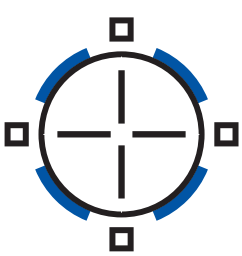
SUMMER 2007

EDRM

Electronic Discovery & Records Management Quarterly

- An Interview with Patrick Oot
  Verizon's Director of Electronic Discovery
  By George Socha
- On the Digital Paper Trail:
  E-mail Analysis & Internal Investigations
  By Amanda J.G. Karls, Esq.
- How to Deal with the Amended
  Federal Rules of Civil Procedure
  By Craig Carpenter

speak softly and carry a big Linux cluster

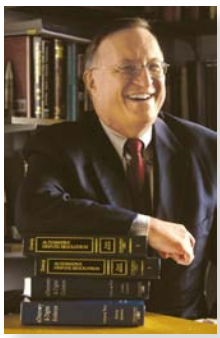


DiscoveryMining

Articles

WEST LEGALworks™

From the Editor



Perils And Benefits Of Electronically Stored Information

Electronically stored information differs from traditionally stored paper information in a number of important ways. There is much more electronically stored information and it is being created at greater rates than paper documents. Electronically stored information is harder to dispose of than paper information. Electronically stored information contains information about the document that is recorded by the computer that may reflect the generation, handling, transfer, and storage of the information. Electronically stored information is more easily dispersed and disseminated than paper documents.

Recent news stories illustrate the impact of electronically stored information on business (and political) organizations. According to one story, a 22-year old HMO employee sent an email throughout the HMO on a Friday claiming that the HMO's $4 billion plan to convert paper files into electronic medical records was a mess. The youthful employee charged that the HMO was wasting $1.5 billion every year on inefficient and ineffective information projects. He also complained of the "misleadership" of the HMO's management. By the following Monday, the email had reached an estimated 120,000 computers at the HMO and had been leaked to the public. Since the email was sent, the story has become front page news in newspapers around the country. The HMO has spent substantial time trying to undo the harmful effects of the email.

In another case, a company has taken steps to recover from mistakes it made in preserving emails in an antitrust case. Apparently, the company's email system automatically deleted emails after 35 to 45 days, if employees did not take action to save them. Despite a duty to preserve, some emails were not saved because employees misunderstood their obligations to do so. According to the *Wall Street Journal*, it is estimated that the cost of recovering the emails will be in the millions of dollars.

These are just two examples of the power of email, and the costs, and burdens of discovery or disclosure of electronically stored information. While they may, or may not be typical, they illustrate the burden and expense of complying with (or failing to comply with) requests for electronically stored information.

In this, the first issue of ELECTRONIC DISCOVERY AND RECORDS MANAGEMENT, contributors provide advice and suggestions on how to minimize costs and burdens, and how to effectively and efficiently handle discovery and disclosure, of electronically stored information.

Readers who have suggestions or comments are encouraged to contact the editor at jgrenig@earthlink.net or at Marquette University Law School, P.O. Box 1881, Milwaukee, WI 53201-1881.

June 2007

Jay E. Grenig, Managing Editor
Professor of Law
Marquette University

ONE YEAR SUBSCRIPTION • 4 ISSUES • $95.00 • (ISSN: 1938-4947; CODE: 40642683)

Please address all editorial, subscription, and other correspondence to the publishers at west.legalworksregistration@thomson.com

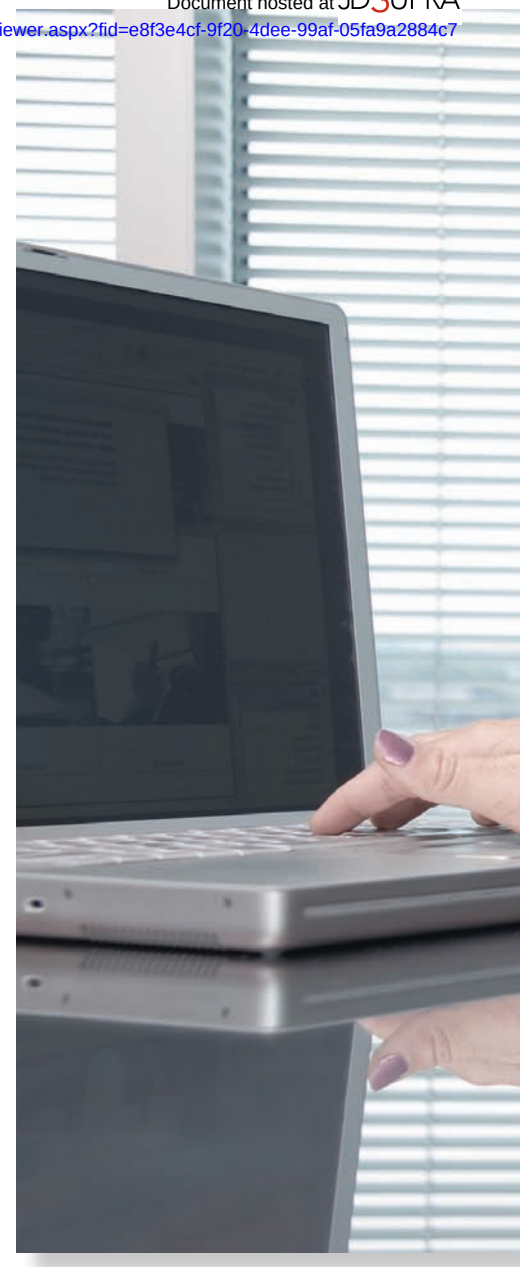
Electronic Discovery & Records Management Quarterly

West Legalworks
395 Hudson Street, 4th Floor
New York, NY 10014

THOMSON WEST

On the Digital Paper Trail:

Using E-mail Analysis & Other Best Practices for Preliminary Internal Investigations



By Amanda J.G. Karls, Esq.*

Corporate misconduct can compromise the financial well-being and reputation of any business. Fortunately, businesses that are prepared to promptly respond to and address suspected incidents of internal wrongdoing can dramatically curb their investigation costs, legal liabilities and business risks down the road. Savvy attorneys understand that corporate e-mail accounts can serve as a prime source for initial investigation and analysis. Just as the computer is becoming a mainstay in today's electronic workplace, e-mail evidence is becoming a vital part in many investigations and legal matters. This article will explore best practices for conducting the first stages of an internal investigation and how e-mail analysis can be critical to that end.

When faced with a suspected incident of internal misconduct, organizations are well served to begin by identifying

a responsible party who can assess the extent to which an internal investigation may be warranted, if it all. Because internal investigations usually involve complex legal issues, attorneys are ordinarily best-suited for this role. Moreover, if the assessment is not carried out by an attorney, the organization risks waiving any attorney-client and work product privileges that may have otherwise applied.

As between in-house and outside counsel, especially at the outset of an inquiry, corporate counsel may be the most logical assessors. Once involved, counsel's primary objective will ordinarily be to evaluate the scope of the suspected wrongdoing.

The scoping assessment serves as the most critical focus of the entire investigation. For example, an investigation that targets only one small group of employees could miss widespread malfeasance among other individuals. Similarly, an investigation that focuses on an overly narrow time period could overlook very important details. Conversely where too much information is considered, analysis can become impractical and further investigation will likely be ineffective, costly and time consuming.

In an age where electronic communication has replaced traditional hard copy documents as the primary medium of correspondence, e-mail provides counsel with a logical starting point for this preliminary scoping.

In an age where electronic communication has replaced traditional hard copy documents as the primary medium of correspondence, e-mail provides counsel with a logical starting point for this preliminary scoping. E-mail can be especially useful in light of the rich trove of information it can provide. In comparison to traditional ink-and-paper communications, many computer users adopt a vastly different level of formality and tone when drafting e-mail communications. With a few casual keyboard strokes, an individual's candid thoughts or intentions are transmitted, copied and recorded. Moreover, e-mail creates its own virtual paper-trail. This affords counsel the opportunity to ascertain who may have been involved in a suspected incident of misconduct, what they said, when they said it and who else they told. While e-mail can serve both as a vehicle for wrongdoing and a record of it, without the proper tools to analyze it, the efforts expended to make sense of it can be overwhelming. In fact, a recent survey estimates the average corporate e-mail user sends and receives approximately 133 messages daily.[1]

The use of e-mail analysis software can significantly aid in determining scope by putting the power to reveal themes, key players and timelines in the hands of an organization's in-house legal team. E-mail analysis software can quickly pinpoint and retrieve employee mailboxes selected by the legal department for further scrutiny. Once retrieved, counsel can use these tools to perform searches, create workspaces for individual cases and investigations, view communication clusters and generate graphs, timelines and other analytics. Honing in on the details, counsel can identify communication patterns that might have never been uncovered using traditional review methods. Armed with this knowledge, counsel is also better equipped assess if and how to best proceed with any further investigation. E-mail analysis may also be useful in evaluating whether a situation necessitates notification of regulatory or law enforcement officials.

After conducting an initial e-mail analysis, corporate counsel may decide to delegate some or all of the subsequent investigatory responsibilities to outside counsel. In making that decision the organization should consider the scope of the investigation and its potential legal implications. For example, especially in the context of investigations that may reveal information pertinent to a regulatory or criminal inquiry, engagement of specially appointed independent counsel may be prudent, if not legally necessary.

The results of the e-mail analysis may also warrant a computer forensic investigation of key individuals' computers. The use of forensically sound processes and procedures will ensure that computer data is treated as evidence at the earliest possible date, thereby increasing the likelihood that can be admitted as such in a court of law. While counsel should ordinarily oversee this process, the actual forensic investigation should be carried out by an individual with experience creating mirror images and maintaining media integrity.

If a computer forensic investigation is warranted, counsel and other corporate officials must determine whether the work should be performed by an in-house IT staff member or outsourced to a computer forensic expert. When making this crucial decision, corporations should carefully consider the training, technology resources and bandwidth of their IT staff. Asking someone with little or no computer forensic investigation experience to conduct the inquiry can be an enormous liability. Failure to adhere to strict industry standards regarding data preservation and collection can compromise the investigation and evidentiary value of any information that is obtained. Experience aside, the corporate IT department may not have the human resources to meet the logistical demands of conducting the investigation or the proper tools to carry it out. Asking IT employees to infiltrate their co-workers' or supervisors' electronic-based communications also opens up a variety of privacy and bias concerns. To the extent the investigation may reveal information pertinent to an ongoing or potential legal matter, the organization should also consider whether expert reporting or testimony may be needed, and if so, whether internal IT staff are suited for this responsibility.

In instances where outside counsel and expert computer forensic investigators are called in, a properly conducted preliminary e-mail analysis will serve as an excellent starting point for their continued efforts.

E-mail analysis software:

Arming corporate counsel with invaluable information

E-mail can be critical to the investigation and litigation of any number of potential incidents of corporate misconduct ranging from harassment to insider trading, misappropriation of client assets, data theft, fraud, antitrust violations and corporate cover-ups.

For example, in Linnen v. A.H. Robins Co., e-mail evidence revealed a damaging communication exchange among employees of A.H. Robins about the negative side effects of the recalled Fen-Phen diet drug. The "smoking gun" e-mail, which led to the pharmaceutical company paying out one of the largest legal settlements in history, read, "Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?"

Similarly, investigations into Enron's accounting irregularities exposed a damaging e-mail. Weeks before Enron filed for bankruptcy, it became apparent that several major financial institutions had helped Enron manipulate its numbers and mislead investors with secret loans. During the subsequent investigations, one piece of evidence that received broad attention was an internal e-mail at JP Morgan Chase that described one of these secret loans called a "prepay." The e-mail chain began, "Enron loves these deals as they are able to hide funded debt from their equity analysts because they (at the very least) book it as deferred [revenue] or (better yet) bury it in their trading liabilities." Another internal e-mail expressed concern: "Five [billion] in prepays!!!!!!!!!!!!!!!" The reply to that email proved even more damaging – "Shut up and delete this email."

Through innovative e-mail analysis tools corporate counsel can reveal key players and themes and promptly assess suspected incidents of inappropriate employee communications or computer misuse. E-mail analysis software can also be used as an early case assessment tool for litigation. Using the software to see e-mail communication relating to the issues in the suit, counsel can form legal strategies and determine whether to settle the case or hire outside counsel to contest the claims.

However, while e-mail analysis software can be an especially powerful preliminary investigation tool, counsel should take care to ensure that that any preliminary analysis they undertake does not compromise the rest of the investigation. E-mail, like other electronically stored information, is easily manipulated and can be altered irrevocably if it is handled incorrectly. Even the simple action of opening an e-mail can alter the metadata properties of the document. For these reasons, e-mail analysis should not be conducted without the use of reliable software designed specifically for early case and investigatory analysis. In particular counsel should be sure that any software they select will not forensically impact the files they are reviewing. Fortunately, with the proper tools and precautions e-mail analysis can ordinarily be conducted by corporate lawyers at the click of a mouse.

*Amanda J.G. Karls is a staff attorney at Kroll Ontrack, a computer forensics and electronic discovery company in Eden Prairie. Amanda has written extensively on issues relating to electronic evidence for national and international legal publications. She holds a Bachelor of Arts in International Business from the University of Saint Thomas, and a Juris Doctor from William Mitchell College of Law.

1. "Taming the Growth of E-mail: An ROI Report by The Radicati Group, Inc." (July 2005). Available at: www.radicati.com.

From concert promoter to Director of Electronic

Patrick Oot is the Director of Electronic Discovery and Senior Litigation Counsel for Verizon Communications, Inc. *Inside Counsel* magazine named Verizon's ediscovery team as one of the ten most innovative legal groups of 2006. Mr. Oot received both his B.A. and J.D. from Syracuse University and his LL.M. from Georgetown University Law Center.

GS: Patrick, thank you for taking the time to talk with us. Could you start by telling us about your background?

PO: I was a computer junkie with no formal technology training. My interest in technology started in the early 1990s before going to law school. At that time, I was a concert and nightclub promoter in the Northeast. I produced shows with artists like Moby, De la Soul, Bad Boy Bill, and Run DMC.

I discovered many people who attended my events were students in the New York area. These students were early adopters of electronic communication (remember PINE and telnet chat?). I found that marketing electronically was much more effective than print advertising. I wanted to learn about technology. It was exciting. I later went to law school, first at Syracuse University, and later obtained an LL.M. from Georgetown University Law Center.

GS: How did you get your position? It sounds like quite a jump from concert and nightclub promoter to electronic discovery director at a major corporation.

PO: John Frantz, who is Vice President and Chief Litigation Officer at Verizon, was managing a multimillion-dollar collections case for the company. I started working on the case as a contractor while I was still studying at Georgetown. The case was Verizon's first big case that involved electronic discovery issues. I helped work out a few vendor issues and later managed the document review. He offered me an entry level position after the case was over. I was promoted to Director when John formed the EDT (Electronic Discovery Team) in 2005.

GS: As the Director of Electronic Discovery and a senior litigation counsel for Verizon, you must have more than a few responsibilities. What are they?

PO: I advise the Verizon business units and their attorneys on various electronic discovery issues. Currently, our team is working on about 29 cases. In addition, I maintain an external-facing role. I am responsible for Verizon's relationships with vendors, firms, and outside groups. When not working on cases, I devote considerable time to external groups, policy development, and attorney education. I speak at conferences two to three times a month.

GS: It sounds like you are keeping busy. To whom do you report?

PO: I report to John Frantz, the Chief Litigation Officer.

GS: Do you have a staff?

PO: We have a team, the Electronic Discovery Team, but I don't consider the EDT "my" staff. The EDT consists of John

Discovery:

An interview with **Patrick Oot**

By George Socha*

Frantz, me, the Director of Legal Technology Strategy and Planning, a litigation counsel, and a litigation and electronic discovery specialist. Three of us are 100% devoted to electronic discovery issues. The other two – John and the litigation counsel, devote a part of their time to electronic discovery issues.

The Director of Legal Technology Strategy and Planning comes from Verizon Corporate IT and brings with him tremendous IT knowledge. The rest of us are attorneys.

GS: What do you find to be the greatest challenges in your position?

PO: Uncertainty in developing law is a challenge. ED practitioners are at the helm of a very large ship heading in an uncertain direction while the cartographers are still tinkering with the maps. Our challenge is to ensure that emerging law doesn't adversely or unjustly affect our clients. Standards of "reasonableness" and "good faith" can easily vary from district to district while no one is lobbying for uniformity.

GS: What best prepared you for the electronic discovery challenges you face?

PO: We sought advice from some of the leading practitioners in this field. We then developed our own privileged advisory for our attorneys that clearly defines roles of the EDT, the inside attorney, and outside counsel and advises the attorney why a specific strategy was taken in developing Verizon's practices.

GS: Where do you turn for help when you need assistance in addressing electronic discovery challenges?

PO: I first turn to our team. For example, John always has an open door. He has been my mentor since the beginning of my career. John is extremely focused and has a unique ability to help keep my ambition and innovation on track.

Also, I feel we have a great ED community. I am fortunate enough to call many of my colleagues (and some times opponents) friends. Funny enough, two ED consultants live just two blocks down the street from my home. Challenges aren't really that difficult when you have so many resources.

GS: Are there any particular electronic discovery providers you prefer?

PO: We have several long-standing relationships with service providers (staffing, ED services, scanning, etc.). Most of these relationships started at Verizon at the same time I did. However, the vendor marketplace is evolving with emerging technology. I am always seeking new and innovative strategies to tackle a problem. We limited the number of providers in order to streamline Verizon's EDRM [electronic documents and records management] process.

GS: What are your main electronic discovery goals for the coming year?

PO: The EDT's top three goals for 2007 are:

1. Delivering service to our clients;
2. Educating clients about our group, what we do, and what they must do in working with us; and
3. Increasing efficiency and innovating to reduce costs.

GS: What advice would you offer to someone interested in learning more about ED?

PO: Get involved. Many organizations (Sedona [Conference], EDRM [Electronic Discovery Reference Model Project], GULC [Georgetown University Law Center] CLE Program, etc.) have great programs that welcome and need fresh input. ED is a fledgling new genre of law that is undeveloped and will evolve quickly in the years to come. I can't imagine another forum where one can interact with such high level thought leaders on a consistent basis.

GS: Patrick, thank you again for taking the time to talk with us.

*Founder of Socha Consulting LLC. Socha Consulting assists in crafting and implementing effective electronic discovery strategies, identifying and selecting appropriate electronic discovery services, and managing the electronic discovery process. B.A. University of Wisconsin, J.D. Cornell Law School

recommind™

Sophisticated Search and Categorization Made Simple

MindServer™ Legal

Enterprise Search
Matters & Expertise
Litigation Readiness
Knowledge Management

For more information:
Recommind Inc.
Tel: (415) 394 7899
email: sales@recommind.com
www.recommind.com

Making the Amended Federal Rules of Civil Procedure Your Best Friend

By Craig Carpenter*

Introduction

Even after more than six months of extensive coverage given the amended Federal Rules of Civil Procedure (FRCP) effective December 1, 2006, many organizations still have not implemented a strategic plan to address the impact of this significant event. While the amended rules certainly made several tactical changes with respect to how the discovery process—or "eDiscovery" process—should be conducted and how digital information (now known as electronically stored information or ESI) should be handled, the gist of the changes can be summed up as ignorance of one's ESI is no longer an excuse. The amended rules will reward those who are prepared for litigation in this new era, and punish those who are not.

The Knee-jerk Reaction to the Amended Rules

The response from most organizations has been predictable: fear.

- Fear of enormous litigation costs
- Fear of greatly increased complexity
- Fear of not finding the proverbial smoking gun before the other side does
- Fear of spoliation sanctions and adverse inference jury instructions
- Fear of increased litigation exposure

The common feeling seems to be that no one wants to be "the next Morgan Stanley," a none-too-subtle reference to the seminal 2005 case (*Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc.*, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005) in which Morgan Stanley was unable to produce certain email in response to Coleman's discovery requests and the court's discovery orders. Morgan Stanley suffering the astounding trio of a $15 million spoliation sanction *and* a highly damaging adverse inference instruction *and* a $1.5 billion verdict for the plaintiff. (That the case has since been reversed on appeal does not seem to have diminished its impact. See *Morgan Stanley & Co. v. Coleman (Parent) Holdings, Inc.*, 2007 WL 837221 (Fla.App. 4th Dist. March 21, 2007)).

Not surprisingly, an expected byproduct of the amended rules and the fear they have engendered is rapid growth amongst vendors who supply the technology that will be used to deal with twenty-first century litigation—the so-called "eDiscovery technology" market.

Not surprisingly, an expected byproduct of the amended rules and the fear they have engendered is rapid growth amongst vendors who supply the technology that will be used to deal with twenty-first century litigation—the so-called "eDiscovery technology" market. According to Forrester Research, this market is expected to grow from a mere $1.4 billion in 2006 to almost $5 billion by 2011, which translates into an average annual growth rate of roughly 30%.

What is the reason for this torrid growth? Most organizations, and especially the largest enterprises who also happen to have the largest information technology and litigation support budgets, believe that incorporating and automating with technology is the easiest, most cost-effective—and possibly only—way to organize, categorize, search, review and produce the vast amounts of data contained within their networks (which, by the way, continue to grow larger every day). Thus, it would seem that the amended rules may be painful and costly for many organizations.

While most people seem to focus on the negative fallout from the amended rules, whether real or perceived, an often unasked question lurks beneath the surface—one that may hold out hope for those organizations that actually do take the time to bring their ESI houses in order. If *not* being prepared to deal with litigation under the amended rules will be punished, shouldn't *being* prepared bring reward through some sort of competitive edge? Put another way; is it possible to use the amended rules to one's advantage? The answer is yes – and the sooner organizations realize they can turn an otherwise daunting task into an offensive weapon the more likely they are to benefit from their hard work.

Benefits of Addressing the Amended Rules

As most organizations realize that the amended rules are here to stay, they are beginning the arduous process of getting their ESI houses in order. This typically involves several steps, including

- Taking inventory of exactly what ESI they have—how much, in what format, and where
- Who is able to access this information and what they are able to do with it
- How and when information is created, saved, backed up and destroyed
- How information is currently being "locked down" pursuant to a legal hold
- How information is being collected in the early stages of the discovery process
- Any early case assessment mechanisms the organization might have in place

This current system (assuming one exists) can then be benchmarked against what would be considered an acceptable system under the amended rules, either by the organization's own legal department, outside counsel, an external consultant or all of the above. Once the organization has established exactly what needs to be done to become prepared to deal with the amended rules, it can decide the steps that must be taken—including the addition of technology where appropriate—in order to achieve an eDiscovery response system that is acceptable to that organization.

Several of the benefits to be enjoyed by such an undertaking are obvious. For starters, the more prepared an organization is to respond accurately and quickly to a lawsuit or subpoena, the more likely that organization will be able to keep legal bills down. The organization should also be able to more effectively minimize risk in litigation as the odds of suffering potentially devastating discovery sanctions or jury instructions should be greatly mitigated.

There are other, less obvious benefits to be enjoyed from these efforts, including the ability of the legal department to conduct internal investigations quickly and inexpensively (for example, if an employee is suspected of stealing intellectual property) and simply having a far more organized information management system. This last byproduct of getting one's ESI house in order can have huge benefits in the areas of compliance, risk management and information lifecycle management (or ILM). After all, once an organization knows what information must be kept for legal purposes, it can destroy as much of the remaining information as it wants, thereby freeing up expensive network bandwidth and storage space.

But for those organizations that are always opportunistically looking for a competitive edge over their rivals, becoming prepared to deal with the amended rules has another important benefit: it allows them to pursue aggressive litigation tactics. Much like a football team with a strong defense is able to become far more aggressive on offense—confident in the knowledge that their defense can "hold the line"—opportunistic organizations can turn the amended rules into an offensive weapon with which to pressure their opponents.

The Best Defense Is a Good Offense

Once an organization knows its ESI is organized and is prepared to deal with litigation, the organization can become the aggressor. To begin with, if an organization has a better handle on its information than its opponent, that organization is far more likely to have a clear understanding of its own case earlier in the process than the opponent—allowing the organization to become much more aggressive in any settlement negotiations that might take place, not to mention the inevitable discovery wrangling that accompanies many suits. If an organization already knows it is comfortable producing all documents in their native format, the organization can insist on native format production from the very outset of the case, a tactic that can place considerable pressure on the opponent to respond similarly or face the wrath of the court in explaining why it won't (or, more likely, can't).

Discovery timelines can be extremely demanding, so the more prepared one side is to meet tight deadlines the more likely that side is to earn the trust and support of the judge in the case. Having a good handle on the strengths and weaknesses of the information that will be turned over to the other side also allows one to build a stronger case earlier on in the litigation, which often has a cumulatively positive effect on that side's chances of victory as litigation progresses.

An organization with it's ESI house in order can also choose to launch more lawsuits than it might otherwise have contemplated, especially where the potential opponent might not have its own ESI house in order. In the past, the time it would take to conduct an investigation, gather potential evidence, and decide that wrongdoing might have taken place was typically measured in weeks or months. By the time an organization figured things out, the window of opportunity—and perhaps even a statute of limitations—may have passed. Now, with a well-organized information system and some sophisticated search technology, it might take an organization a matter of hours or days to compile sufficient evidence on which a complaint could be filed. Thus, having one's ESI house in order is not only a huge benefit when defending a suit, but it gives organizations far more options when contemplating their proactive litigation strategy.

Technology as an Offensive Weapon

eDiscovery technology comes in all shapes, sizes and prices; some of which may typically be utilized only by outside counsel in defending or prosecuting a case on behalf of an organization. There are, however, several key technologies that can be tremendously helpful in allowing an organization to not only organize and manage its own information, but quickly to gain critical insight into what may be lurking within the organization's email servers, databases, applications and other repositories of information. Arguably the three most important areas to be addressed are effective records management—especially for those employees most at risk (e.g. human resources, the legal department, the executive staff and the financial department), accurate legal hold func-

An organization with it's ESI house in order can also choose to launch more lawsuits than it might otherwise have contemplated, especially where the potential opponent might not have its own ESI house in order.

tionality, and sophisticated search and analysis technology.

The concept of records management may elicit images of old, stodgy librarians with intimate knowledge of the Dewey Decimal System. However, today's cutting edge records management technology is anything but old and stodgy, and is increasingly automated as opposed to manual. Automation is an extremely important factor, as most employees will not use or even accept tools that disrupt their day-to-day activities in any way. By using sophisticated categorization technology that is able to automatically identify the meaning of documents and email messages and their value to the organization and integrating such technology with an organization's key applications and databases (customer relation management systems, document management systems, exchange servers, etc.), organizations are able to accurately and automatically categorize and tag information as it is created by users. This makes such information infinitely more organized and quickly retrievable thereafter, supporting the organization's compliance, investigatory and eDiscovery needs.

Once an organization can reasonably anticipate being sued or suing another, it has an obligation to preserve potentially discoverable information within its control. Known as a legal hold or litigation hold, for organizations that do not have a good handle on their ESI the implementation of a legal hold can be an extremely painful and arduous process—and one fraught with significant risk. For those with effective legal hold technology integrated into their information system, legal holds should be a relatively simple and highly accurate process.

The keys to effective legal hold technology are threefold. First, the system must not interfere with how users go about their daily lives. This is especially true with large enterprises that may have multiple legal holds in place at any given time. Second, the system must be able to tap into all repositories of information, including applications, databases, servers and even desktops and laptops where necessary. Third, the system must be able to find all potentially relevant documents, whether or not they were sent by or to a particular person and/or contain a particular set of key words. This last requirement typically requires sophisticated, concept-based search technology that can discern that certain concepts are related (e.g., backdating to timing of options grants) regardless of the words used to describe them.

Last but not least, once all potentially relevant and discoverable information has been located and preserved, the organization's legal department (or outside counsel as the case may be) will need an effective way of sorting through this massive amount of information and quickly honing in on a few key pieces of data—the proverbial smoking guns—which will go a long way towards determining the outcome of the lawsuit or investigation.

Utilizing tools similar to those employed in the legal hold phase, organizations will want to have the information placed into certain "buckets" depending on any number of factors, including more pedestrian classifications like custodian, date range or format, as well as far more sophisticated factors like whether or not a document contains a particular concept (irrespective of the exact wording used in it), deals with a certain matter or is related to a certain string of correspondence. The more intelligent this technology is, the more it can group information automatically, which will save the legal department a tremendous amount of time as the department conducts its investigation or review.

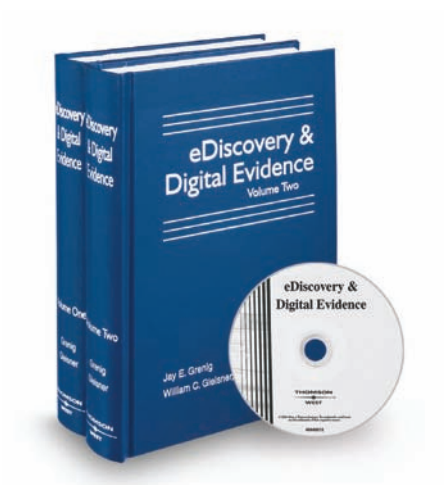
Conclusion

The amended FRCP have caused a great deal of fear among most organizations and with good reason, as the downside of greatly increased litigation cost and potential spoliation sanctions, to name only a few items of concern, are significant. But for those organizations that take these concerns seriously enough to address them proactively with the right technology, the amended FRCP offer a surprising silver lining: the ability to gain a competitive advantage over their less-prepared rivals. As a result, "getting one's ESI house in order" not only makes good business sense but can even give an organization another area in which it can beat its competitors.

Craig Carpenter is Vice President of Marketing at Recommind, a leading enterprise search company named to a list of "100 Companies That Matter in Knowledge Management." He has extensive experience in enterprise software, information security, and eDiscovery industries. Mr. Carpenter is an adjunct faculty member at the University of San Francisco where he teaches graduate classes on high tech marketing, content management, and digital rights management. Mr. Carpenter received his JD and MBA from Santa Clara University and his BA from UCLA.

eDiscovery & Digital Evidence

by Jay E. Grenig and William C. Gleisner III
with General Consultants Troy Larson
and Dean John L. Carroll



Electronic evidence becomes more essential every year, and practitioners need up-to-date guidance and practical tips to navigate this rapidly-changing world.

eDiscovery & Digital Evidence provides guidance in determining when forensic or similar specialized technical help is necessary. It covers preservation and retention policies, discovery, disclosure, cost sharing, spoliation, and the admissibility of digital evidence, including computerized business records and computer-generated evidence. Its appendices include a detailed glossary, practical forms in print and on CD-ROM, pertinent Federal Rules of Civil Procedure, proposed changes to the Civil Procedure Rules, and Federal Rules of Evidence, comprehensive manuals concerning searching for digital information, and the effective use of technology in the courtroom.

eDiscovery & Digital Evidence helps lawyers and judges skillfully handle digital information and become more intelligent consumers of technical services.

To Order, call West at
1-800-328-9352 EXT 7-1183

THOMSON
WEST

Prepare Yourself to Confer Before Conferring

UNDER THE AMENDED FEDERAL RULES OF CIVIL PROCEDURE

By Albert J. Kassis*

Introduction Everyone has heard of the saying, "Don't put the cart before the horse." The "cart" in this scenario is the Rule 26(f) confer requirement. And the "horse" is all the electronically stored information likely to be the subject of the meeting. For the sake of chronology, we will discuss the "cart" first and then the "horse." In the end you will see that developing a good working relationship with your client and becoming familiar with your client's electronically stored information and infrastructure will make conferring easier.

The Cart

The first 99 days of federal litigation are now even more important than ever before. Parties must confer and develop a discovery plan at least 21 days before the Rule 16(b) scheduling conference. Under Rule 26(f) of the amended Rules of Civil Procedure that went into effect December 1, 2006, the parties must confer before the Rule 16(b) conference regarding the following:

- A plan for discovery
- Disclosure of electronically stored information and preservation of that information.
- Sources of electronically stored information from which the clients are and are not producing information.
- What electronically stored information will be included in the search for relevant documents.
- What electronically stored information the clients have that will not be searched.
- The form of production to opposing counsel (e.g., native file vs. another format and the load file specifications for eventual use).
- Issues dealing with privilege, such as the prospect of including a clawback agreement in a court order.
- The type of case and the amount at risk.

This duty to confer is mandatory and the substantive communications between counsel may later be considered by a court in deciding issues regarding a particular side's good faith. Sending a brief email to the opposing side demanding electronically stored information does constitute conferring. The conferring is likely to take place over a period of time where both sides confer back and forth on several occasions attempting to hammer out issues.

The foundation for a successful Rule 26(f) conference is one of cooperation and communication. The substance of this communication under the amended Federal Rules will likely entail electronically stored information—commonly be known as "ESI." If your previous discovery endeavors involved only paper, this will no longer be the case. ESI will be an important part of discovery and the discovery conference.

The Horse

Proactive measures with your client may now be necessary. This is particularly so if the client is litigious with matters historically involving ESI. Counsel should consider meeting with the client and those responsible for the client's ESI to ascertain the client's electronically stored information layout.

Many attorneys can utilize Microsoft's submission (www.uscourts.gov and search for "04 CV 001") to the Federal Rules Committee showing the typical data architecture of a company. This chart may assist attorneys in understanding the client's electronically stored information when meeting with the client's information technology staff. Microsoft's submission may also help facilitate discussions between the parties if they are less than forthcoming with the information. Time frames and deadlines will be more realistic when all the necessary information is considered.

If your client has legacy databases that prove difficult from which to mine electronically stored information, this will delay matters. If one side demands relevant information from a database, counsel should consider working with opposing counsel to determine what is needed. Is it the electronically stored information? A report? Other artifacts from that database that would be useful? The raw data? Some databases will not produce any relevant information unless the requesting party also has a similar database.

Since organizations must quickly identify what sources of ESI exist, now is an excellent opportunity for a determination to be made as to what ESI is regularly being deleted, what data systems are no longer being used, and what ESI is in a remote or third party location. Additionally, the parties in the meet and confer should do the following:

- Determine what ESI is active and what ESI is inactive.
- Formulate a map and inventory of the ESI.
- Ascertain which ESI the client deems accessible and the reasons why a client deems certain ESI not reasonably inaccessible.
- Identify the personnel in the information technology department; specifically, what personnel control which ESI—including the records management component.

"If your client has legacy databases that prove difficult from which to mine electronically stored information, this will delay matters."

- Come to an agreement that will be incorporated into an updated discovery plan requiring a description of the process of production for ESI.

Some personnel may only control limited ESI, thus hampering a necessary preservation of ESI. In regard to preservation, ESI relevant to a federal case must be preserved for the life of the case for production to the other side. In large organizations, different individuals may own ESI at different levels. It will be difficult for counsel to protect the client from a spoliation claim if counsel does not know where the ESI is.

This work may also allow for both the client and counsel to determine if the current ESI environment is one susceptible to a cost efficient harvesting of information. This efficiency, particularly of ESI that is more likely to be in "play" in a lawsuit, will result in lower costs in retrieval and the potential for lower legal costs otherwise (i.e. reductions of related court actions, including but not limited to motions for protective order and the defense of motions to compel).

As counsel speaks to the client, counsel can guide the client to help to avoid a costly scenario of casting a "big net" in a preservation hold. If organizations are not certain exactly where ESI resides, these "nets" may become large and hamper other natural courses that ESI goes through as part of the document destruction or retention policy. There must be an analysis of where the content resides and their inclusion of responsive ESI. In addition to that, counsel should determine whether the client has systems in place to identify ESI that is potentially relevant.

For corporate counsel, the mandate is clear. While the rules affect cases in a practical manner, they also affect companies that find themselves in court on a regular basis. When your clients put some work into the front end, counsel's efforts in a meet and confer will be easier. If all the components of a client's information technology infrastructure are known, in a preservation scenario, those systems whose ESI is not relevant to a proceeding will not be implicated in a preservation mandate. Routine business processes including archiving, and destruction will not be hampered and the day-to-day processes and procedures will remain. With day-to-day processes intact, costs will be reduced. Otherwise, preservation holds could be wide-reaching. The juxtaposition to all of this is that the ESI net that is cast is smaller, and it carries the risk that ESI outside this net may be relevant but destroyed. Of course, preservation of ESI also involves preserving ESI of former employees. A corporate roadmap of the ESI, updated as the system changes, will give counsel more time to strategize on issues as it relates to the ESI with less time devoted to the precursor of where and what the ESI contains.

Perhaps you have heard the phrase "first seek to understand to be understood." The relevance of that phrase to ESI is particularly appropriate. You will have difficulty in describing to the other side within a reasonable time what ESI your client has, if your client does not understand its own ESI. There will be occasions when client systems are so complicated that it may be necessary to consult with a systems person from the company. That systems person can speak to information technology issues, which databases are proprietary, which are not, etc.

Privilege

Equally important are issues regarding privilege. Rule 26(b)(5)(B) addresses the return of inadvertently produced documents. Agreements regarding privilege should be discussed during the discovery conference. While the best laid plans regarding review of discovery production sent to opposing counsel have the intention of complete review and cull of privileged documents, the reality is there will be inadvertent inclusions. Rule 26(b)(5)(B) provides a procedure for addressing accidental production of privileged information.

In addition, clawback agreements should be given serious consideration. Clawbacks can be used in those circumstances where information that is actually privileged is produced. A clawback agreement would include a mechanism returning, sequestering, and destroying the privileged information. In the event that the receiving party has

disclosed the information before receiving notice from the producing party, the receiving party must take reasonable steps to retrieve the disclosure.

Frequently there will be disagreements between the parties and a privilege dispute will require a court's involvement. The privilege claim must be made by the producing party within a reasonable time. This will be critical in that courts will consider the time factor in determining whether there has been a waiver or forfeiture of the claim.

Accessibility

During a conference, one area of disagreement regarding the exchange of ESI will involve the issue of accessibility. The days of requesting ESI that is difficult to search and retrieve are limited. Under Rule 26(b)(2)(B), ESI that is not reasonable accessible because of cost and undue burden does not normally have to be produced. ESI that is not reasonably accessible may involve hardware or software that is dated or obsolete, and restoring the information would entail undue burden or cost.

If, at the end of the discovery conference and after good faith efforts are undertaken by counsel on both sides, the parties can within a reasonable time not resolve the issues around ESI that is claimed not to be reasonably accessible, the party resisting production can seek a protective order barring production. The burden is then on the movant to prove the information is not reasonably accessible. The party seeking the information, despite the fact that the information is inaccessible, may show good cause that the evidence should be produced considering the limitations of Rule 26(b)(2)(C).

What exactly is "good cause"? Courts have looked at a number of factors including if the request is cumulative or duplicates other evidence produced. If the ESI exists elsewhere, including paper-based evidence, courts may look to that medium. Additionally, courts will disregard the expense of harvesting ESI that is not reasonably accessible if the benefit of the ESI is so great that production must occur. Moreover, courts may allow for sampling of ESI when the usefulness of the ESI that is not reasonably accessible must still be determined. If a sample of the ESI provides relevant useful information, then those findings would be considered in ordering greater production from the unreasonably accessible location. Courts will also consider the quantity of ESI involved. The court may specify conditions of discovery, including cost shifting.

Having some core knowledge regarding the issues of accessibility can make a big difference for both sides. Those attorneys that are versed in the technical issues will have a much easier time at deciding what to go after and what not to go after.

Conclusion

In order to be properly prepared under for the conference under the amended Federal Rules, counsel should do the following:

- Send out the preservation letter as soon as possible. If your client has received one, its dissemination, monitoring and fulfillment is a process and not an event. It is important to follow up to ensure its compliance.
- Contact and involve the corporate information technology personnel early in the process. Litigators have a very short window of time to understand their client's ESI. It is best not to play catch up within the first 99 days.
- Produce accurate inventories of ESI to the opposing side. Let them know what you will and will not be searching.
- Draft an agreement regarding the inadvertent production of privileged documents including ESI.
- Document your efforts to reach an accord regarding discovery and efforts to work out an agreement when disputes arise.

**Albert Kassis is National Director of Esquire Litigation Services, Hobart West. Esquire Litigation Solutions provides nationwide litigation support and technology-based document management solutions. He has advised in-house and outside counsel for Fortune 100 companies on electronic discovery issues. Mr. Kassis received his JD and BA from the University of Maryland. He is also a CPA.*

Esquire Data Discovery Services

Because Every Piece of Electronic Evidence Counts: Count on Esquire

Esquire Litigation Solutions' experienced staff ensures that all documents are forensically sound. They are carefully harvested, preserved, organized, processed and exported to protect against spoliation.

Count on Esquire to:

- Preserve the integrity of the documents
- Process files to your specifications
- Provide a searchable online database

Other Esquire Litigation Support Services:

- Full discovery services
- Video services
- Discovery repository and production
- Trial preparation services
- Trial presentation services

Contact us today for a free consultation or download a white paper at www.esquirelitigation.com.

Esquire Litigation Solutions

EDRM

Electronic Discovery & Records Management Quarterly

SUBSCRIBE TODAY!

3 Easy Ways to Order

Phone: (800) 308.1700 or (212) 337.8444

Email: west.legalworkspublications@thomson.com

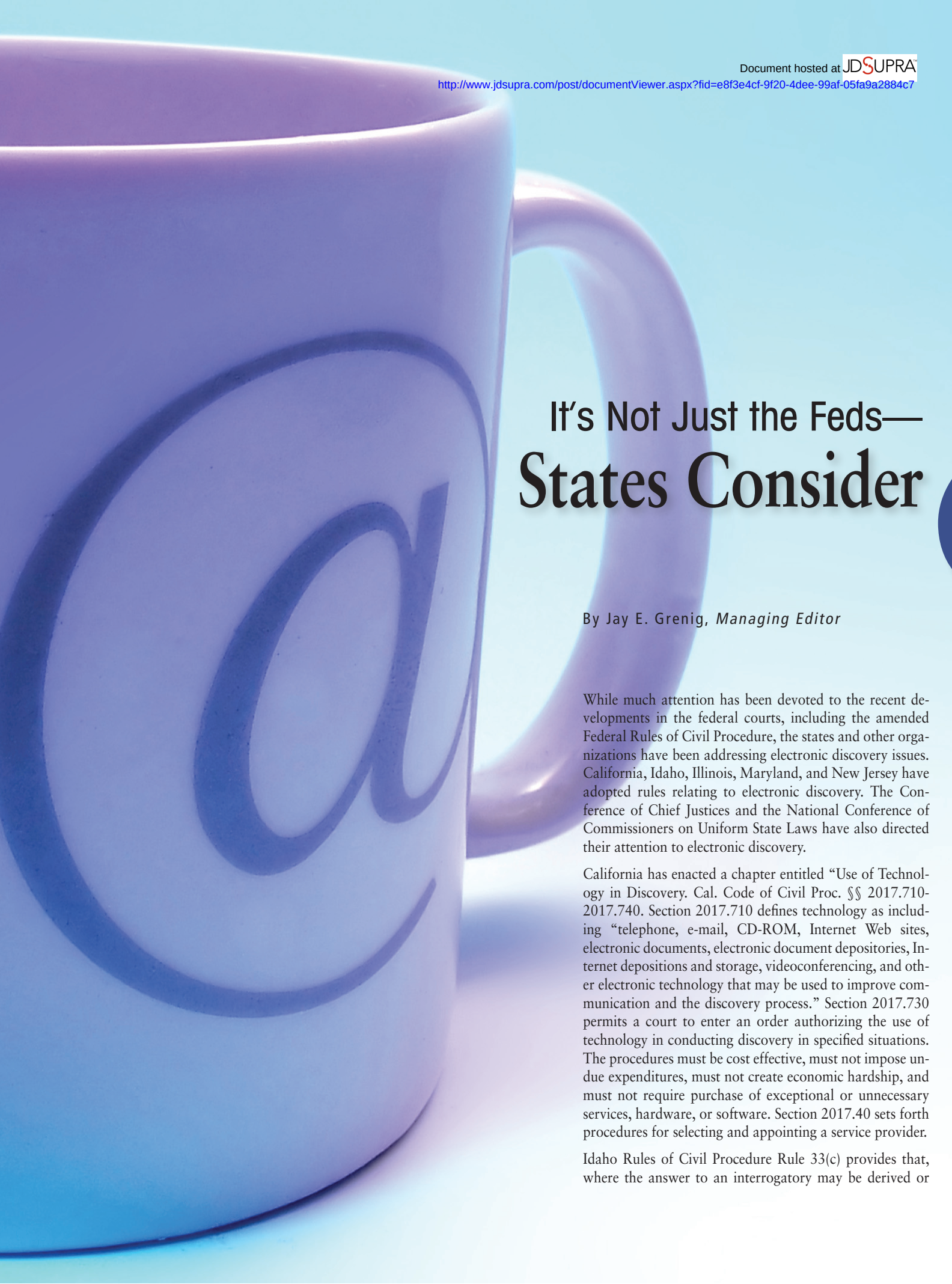
Web: www.westlegalworks.com

One Year Subscription • 4 Issues

Price: $95 • **ISSN** # 1938-4947 • **Code** # 40642683

THOMSON WEST

WEST LEGALworks™



It's Not Just the Feds—States Consider

By Jay E. Grenig, *Managing Editor*

While much attention has been devoted to the recent developments in the federal courts, including the amended Federal Rules of Civil Procedure, the states and other organizations have been addressing electronic discovery issues. California, Idaho, Illinois, Maryland, and New Jersey have adopted rules relating to electronic discovery. The Conference of Chief Justices and the National Conference of Commissioners on Uniform State Laws have also directed their attention to electronic discovery.

California has enacted a chapter entitled "Use of Technology in Discovery. Cal. Code of Civil Proc. §§ 2017.710-2017.740. Section 2017.710 defines technology as including "telephone, e-mail, CD-ROM, Internet Web sites, electronic documents, electronic document depositories, Internet depositions and storage, videoconferencing, and other electronic technology that may be used to improve communication and the discovery process." Section 2017.730 permits a court to enter an order authorizing the use of technology in conducting discovery in specified situations. The procedures must be cost effective, must not impose undue expenditures, must not create economic hardship, and must not require purchase of exceptional or unnecessary services, hardware, or software. Section 2017.40 sets forth procedures for selecting and appointing a service provider.

Idaho Rules of Civil Procedure Rule 33(c) provides that, where the answer to an interrogatory may be derived or

ascertained from the business or other records, including electronically stored information, it is sufficient for the responding party to specify the records from which the answer may be derived or ascertained. Rule 34(a) permits a party to serve on any other party a request to produce and inspect electronic and data storage devices in any medium. Rule 34(b)(1) permits discovery of data or information existing in electronic or data storage devices in any medium. The requesting party must specifically request production of such data and specify the form or manner of delivery in which the requesting party wants it produced. Rule 34(b)(2) permits a responding party to produce data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If production is ordered, payment of reasonable expenses of any extraordinary steps may be required. Rule 45(b) provides for the issuance of a subpoena to a nonparty to produce or permit the inspection and copying of electronically stored information.

Illinois Supreme Court Rule 201(b)(1) provides that a party may obtain full disclosure regarding any matter relevant to the subject matter involved in the pending action including all retrievable information in computer storage. Illinois Rule 214 requires a producing party to produce the documents as they are kept in the usual course of business or organized and labeled to correspond with the categories in the request, and all retrievable information in computer storage in printed form.

In Kansas, the COURT DISCOVERY GUIDELINES provide that the Kansas Rules are meant to facilitate the Federal Rules of Civil Procedure. The GUIDELINES require counsel to be familiar with a client's electronic management system prior to a Rule 26(f) conference. The GUIDELINES state that counsel has a duty to disclose and notify opposing counsel of electronically stored information. Both parties should also meet and confer to identify issues related to identification and scope of ESI generally, email, deleted information, metadata, backup or archived information, format and media, costs and privileged information. The GUIDELINES also apply to issues regarding the production of ESI from non-parties.

Supreme Court of Mississippi Rule 26(b)(5) provides that a party must specifically request electronically stored information and the form of production. A responding party must produce what is reasonably available in the course of business. If the ESI cannot be produced with reasonable efforts, a motion may be filed. If the motion is granted, the court must also issue an order requiring the requesting party to pay for the reasonable expenses in retrieving the information.

Rule 1:9-2 of the Rules Governing the Courts of the State of New Jersey provides that a subpoena may require production of electronically stored information. Rule 4:5B-2 provides for a case-management conference to address ESI. Rule 4:10-2(a) extends the scope of discovery to include ESI. It limits production to reasonably accessible information absent good cause. Rule 4:17-4(d) provides that a party may produce ESI in response to interrogatories. Rule 4:18-1(a)(1) provides that a party may request ESI and Rule 4:18-1(b) permits the requesting party to specify the production format. Rule 4:23-6 provides that a court may not impose sanctions for ESI lost through routine, good-faith operation.

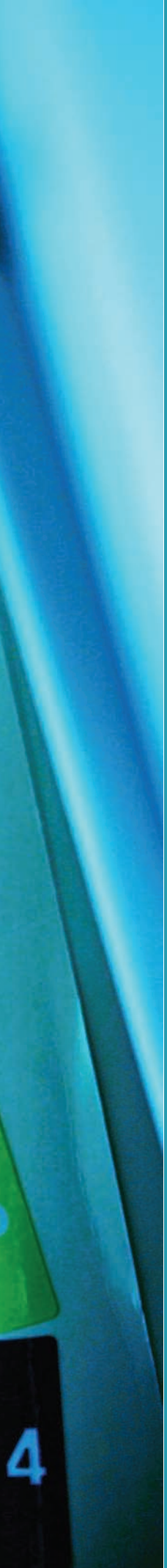
& Adopt E-Discovery Rules and Guidelines

Texas Rules of Procedure Rule 196.4 provides that a party must specifically request electronically stored information and the form of production. The responding party must produce what is reasonably available in the course of business. If the ESI cannot be produced with reasonable efforts, a motion may be made to the court. If granted, the court must make an order requiring the requesting party to pay for the reasonable expenses in retrieving the information

In August 2006, the Conference of Chief Justices authorized the distribution of GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION. The GUIDELINES address the duty of counsel to be informed about client's electronically stored information, subjects should be addressed by the parties in conferring about discovery of electronically stored information, the form of production, the reallocation of discovery costs, inadvertent disclosure of privileged information, preservation orders, and sanctions. Copies of the GUIDELINES can be downloaded from the website of the National Center for State Courts (www.ncsconline.org). The National Center for State Courts also publishes an informative "Civil Litigation Discovery Resource Guide."

The National Conference of Commissioners on Uniform State Laws is drafting a Uniform Discovery of Electronic Records Act. Information on the progress of the Uniform Act can be obtained at http://www.nccusl.org/Update/DesktopDefault.aspx?tabindex=0&tabid=59.

By Conrad J. Jacoby,* Kim Aronchick* and Mel Goldenberg*



Finding the Right Format of Production for

Electronic Information

Under the amended Federal Rules of Civil Procedure that took effect December 1, 2006, litigants must discuss specifically how they would like to receive electronically stored information—e-discovery materials—that will be exchanged over the course of the lawsuit. In the past, such discussions about the "format of production" tended to be afterthoughts delegated to a litigation support professional or the least experienced member of the legal team. This is a topic that requires active involvement by the top members of a legal team, some of whom may never have had a reason to get involved with what seems to be a minor logistical detail.

Competing issues arise in the context of picking a production format for digital discovery materials in a case. While several formats are used today, each has benefits—and shortcomings—that may make it suitable for some but not other electronically stored information (ESI) productions. Put another way, no one single "best" production format works in all cases, and it is up to the legal team to make a judgment call based on their understanding of the needs of their case.

With today's technology, three basic formats are used for producing electronic documents, plus a few minor variations on each. First, of course, people simply print out electronic documents and exchange paper. While paper is universally criticized as old fashioned and fundamentally inadequate, consider the following:

- Paper can be read without any additional technology investment.
- Paper production can easily be divided among multiple reviewers.
- Paper productions can be redacted and bates-numbered with a minimum of technology investment.

Balanced against those considerations, consider the following shortcomings of print production. First, printing electronic documents can create a voluminous physical record that is impossible to review. A single Excel spreadsheet, for example, may print out as over 10,000 pages. Second, printing electronic documents hides some information—the legendary "metadata"—that could be important in helping authenticate a document or convey information about what the author was thinking. Finally, paper documents are not searchable—at least, not very easily. Every lawyer has worked with a box of discovery documents where key documents were identified by post-it notes and color-coded tape flags. That approach may work for very small document collections where a lawyer can keep a general sense of the entire discovery request in short-term memory, but it breaks down for any collection that exceeds even half a box of material. This is perhaps the most important reason why judges increasingly disfavor paper productions unless they are made pursuant to a specific request by the party seeking discovery.

A second format for producing electronic materials is through digital images, usually in Group IV TIFF format. A TIFF image is nothing more than a digital photograph of the document. It's much like printing a document to paper, except that 14,000 images can be stored on a single CD, dramatically shrinking the amount of physical storage space required to store a document collection and greatly reducing the cost of duplicating large portions of the collection when required. TIFF images can be used in just about every litigation support tool on the market; they've been an industry standard for over a decade. It's a very popular production format, and even in an era where "native format" productions are receiving significant publicity, many litigants still exchange discovery documents in TIFF image.

TIFF images didn't become so popular just because they could be squeezed onto CD-ROMs and computer hard drives. TIFF productions commonly include log files that break these images into discrete documents, making it much faster and easier to work with discovery documents. Instead of flipping through all 10,000 pages of a voluminous Excel spreadsheet—to find where it ends (if nothing else), that entire document in TIFF form can be classified and moved about as a single entity. In addition, storing that one document won't take up a quarter of an associate's office. TIFF images can also easily be redacted and electronically numbered using relatively inexpensive tools. Several studies and numerous document review teams have found it is generally much faster to review TIFF images than an identical hard-copy production, particularly if the review team is using flat-panel monitors that don't create as much eyestrain as older CRT displays.

As recently as only a few years ago, many TIFF productions were merely just that—TIFF images with a data file providing document breaks. That was considered a reasonable production format at the time, and this format is still used as a production format in some cases today. However, TIFF images in and of themselves have the same problem as paper documents—they cannot easily be searched. To do that, the recipient of the TIFF images must spend money to have the documents run through an OCR process to create searchable text. For documents that started out in searchable electronic form, this is a extremely inefficient way of extracting information, especially since the process that creates the TIFF images can also harvest the full text of those documents—with no OCR errors—at the same time.

Today TIFF productions have expanded to include a database load file that contains searchable text that has been extracted from the document at the time of TIFF conversion. Extracting the raw text gives you exactly what was typed into the document—there are no OCR transcription errors. In addition, a few courts have found that

Today TIFF productions have expanded to include a database load file that contains searchable text that has been extracted from the document at the time of TIFF conversion.

some amount of extracted text or objective data should be included as part of a TIFF production in order to make the production format "reasonably useful" under the Rules of Civil Procedure. As one final caveat, though, native text extraction preserves all the spelling errors of the original writer. Materials like Instant Messaging ("IM") logs that contain many abbreviations and misspellings can still be difficult to search, even if their text is perfectly extracted.

While a combination of TIFF image and extracted text is the most common production format at the moment, continuing limitations—and developments—in technology highlight a number of shortcomings that make this production methodology unsuitable as a universal production format for all cases. First, TIFF conversion doesn't necessarily guarantee the document will show up exactly as it might have looked when it was printed out on a specific computer. Usually, the substance of the document is more important than its appearance, but disputes can center on how prominently specific contract terms or disclaimers were displayed in a particular document. Second, current text extraction technology does not necessarily pull out every single shred of potentially searchable information from a document. This is done as a matter of policy, since much document metadata has little if any value. Service bureaus and extraction software make educated decisions about which fields are likely to contain potentially interesting information and extract only those, inevitably leaving behind other metadata. Most of the time, this level of text extraction is sufficient to meet a party's discovery needs, but it is possible that a particularly esoteric piece of metadata might be required to help make a point about a specific document. If that metadata wasn't extracted at the time of initial processing, it may not be easily available.

A final concern about producing electronic information in TIFF format is the cost of converting into TIFF image and extracting their searchable text. For voluminous amounts of ESI, it can be expensive to process the collection—money the producing party has to spend just to determine that many of the electronic documents are irrelevant and will not have to be produced in discovery. At some level, this simply feels inefficient.

That line of reasoning has been one driving factor for the rapidly increasing popularity of the third format—the so-called "native file" production format. The idea behind native file production is remarkably simple: Why pay to process voluminous electronic information that's already searchable? Why not simply review these electronic files in their existing format to find the files that are actually responsive? After completing review, only the responsive files would be turned over, still in the same format that they were originally received. The receiving side then has the option (and cost) of processing these materials into whatever they want—TIFF images, paper, or other appropriate format.. On a theoretical level, native file production saves the producing party a significant amount of money and permits the requesting party access to exactly the same information that the producing party has. Imagine a litigation environment with no more disputes over incomplete production of information!

Unfortunately, nothing is ever simple in litigation. First, it has been difficult to develop technology permitting a legal team to search, review, and categorize large amounts of disparate file types and documents. While amazingly sophisticated search tools have long been available—think of Google and Yahoo! and old-time search engines like Altavista—output from these search engines simply did not fit into the work flow of a litigation document review. You couldn't tag batches of documents. You couldn't add notes describing why a given document is important to the case. Tools that integrate solid search with those kinds of review functions had to be built from the ground up—something that continues to this day.

Second, working with electronic files in their native format may actually hinder typical document review efficiency. Most importantly, current technology does not permit a reviewer to redact a native file. One can easily remove or alter text in a native document, but taking these actions changes enough key information used to authenticate ESI that normal automated protocols cannot easily validate the edited document against the original version stored in the ordinary course of business. A second limitation to native file review is that current technology does not permit Bates numbers to be attached to pages of native files. Page-level control numbers offer an easy way to identify

a few courts have found that some amount of extracted text or objective data should be included as part of a TIFF production in order to make the production format "reasonably useful" under the Rules of Civil Procedure.

specific passages in key documents, but, as with redaction, adding a running number to native file documents changes document metadata, making it difficult to authenticate the file for admission into evidence. As a consequence, using native files as exhibits can be awkward and inconvenient. Instead of quickly referencing a specific page within the production, the examining attorney may need to reference "screen X of document entitled 'working notes in preparation for meeting,' as found on John Smith's computer on November 8, 2006."

Between the separate shortcomings of native file and TIFF image plus extracted text productions, decisions about production formats depend greatly on the needs of a specific litigation matter. First, consider the technology available to the legal team for working with incoming electronic discovery materials. Paper is unlikely to be a viable production format, unless discovery is limited to a very small number of documents and e-document metadata will never be of any use in the case. That situation is ever less likely to occur, so legal teams will mostly likely choose between some variation of TIFF production and native file production.

Most legal teams already have ready access to software tools that will work with TIFF images and searchable database text. If not, basic litigation software is a fairly modest expense. However, software may not be the problem. TIFF images can take up a lot of digital storage space. Does a law firm have the empty hard disk space on its computer network to store five million TIFF images? Ten million TIFF images? Once considered exotic, these document collections are increasingly commonplace in the world of e-discovery.

For law firms that do not have the internal infrastructure to hold all the discovery data—or the paraprofessional specialists to maintain large databases—a key question is whether a legal team has a sufficient litigation budget to hire a third-party hosting service to store the data.

For law firms that do not have the internal infrastructure to hold all the discovery data—or the paraprofessional specialists to maintain large databases—a key question is whether a legal team has a sufficient litigation budget to hire a third-party hosting service to store the data. External hosting, also known as "online repositories" or "ASPs," offers outsourced expertise and virtually unlimited storage capacity, albeit for a sometimes steep price. ASPs charge monthly fees for data storage and user access. For litigation lasting a year or less, online repositories may be cheaper than investing in new storage capacity but relatively few cases settle that quickly. Over time, the recurring costs of online repositories can put a significant dent in a litigation budget. On the plus side, outsourcing discovery document hosting also purchases dedicated project and document management expertise, which may not be available from an overbooked internal litigation support staff

Given the cost and storage issues inherent in generating and working exclusively with TIFF images, are native files a better solution? After all, producing these files in their original form avoids substantial processing costs. In addition, multiple tools can index and search native file collections. Shouldn't this be the less expensive and more efficient option?

Unfortunately, working with native files may require investing in entirely new infrastructure or ASP hosting. The two most common litigation support software systems in use today—Concordance and Summation—aren't as adept at working with native files as they are with TIFF images and extracted text. Indeed, they can't deal at all with certain types of native electronic data, such as mainframe computer files, complicated databases, and other data files increasingly exchanged in discovery. Using existing litigation support tools to work with native files may end up working smoothly only after the production has been converted from native format into TIFF image and extracted. That can quickly eliminate any theoretical savings from working with native files.

Second, a receiving party may not care about its ability to redact sensitive information—that's a problem for the party that produced the native files—but it certainly does care about using these documents as substantive evidence. It can be a tedious process to authenticate native files, and a law firm may need to bring in an e-discovery expert for that purpose. Dealing with the logistical issues of authenticating ESI can be a powerful distraction for a legal team and one that reduces the amount of time and energy available for substantive legal analysis and case preparation.

Given the many competing priorities in litigation, no single production format consistently stands head and shoulders above others at this time. Litigation-specific analysis will continue to point one way in some cases and another at other times. That said, legal teams will usually find their choice of production format becomes clear after they have answered the following questions:

- What tools does the team already have for working with electronically stored information?
- What internal expertise and staff does the team already have for working with electronically stored information?
- What budget does the team have for working with electronically stored information?
- Does the team have a protocol in place for authenticating electronic materials exchanged in discovery?

In addition to helping legal teams understand their priorities for a specific case, these questions also serve as a consistent analytical process that can be used in a broad range of legal matters to identify the best way with which to work with digital information. Over time, working through this analysis in a variety of matters will help attorneys and paraprofessionals develop a "gut feeling" about the most efficient ways to proceed with e-discovery. While such instincts must always be reviewed in light of developments in the law and in technology, they still provide a helpful foundation for working successfully with these materials.

*Conrad J. Jacoby writes and lectures extensively on e-discovery and litigation management. He received his B.A. from Yale University and his J.D. from Georgetown University Law Center.

*Kim Araneo has been working in the field of electronic discovery for nearly 15 years. She earned a B.S. from Louisiana Tech University and J.D. from Mississippi College of Law.

*Mel Goldenberg is president of TechLaw Solutions. He received his B.S. from Boston University. TechLaw Solutions is a pioneer in litigation support and information management.

TechLaw's law: use better tools.

ELECTRONIC DISCOVERY is only as good as the tools available and the experts supporting you. TechLaw Solutions helps law firms and corporate legal departments develop and implement strategies to manage electronic and paper document collections for litigation and archival applications. TechLaw Solutions is a trusted discovery management partner offering the most advanced electronic document processing, accelerated content review, and native file review available. Backed by 23 years of experience in litigation support services, our staff has the expertise to understand our client's unique problems and develop tailored solutions to fit their needs with the right tools for the job. TechLaw specializes in creating individualized processing systems on isolated, secure networks for multi-terabyte cases. In addition to 15 branch offices nationwide, the company has five processing centers in Washington, D.C. (Chantilly, VA), Dallas, Denver, Minneapolis and San Francisco.

For more information, call 800-TECHLAW (832.4529).
www.TechLawSolutions.com

TechLaw
SOLUTIONS

West Legalworks™ Presents

Fall 2007 Events

UPCOMING E-DISCOVERY EVENTS

West Legalworks is one of the foremost providers of events to attorneys in the U.S. From local to international conferences and forums, West Legalworks offers over 100 events a year to legal professionals.

Learn more about how West Legalworks can help you and your organization in meeting professional goals by attending these informative events.

SEPTEMBER 28, 2007
Austin, Texas
E-Discovery After the New Federal Rules

OCTOBER 25 - 26, 2007
Chicago, Illinois
E-Discovery and Records & Retention Forum

NOVEMBER 13 - 14, 2007
New York, NY
E-Discovery and Records & Retention Forum

DECEMBER 13 - 14, 2007
San Francisco, CA
E-Discovery and Records & Retention Forum

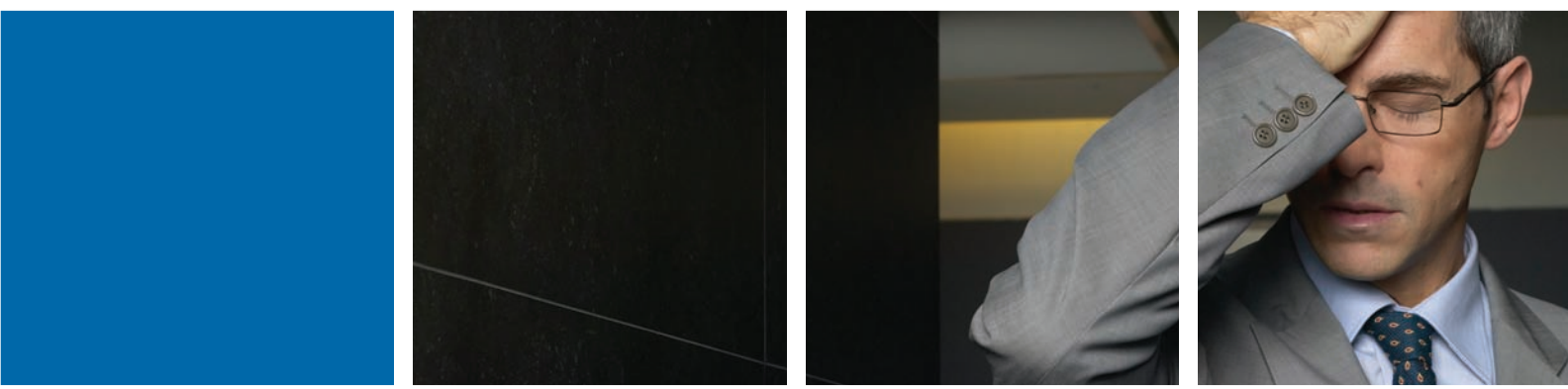
For more information or to register:
visit: www.westlegalworks.com
email: west.legalworksregistration@thomson.com
phone: 800-308-1700

Essential for the professional in you.

THOMSON WEST

WEST LEGALworks™

They e-mailed what?!



You know the people in your organization, now find out what they said.

Ontrack® Firstview™ software gives you the power to analyze e-mail traffic for pre-discovery or internal investigations. Imagine if you could see e-mail connections with just one mouse-click.

Now you can.

Ontrack® Firstview™

www.ontrackfirstview.com

KROLL ONTRACK®