that privileged material is produced (regardless of whether the production was inadvertent); 2) the “lenient” approach in which the privilege is not waived unless the material is intentionally produced or a party is grossly negligent in its relinquishment of the material; and 3) the “balancing test” approach in which the court engages in a case-by-case inquiry into whether the conduct leading to disclosure is excusable. *Id.* at 235-36.

The practical lesson from the *Hopson* case is that if lawyers prepare their e-discovery plans with the assumption that the court will adhere to the “strict-accountability” approach, then they will likely succeed in avoiding spoliation issues and “clawing back” any documents that are inadvertently produced to the opposition. Generally, Judge Grimm noted in *Hopson* that a party seeking to preserve privilege claims must: 1) take *reasonable* steps to conduct a privilege review given the volume of ESI and the time permitted in the scheduling order to conduct the review; 2) take *reasonable* steps to assert the privilege once it learns of an inadvertent production of confidential information; and 3) production of the confidential ESI must be compelled by court order (in other words: have the court incorporate the e-discovery collection and screening methods into the scheduling order). *Id.* at 242.

The question then is: What specific steps are *reasonable* in collection and privilege review of voluminous ESI to avoid spoliation and maintain the confidentiality of the documents? (Note that I continually put the word “reasonable” into italics: the Federal Rules of Civil Procedure (and many state courts are adopting similar, if not identical rules regarding ESI) and the cases interpreting those rules require that only reasonable steps be taken.) While the answer to that question will necessarily depend on the circumstances of the particular case, a few steps should be generally undertaken. These steps will not only ensure that you are properly preserving and collecting relevant ESI (and thus protect you from accusations of spoliation later down the road), but are also

necessary if privileged ESI slips through your screening efforts and ends up in the hands of your adversary.

The first step, after issuing your litigation-hold notice, is to make sure your legal counsel is both fully aware of the rules regarding ESI (which as I stated is a fairly common trait in litigators that routinely litigate large cases) *and* able to understand the technical side of the equation so that he or she can communicate with in-house IT personnel and/or retained technology experts. This second part of the equation is much more difficult to find. Many law firms boast the ability to address the technical side of e-discovery, but very few that I have talked to truly have this ability. (As a litmus test, if the firm in question doesn't show up with at least one lawyer packing his or her own pocket protector you don't want them.)

Once you are confident your legal counsel has a team that can bridge the gap between the legal and technical worlds, the litigation team needs to educate itself on the IT systems used by your company. Remember that in-house IT personnel may be perfectly capable of maintaining the software and hardware utilized by your company, but they are not always litigation savvy. Along those lines, IT personnel may not appreciate the difference between the manner in which ESI may be collected or viewed in the everyday running of the business versus the manner in which it needs to be collected for litigation. (That's not a knock on the IT guys; it's just a reality that acting as an expert witness in litigation generally isn't in their job description.) In order to ensure that your e-discovery plan is designed to capture all relevant ESI, your lawyers (and their outside IT or forensic experts) have to be able to question your in-house IT personnel on the types of ESI stored by your company and on the locations where the ESI is stored. If your litigation team fails to ask the right questions, they may not (and probably will not) get a complete picture of where and how to find relevant ESI.

If the litigators themselves are not dedicated techno-geeks (and there are very few of these that I am aware of), then they will need to bring in an outside expert to assist them in developing a defensible e-discovery plan (and should anyway because you do not want your lawyers or your own IT personnel being the "experts" that testify as to the search methods undertaken by your litigation team in the event you are challenged by opposing counsel). One court recently reiterated this point stating, "determining whether a particular search methodology, such as keywords, will or will not be effective certainly requires knowledge beyond the ken of a lay person (or lay lawyer) and requires expert testimony that meets the requirements of Rule 702 of the Federal Rules of Evidence." *Equity Analytics, LLC v. Lundin*, 248 F.R.D. 331, 333 (D.C. Cir. 2008).

Outside experts should work with your own IT personnel to determine where ESI is stored and the types of ESI your company routinely uses. (I am not even going to attempt to describe all of the various software, hardware, shared drives, structured data, and back-up data that this may include, but you get the picture.) One very important element of this discussion is to determine what data is *reasonably* accessible and will not break the company's budget to access and search. Remember the watchword is "reasonable" and the burden is on you to demonstrate what will be overly burdensome.

Meanwhile, litigation counsel is simultaneously working through a list of custodians previously developed for the litigation-hold to determine who may have relevant records and whether the list should be narrowed or broadened. The litigation team can then use the information obtained by the IT experts to determine what type of technology a particular custodian uses to communicate and to store their business records. This is routinely characterized as conducting a “data survey” and, under a best-case scenario, will involve your techno-lawyer or outside expert questioning each custodian about their use of technology. Areas to cover with each custodian may include use of: email, voicemail, cell phones, laptops, PDA’s, scanners, hard-copy files (don’t forget about the old-school “stuff”), text messaging, instant messaging and other social media, and thumb drives (the little thingamajigs that you can stick into your computer and use as a portable device for saving data). This is by no means intended to be an exhaustive list, but it does give you an idea of some common devices that you will need to consider in developing your plan. You should also question the custodians on whether anyone (such as an administrative assistant) retains files for them or, conversely, whether the custodian maintains copies of files for someone else in the company.

The next question you face in developing your e-discovery plan is, how you actually identify and access the relevant data. This is the time that your litigation team (now knowledgeable about both your internal technology and the various custodians) needs to approach opposing counsel and attempt to limit both the places that will be searched and the types of ESI that will be collected.

You can begin your negotiation with opposing counsel by identifying areas of ESI storage that you do not intend to search because of the burden caused by either expense or time constraints (or, as is more often the case, a combination of both time and money). Difficult-to-access backup tapes are one area you may be able to cut from the list. Additionally, you may have learned that your IT department has numerous drives that are no longer actively used and that, given the relevant timeframe, are not likely to be a source of relevant information. Hopefully, opposing counsel will agree that searching these databases is not necessary; although she may insist that they be preserved until the litigation is over. However, you might not want to agree to preserve non-relevant data depending on your company’s document-retention policy. For instance, if the data is scheduled to be destroyed pursuant to your company’s regular retention schedule and is not relevant to the current litigation, you probably do not want to unnecessarily retain it for fear that it may represent a mountain of data in a new case that would have been destroyed but for your agreement to hold on to it even though it had nothing to do with the first-filed lawsuit.

Depending on the type of case there may be categories of electronic data that can be eliminated either all together or for a group of the custodians (*e.g.*, to avoid slowing the collection effort down and adding to your reviewing burden you may be able to agree with opposing counsel that .jpeg files (picture-containing files) only have to be collected from the marketing department (who ostensibly routinely use .jpeg files for business purposes) to avoid collecting the family photo album of every custodian on your list).

You might also agree that it is unnecessary to collect system files (these are the files that basically tell the computer what to do and are not likely to have relevant information in most cases). You might also haggle over whether the ESI will be turned over with searchable metadata (this is the stuff that IT forensics geeks can mine for information such as the date the file was created, the author, any person who modified the file, and the date the file was modified).

Your collection and review efforts can also be narrowed and made more manageable by the use of search terms. Like everything else in the e-discovery process, there are a variety of different methods out there and your selection of terms will depend on your particular circumstances. However, as Judge Grimm pointed out, not all searches are created equal and you should expect that the terms and methodology you incorporate into your search will eventually need to be explained. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 257, 262 (D. Md. 2008). Again, the experts will be helpful in crafting search terms that will identify relevant information without leading to an avalanche of ESI—hopefully.

When possible, you should attempt to discuss search terms and methodology with opposing counsel prior to implementation. The courts will be looking for evidence that you have cooperated with opposing counsel, potentially included technical experts in the negotiations, and that you included quality assurance techniques (such as sampling) as necessary in your search protocol. *In re Seroquel Prods. Liab. Litig.*, 244 F.R.D. 650, 662 (M.D. Fl. 2007); *William A. Gross Constr. Assoc., Inc. v. Am. Mfr. Mut. Ins. Co.*, 256 F.R.D. at 136. You should consider not only the obvious keywords, but common misspellings and alternative spellings. Further, for words that will likely lead to frequent hits (both relevant and non-relevant), consider using Boolean searches by placing the word at issue in a proximity string with other words using connectors (“and” “or”) and limiters (“not”) that will weed out the irrelevant hits. Importantly, keywords alone are not going to hack it—I am told by the techno-lawyers with whom I routinely work that some studies show keyword searches used in isolation (with no other controls) are effective in identifying only about twenty percent of relevant documents. Also remember that the keyword searches you use to identify and preserve relevant documents may be very different than the keywords you use to help ferret out privileged ESI.

Be mindful that judges will not appreciate e-discovery plans that are designed “in the dark, by the seat of the pants, without adequate (indeed, here, apparently without any) discussion with [the custodians].” *William A. Gross*, 256 F.R.D. at 135. Further, while using an outside expert is highly important to the task, litigation counsel (both inside and outside) obviously need to stay actively involved and educate themselves on the entire process. As one court noted, “ultimate responsibility for ensuring the preservation, collection, processing, and production of electronically stored information rests with the party and its counsel, not with the nonparty consultant or vendor.” *In re Seroquel Prods. Liab. Litig.*, 244 F.R.D. at 664 n. 14.

Finally, whether you are able to agree with opposing counsel on every part of the discovery plan (yeah, right) or on none of it (more likely), get your plan before a judge

for approval. This will help to eliminate any argument that opposing counsel may have regarding spoliation and it will ensure that, even in the most strict jurisdiction, you are able to “claw-back” any privileged documents that are turned over to opposing counsel. But beware of entering into stipulated orders if your litigation team has not informed itself regarding your company’s ESI, and taken reasonable steps to preserve and collect relevant ESI and to identify and protect privileged information. Consider the recent example of a government lawyer who entered into a stipulated order stating that “the Individual Defendants will specify the search terms to be used.” *In re Fannie Mae Sec. Litig.*, 552 F.3d 814, 817 (D.C. Cir. 2009). In upholding a sanctions award against the government, the court of appeals noted that the order gave the defendants carte blanche to decide what search terms to impose upon the government, and that the government abandoned all protections it might have otherwise had by entering into the stipulated order. *Id.* at 819, 822. The result: despite spending over \$6 million (*nine percent of the agency’s annual budget*) to comply with the defendants’ discovery request, the government was unable to comply with the discovery deadline and was ordered to turn over thousands of privileged documents. *Id.* 818, 824.

IV. Conclusion

The mere thought of e-Discovery is enough to send even the bravest of litigators into uncontrolled spasms of panic; however, once the initial fear wears off the process is manageable (although it will never be cheap). The key is to assemble a knowledgeable team and coordinate with the opposition and the court early in the process. Remember too that the rules only require reasonable measures be taken, which, if you properly document and prove the burdens, can save your client both heartache and money as discovery continues.¹

¹ Special thanks to the E-discovery Practice Group of Seyfarth Shaw; particularly Scott Carlson and Jason Priebe. They guided me through some very difficult collection efforts and, amazingly, have helped a sworn knuckle-dragger (me) become much more comfortable with the world of e-discovery. Any errors made in this paper are solely my own. (Incidentally, both have their own pocket protectors.)

Review Techniques and Technology in E-Discovery

By Richard Munisteri – Vice President and Associate General Counsel, Live Nation

Litigation has always been a place where budgets go to die, and with the advent of electronic discovery, no single event has placed more responsibility and stress on in-house and outside counsel in decades.

Document review is an area of increasing concern because of the disproportionate expense associated with review.¹ The increase in storage capacity combined with the eager adoption of electronic software programs have dramatically increased the amount of electronic data generated and stored by corporations the world over.² Between 2004 and 2007, the average amount of data stored by a Fortune 1000 corporation grew from 190 terabytes (190,000 gigabytes) to 1 petabyte (1 million gigabytes). During that same 3-year period, mid-size companies experienced similar growth, with the amount of corporate data growing from an average of 2 terabytes to 100 terabytes.³

The Traditional Approach vs. Today

In years past, attorneys managed large rooms full of boxes. Today, ten or more times that amount of data can arrive encased in a hard drive. And, once that data has been loaded onto servers and “unpacked,”⁴ the total amount of data can explode to enormous proportions, not to mention the fact that new technologies such as email archival programs have made it difficult to accurately gauge how much potential data is actually in existence. What used to be manageable by a small team of attorneys now may require hundreds of attorneys to sift through and review the material for relevance, responsiveness and privilege.

¹ According to “A Revolution in e-Discovery – The Persuasive Economics of the Document Analytic Approach” by KPMG.

² According to the International Data Corporation’s White Paper, “A Forecast of Worldwide Information Growth Through 2010” by John Gantz, David Reinsel, Christopher Chute, Wolfgang Schlichting, John McArthur, Stephen Minton, Irida Xheneti, Anna Toncheve and Alex Manfrediz, March 2007.

³ Mearian, Lucas. “A zettabyte by 2010: Corporate data grows fiftyfold in three years.” ComputerWorld. March 6, 2007.

www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012364&pageNumber=2.

⁴⁴ “Unpacking” is generally considered to be the practice of expanding compressed files, extracting attachments from email messages and extracting metadata from electronic files.

Live Nation's Experience

In a recent matter, Live Nation experienced this effect first-hand. We believed that our initial collection would contain roughly 100 GB of information. This was based on sound logic. Our custodians were not accustomed to sending and receiving excessive amounts of email nor were they responsible for the regular creation of Word, PowerPoint, Excel spreadsheet or other such user-created documents. Unfortunately for all of us, we were not familiar yet with email archival technology. We had been told by our IT department that, in addition to the unstructured, user-created documents from our target custodians, we had a "database" that would contain relevant information. Without any additional information, we couldn't know what kind of database this was or what it contained. However, we still felt confident in our initial assessment of a relatively manageable collection of data.

The Other Shoe

We engaged an outside vendor to assist us with our collection and processing efforts. They, in turn, began to explore what the parameters of the "database" might be. After discussion with our IT department, it was determined that the "database" was actually an email archival program that had been instituted some 2 ½ years prior to our litigation. It certainly encompassed our time frame, however. And, the system had been programmed to save each incoming and outgoing email for every employee who had worked at Live Nation since the archival program had gone live.

Once we compared our list of target custodians against the data that the email archival program had within its archives, our estimate of 100 GBs was crushed by the reality of 1.85 TBs of data. Needless to say, this equally crushed our cost and time estimates. As has been said many times before, "necessity is the mother of invention," and, in our case, we needed to become very inventive in order to both meet our deadlines and somehow find a cost-effective method for dealing with the drastic increase in the amount of data.

The Review Process in Detail

First Things First: Planning

Planning is and always should be the first thing you do. Creating a solid plan for what you need to accomplish at the end of the process will help determine the path you take and the decisions you make to get there. In other words, understand what the end goals are and then plan backwards. This will help you set realistic timetables for completing your review and to meet any looming deadlines.

Your plan will likely include information regarding your collection effort. Paying attention to collection techniques will help keep your initial collection of data to a reasonable limit and will

help you adhere to and plan for meeting deadlines. This is especially true if you have to collect from multiple sites or from foreign jurisdictions. In our case, we had to collect from 10 different locations in a mere six weeks. This required multiple collection teams and coordinated efforts to ensure that consistent protocols were followed throughout the different sites. Without adequate planning, we would have likely had poor results and multiple collection efforts rather than one well-timed and coordinated project by which we completed the task.

Determine What Kind of Data You Will Have

Next in line will be to determine what kind of data will be encompassed in your collection. The types of data present will, in turn, have an effect on both processing times and review schedules. For example, if your collection includes financial databases, then those will need to be handled differently than will unstructured data such as Word documents.

Also, will there be documents in a foreign language? Will you have highly technical documents or financial documents that may require special skills to adequately review? Will there be sensitive content that will require protection such as HIPPA-protected information or trade secrets?

If any of the above exists, then you will need to plan to segregate the documents into specific queues so that those with the requisite skills can review the documents or to ensure that you secure data that requires protection. The optimum method for segregation is to utilize a software tool to accomplish this with little or no human intervention. Such technology is available from many companies and can occur simultaneously with de-duplication and key word identification efforts. The key to success, however, is having a thorough understanding of what the technology can and cannot accomplish and planning your technology's decision tree with care. Test your efforts before you deploy your chosen technology across the entire collection so that you can easily make adjustments when needed.

Automated De-Duplication and Near Duplication Technology

It is common practice to de-duplicate initial collections. This is accomplished typically by using the document's MD5 HASH value, a unique identifier assigned to each electronic document. Documents bearing identical HASH values will be identified automatically using commonplace technology and will be removed from the initial collection.

In recent years, near duplication technology has emerged that can help identify and group documents with substantially the same information for review to determine if, indeed, these documents are duplicates or if they are unique. While not foolproof, such technology can help to ensure a more consistent review and reduce the amount of time and cost required to complete reviews.

Identification of Relevant and Potentially Privileged Information with Technology

In Live Nation's case, because we had such a large collection of data, there was no other feasible choice but to utilize technology as often as permissible in order to meet our deadlines and to try to curb the mounting costs of review. We were able to reduce the initial collection from 1.85 TB down to 660 GB of relevant data via de-duplication and key word searches for relevancy. Our case was made much more complex because each location at which we collected data had a unique set of search terms, each custodian's data had to maintain its identity as having come from that custodian, and the location where the data had been collected was also required to be identified within the production logic. Keeping all of these competing interests straight was only possible through the use of technology and careful planning.

Key word searches are ubiquitous as a methodology of identifying relevant and potentially privileged information. In *Victor Stanley, Inc. vs. Creative Pipe, Inc.*⁵, Magistrate Judge Paul Grimm found that because of the defendants' lax testing of their key words, they had waived privilege and work-product protections for 165 documents that were produced. In that case, the defendants could not demonstrate adequate due diligence in their document search and review process. Judge Grimm cites that the defendants were "regrettably vague" in their description of how they developed the keyword list, and that supporting affidavits did not demonstrate that the list was developed by individuals who were qualified in search strategy design. In addition, the defendants did not test the key words to determine whether the search results were accurate and, therefore, reliable. Specifically, Judge Grimm said:

"Selection of the appropriate search and information retrieval technique requires careful advance planning by persons qualified to design effective search methodology. The implementation of the methodology selected should be tested for quality assurance; and the party selecting the methodology must be prepared to explain the rationale for the method chosen to the court, demonstrate that it is appropriate for the task, and show that it was properly implemented." *Id.* at *6.

Essentially, key word lists need to be crafted by those who have an intimate understanding of the facts and other key issues of the case, and the words must be tested against a sampling of the collection to ensure that the results returned are accurate and reasonable. Without such testing and comparison, you run the real risk of either missing relevant or privileged documents or failing to identify additional custodians or key terms that are, indeed, important to your production.

⁵ *Victor Stanley, Inc. vs. Creative Pipe, Inc.*, 250 FRD 251 (D. Md. 2008)

Key Word Searching in Live Nation's Matter

As mentioned, we had culled our 1.85 TB of data down to 660 GB of relevant data. Then, it was time to identify the potentially privileged documents. When we completed our term testing and compared our privileged terms against the collection, we identified approximately 300 GB of potentially privileged documents. This was an extremely high number of documents to review. When we calculated the amount of money and time that would be required by such a large document review, it became clear that human review was simply not feasible.

Our discovery vendor suggested that we rely upon the automated review technology alone and forego human review altogether. We decided to see if this approach would work and embarked upon extensive testing of the privilege and relevancy terms along with periodic quality control testing to satisfy ourselves that the technology was reliable. Once we were satisfied with the reliability of the results, we decided to play it safe and approach the court with our methodology.

Opposing counsel resisted our planned approach to the situation, as they apparently hoped to drive us to a quick - and by our estimation, undeserved - settlement as our side faced the prospect of extraordinary cost. However, opposing counsel had very little to offer in the way of explaining why this solution was not prudent. After all, we would be able to produce documents much more quickly than with traditional human review efforts. In fact, the only potential issue that they could muster was to call into question the accuracy of the key word search to identify only privileged documents. However, we were able to demonstrate our testing and quality control procedures as well as the cost savings of this approach.

In the end, our court struck a novel balance. The court allowed the plaintiffs to select a certain number of documents from the privilege log at random. Live Nation would then conduct a human review of those documents. If the "failure rate" (i.e. rate of non-privileged documents found within the privileged collection) approached a pre-determined percentage, then Live Nation would review all of the documents on the privilege log. However, if the "failure rate" remained below the negotiated percentage, then all documents listed on the privilege log would be deemed to be privileged.

This solution worked very well in our situation. It saved our company an enormous amount of money and allowed us to meet our production deadline. However, each matter has its unique needs and risks, and you should evaluate carefully whether a solution of this type is right for your matter. In addition, the use of a strong claw-back agreement in such a situation is wise. Investigate your jurisdiction for privilege waiver case law specific to your court.

Effective Human Review Techniques

Most litigation matters will entail some level of human review. The keys to effective and efficient human review are planning, effective management and flexibility.

1. Standardize Your Review Criteria: Make sure that every reviewer is operating off the same game plan. This will ensure consistency and accuracy.
2. Appoint a Seasoned Review Manager: Your point person needs to have been through a few review projects in the past in order to effectively manage a team of reviewers. Using inexperienced attorneys or paralegals invites second-guessing, re-work and disaster.
3. Establish Problem Resolution Protocols: Create a problem resolution matrix for the escalation of issues to an appropriate person within the team who can make final decisions regarding review issues.
4. Create Custom Review Teams when Necessary: If your collection contains foreign languages, financial information or technical documents, then consider creating specialized review teams with those special skills in order to review the documents. You can use technology to drive the documents into these specialized queues for review.
5. Be Flexible: It is commonplace for new terms to be added or current terms to be altered during the life of a case. It is not uncommon for this to take place after review has begun. Therefore, build extra time into your timetable to accommodate such changes and plan for what you will need to do re-review or to double-check documents whose review is complete.

Conclusion

Knowledge and planning are the keys to a successful e-discovery review project. You have no choice but to take a hands-on approach. The consequences for mistake or lax attitude can be expensive in all sorts of ways. Ensure that you trust and regularly communicate throughout the process with both your outside counsel and involved vendors. Set appropriate expectations with your internal clients - law department management, finance, IT and the relevant operations personnel – to avoid surprises down the line with the cost, components and logistical demands required. By following steps like the ones outlined in this article, you can put yourself on the path to feeling confident that you have done the job expected of you for the company in competently managing this process.

ACC Extras

Supplemental resources available on www.acc.com

Outsourcing/Offshoring First Level Document Review in an Era of eDiscovery.

Program Material. December 2007

<http://www.acc.com/legalresources/resource.cfm?show=19871>

Hot Topics in Ediscovery: Are There Any Other Kinds?

Program Material. October 2008

<http://www.acc.com/legalresources/resource.cfm?show=162096>

Taking Control of eDiscovery: Strategic Considerations.

Webcast Transcript. December 2008

<http://www.acc.com/legalresources/resource.cfm?show=130761>

Please note, these additional resources are provided by the Association of Corporate Counsel and not by the faculty of this session.