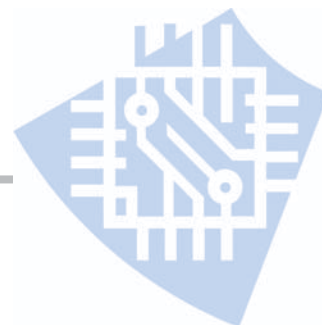


Digital Matters

The Newsletter of the Technology for the Litigator Committee
Section on Litigation, American Bar Association



Vol. 2, Issue 1 Spring 2008

This Issue's Theme:
"The Continued Evolution of eDiscovery and the eDiscovery Rules"



What's Inside:

- From the Co-Chairs... (Page 2)
- Ten Ways to ... Increase Your Knowledge of eDiscovery (Page 4)
- eDiscovery in Canada (Page 6)
- ESI Triage (Page 13)
- Wading Deep in eDiscovery (Page 23)

eDiscovery in State Courts

By Gregory D. Shelton

The Federal Rules of Civil Procedure were amended on December 1, 2006 to address discovery of electronically stored information (ESI). Several states have recently followed suit and adopted new rules, some of which are modeled after the Federal Rules. Other states are currently con-

(Continued on page 5)

eDiscovery 101: What is Metadata and How Do you Produce ESI Containing Metadata?

By H. Hunter Twiford, III and John T. Rouse

The year 2006 saw unprecedented changes in electronic discovery in civil litigation, in part in order to keep pace with the significant changes in the business world.

According to some sources, over 93% of all commercial documents are produced and stored on computers, and of those, only 0.003% are ever printed on paper. Add to that an estimated 3.25 trillion e-mails generated by U. S. businesses in 2002.

Despite this widespread use of electronically generated and stored information, most businesses did not however, adequately take into account the effect of this massive amount of information in litigation decisions.

For example, in a 2003 survey conducted by the American Bar Association, the corporate attorneys surveyed acknowledged that over 83% of their business clients had no formal documentation retention/destruction policies in place.

Federal courts, perhaps in recognition of the almost

universal use of electronically stored information in business (and perhaps as a result of failure of business to proactively manage retention and production of electronic data in litigation), responded with the 2006 amendments to the Federal Rules of Civil Procedure.

The adoption of the amendments to the Federal Rules and the increasing number of judicial opinions require that attorneys, and particularly, litigators, pay close attention to Electroni-

cally Stored Information (ESI) in their cases.

In this article, we take a broad-brush look at the Federal eDiscovery amendments, and take a more in-depth look at "metadata," including why both attorneys and their clients should be concerned about metadata; how to find it; whether it is ethical to "peek" at metadata in documents transmitted or produced to the attorney; whether to scrub metadata prior to transmission or

(Continued on page 6)

Let the Lawyer Beware:

Qualcomm v. Broadcom Judge Holds Lawyers Responsible for Improper eDiscovery Conduct

By Melissa Klipp and Kate Seib

In the most recent decision in Qualcomm v. Broadcom, a contentious patent lawsuit, the United States District Court for the Southern District of California sent a powerful message to attorneys everywhere regarding their obligation to understand and conduct electronic discovery.

Magistrate Judge Barbara L. Major ordered Qual-

comm to pay Broadcom over \$ 8.5 million in attorneys' fees and costs, and referred six of Qualcomm's attorneys to the State Bar of California for possible ethics violations regarding electronic discovery. Although there has been a growing understanding of attorney obligations regarding electronic discovery, it is now very clear that the consequences for failing to meet these obligations are enor-

(Continued on page 7)

Digital Matters

Technology for the Litigator Committee Co-Chairs

Kim R. Jessum

Stradley Ronon

kjessum@stradley.com

Janice V. Mitrius

Banner & Witcoff, Ltd.

jmitrius@bannerwitcoff.com

Digital Matters Editor-in-Chief

Richard S. Stockton

Banner & Witcoff, Ltd.

rstockton@bannerwitcoff.com

Digital Matters Editorial Board

Ernest V. Linek

Banner & Witcoff, Ltd.

elinek@bannerwitcoff.com

Danielle M. Panetta

Goodwin Procter LLP

dpanetta@goodwinprocter.com

Bruce D. Vargo

Robertson, Freilich, Bruno & Cohen, LLC

bvargo@rfbclaw.com

Derek S. Witte

Miller Johnson

witted@millerjohnson.com

From the Co-Chairs



Kim Jessum
Co-Chair,
Technology for the
Litigator Committee



Janice Mitrius
Co-Chair,
Technology for the

Happy Anniversary, eDiscovery!

Welcome to our first *Digital Matters* issue of 2008. The theme of this issue is “The Continued Evolution of eDiscovery and the eDiscovery Rules, which is quite appropriate as we have now passed the one-year anniversary of the implementation of changes to Federal Rules of Civil Procedure relating to eDiscovery (i.e., the eDiscovery rules).

The purpose of this issue, then, is to review how courts have applied the eDiscovery rules in practice, and, more broadly, how federal, state and other courts are handling eDiscovery generally.

“The purpose of this issue, then, is to review how courts have applied the eDiscovery rules in practice . . .”

Thus, the articles in this issue of *Digital Matters* review, among other things, recent federal court deci-

sions framing the scope of eDiscovery, review eDiscovery in the state courts and in Canada, and outline strategic tips for handling eDiscovery in large cases.

What is to be learned from recent court cases regarding eDiscovery and the eDiscovery rules? As detailed in Melissa Kilpp’s piece on the ongoing *Qualcomm v. Broadcom* case starting on page 1, one thing is clear—courts are imposing stiff penalties for

“Courts are imposing stiff penalties for taking eDiscovery obligations lightly”

taking eDiscovery obligations lightly, including holding certain attorneys personally responsible for violations!

Committee Matters

Turning to committee matters, I would also like to welcome my new co-chair for the Technology for the Litigator Committee, Kim Jessum. Kim was formerly one of our Website Editors whose hard work and efforts did not go unnoticed by the Section. As the year progresses, Kim and I are looking forward to an active and productive year.

We want to thank all of the hard working and talented people who continue to volunteer their time and efforts to this committee

(Continued on page 3)

(Continued from page 2)

and the Section of Litigation. In particular, our newsletter editors, website editors and programs subcommittee have put forth significant efforts. Special recognition goes to our Editor in Chief, Rich Stockton, and Editorial Board Member Danielle Panetta who have made significant contributions in putting together this issue and providing a framework to publish multiple issues per year. Also, we provide special recognition to our Web Site Editors, Aimee Kolz and Alan Lamar for all the time and effort spent last year in making

“If you have not visited the Technology for the Litigator committee web site lately, check out what’s new at www.abanet.org/litigation/committees/technology/”

sure we have updated and timely content on our web site. If you have not visited the Technology for the Litigator committee web site lately, check out what’s new at www.abanet.org/litigation/committees/technology/.

Upcoming Programs

Finally, programs are an important aspect of providing member services and we must recognize the significant efforts from our Program Subcommittee Chair, Greg Shelton. Our program in San Antonio would not have been the standing-room-only success without the contributions of Greg. We thank you for your efforts.

This bar year, our committee will have a program at the Section Annual Meeting in April 2008 in Washington DC and also plans to have a breakfast meeting. We are looking forward to continuing the work of the committee in putting on quality programming and we hope that all of

“We hope that all of you can join us at the Section of Litigation Annual Meeting”

you can join us at the Section of Litigation Annual Meeting.

We are looking forward to the new bar year and welcome your thoughts, input and participation. If you would like to become active in the Technology for the Litigator Committee, please contact us. There are several projects within the committee where we could use your help.

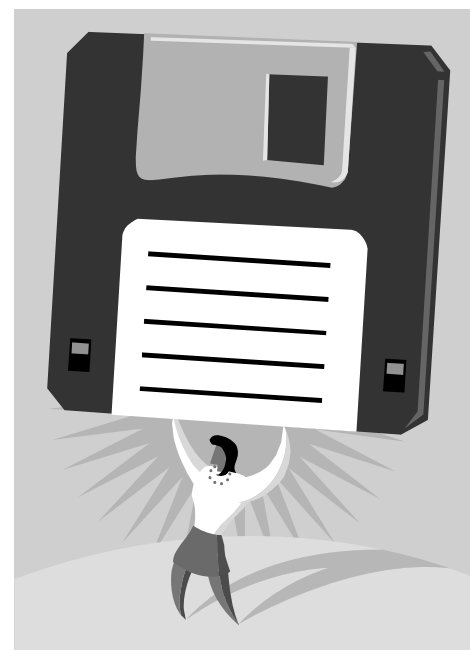
Digital Matters, the Technology for the Litigator Committee Newsletter, is published four times a year: Winter, Spring, Summer and Fall by the Technology for the Litigator Committee, Section of Litigation, American Bar Association. The views contained within do not necessarily reflect the views of the ABA, the Section of Litigation or the Technology for the Litigator Committee. Issue: Spring 2008

© 2008 American Bar Association
321 N. Clark Street · Chicago · IL · 60610

To change your address or be removed from the mailing list, please contact Rich Stockton at rstockton@bannerwitcoff.com or (312) 463-5000.

Visit the Technology for the Litigator Committee on the Web:

<http://www.abanet.org/litigation/committees/technology/home.html>



Column

Ten Ways ...

10

...to Increase Your Knowledge of eDiscovery

More than a year has passed since the implementation of the new rules and the term eDiscovery is still considered a bad word by most of us. There is good news. By increasing your knowledge in a few key areas you (and your clients) can breathe a little easier.



Danielle Panetta
Ten Ways ...
Columnist

1. Know Your Documents

With smaller document universes and paper collections one can cast a wide net reviewing every document with even the slightest potential for relevance. But as technology grows so do the number of documents. In the time it takes to write a letter, you can send ten emails or twenty text messages. It's almost never practical to look at "everything". In fact, the growing number of documents brings this increasingly closer to impossible.

Start with a very targeted universe

that is likely to lead to the discovery of the most on import documents. Armed with that information add custodians and develop terms, continuing to expand this initial targeted search until you keep returning to the same documents.

This is the electronic equivalent of "shepardizing" a case with books. You stop looking for more cases when you keep coming back to the same ones. You know that you have the right custodians and the right search terms when the results keep turning up the same documents. Keep reminding yourself of the main goal: review the smallest universe that captures all relevant documents.

2. Know Your Vendors

With a large matter you are likely to need several vendors. There are companies that collect data, store it, provide the review tool, produce documents, restore old and damaged data or provide any of these services in a foreign country.

You may be able to combine some of these services but there is very little eDiscovery one stop shopping available. Know which services are required for your matter and find the vendor or vendors that best meet your clients needs.

3. Know Your Tech Team

A good litigation technology staff is essential to successful eDiscovery. This is true whether you have a single paralegal who is a bit of a techie or if you have a staff of a few dozen that reside on an entire floor of a large city building. Even if you have the finances, the space and the personnel to forensically restore old back-up tapes at your firm, this is much better left to an outside vendor that specializes in the practice. Talk to your tech-

nology team, know what they can and should handle in-house and what is best outsourced.

4. Know Your Review Team

It just doesn't make sense to have your core legal team vetting out thousands (dare I say millions) of irrelevant documents. A contract review team is essential in any large scale review.

Your review is only as good as your first cut. Your entire discovery process can be negatively impacted if you fail to focus on a few key areas of first line review. Someone from your core team must provide training on your legal issues and get feedback from your review team on a daily basis. Should you have any issues (there are always issues) you can isolate and fix them right away.

Trying to get through a massive amount of documents in a short amount of time will have your review team sitting in front of monitors for many hours a day. Make sure you provide comfortable chairs and the largest monitors that you can afford.

5. Know Your Client's IT Team

Your client will need define all potential data sources and assist in the collection of that data. The client's IT staff must work with the employees, the firm and the vendors to retain and image all documents that become part of your review. Most company's also use some sort of encryption for security measures. If the data is not unencrypted before an image is taken, your copy contains only a corrupt image and the data will need to be recollected.

(Continued on page 5)

(Continued from page 4)

6. Know Your Case

The best eDiscovery practices are going to vary with the facts and legal issues at the core of your case. No one can give a laundry list of what to do and what not to do. The real answer is almost always “it depends”.

Don't lose the forest for the trees. As you re-evaluate your case remember to have the procedure follow the substance. If you have reviewed 15,000 out of 30,000 emails for a custodian who has become moot, don't review the remaining 15,000 emails just because you already started looking at these documents. As the case issues change so must your process.

7. Know Your Custodians

End-user computer usage varies greatly. Some people delete emails as soon as they cross an issue off their list, others keep every email and every draft on the same machine for years. Some custodians put notes in hidden

text, use embedded documents, create multiple drafts or hold data in very large spreadsheets. Any of these uses can have a big effect on your review and production.

8. Know What Your Client Knows About eDiscovery

In-house counsel may not know much about eDiscovery or they may know it much better than you. eDiscovery is an important litigation matter. Make sure that you and your client are on the same page.

You do not want your client to feel lost in the eDiscovery. More importantly, you do not want to appear as if you are lost in the eDiscovery.

9. Know That eDiscovery is an Emerging Practice Area

The practice of eDiscovery is yet to be really developed (or even understood) by many litigators. There is a high level practice of eDiscovery. Understand that your eDiscovery is your

case, your evidence and the essence of your investigation. It directly effects the legal analysis that you are able to provide for your clients.

10. Know What You Don't Know

You don't need to know how to perform all of the day-to-day technical aspects involved, but you do need to know how that effects the day-to-day management of your case and the advice that you ultimately provide.

It is unfortunate, but true: a very small eDiscovery mistake can have very big consequences. Make sure that you understand what has been accomplished and what has not. Know that eDiscovery is frustrating practice development with which most of us struggle.

I will leave with one final need-to-know piece of information: I can think of no time where an eDiscovery issue can be prepared so that someone, somewhere can “Just push a button”; there is no easy button in eDiscovery.

eDiscovery in State Courts (Continued)

(Continued from page 1)

templating changes, have decided not to implement specific eDiscovery rules, or have adopted a “wait and see” approach to see how the Federal Rules work before adopting state rules. Following is a short overview of the Federal Rule amendments and a survey of the eDiscovery rulemaking that has taken place in various states.

Overview of eDiscovery Amendments to Federal Rules of Civil Procedure

Federal Rule of Civil Procedure 26 now requires parties to address early

in the litigation electronic discovery issues including scope of discovery, preservation of evidence, privilege issues, and the format of ESI for production. Parties now must provide “a copy of, or a description by category and location of . . . electronically stored information” as part of their initial disclosures. Fed. R. Civ. P. 26 (a). The Rules explicitly empower courts to enter the parties' agreements into case management orders. Fed. R. Civ. P. 16(b)(5). They also provide for a bifurcation of discovery; permitting a party to produce reasonably accessible data, and hold back less accessible data until the cost of production and need for the data can be assessed. Fed. R.

Civ. P. 26(b)(2)(B). The Rules now contain provisions regarding the procedure for addressing inadvertent production of privileged information. Fed. R. Civ. P. 26(b)(5)(B). Finally, the new Rules provide a safe harbor from sanctions for spoliation if electronic infor-

(Continued on page 24)



The Rules Up North: eDiscovery in Canada



By **Peter Mantas and Genevieve Pellerin**

Traditional rules regarding document discovery have undergone a dramatic transformation in Canada, as they have in the United States, over the past several years. The reason for this change is due primarily to the impact of technology on the creation, storage and retrieval of documents.

In particular, the rise and popularity of email communication has resulted in an explosion in the volume of documents. Email has also become a common form of communication that was previously confined to memory. Unlike memory, emails leave a detailed record of the communication, along with additional information (metadata) which can provide evidence such as the time of the message, and the identity of all the parties who sent and received it. Furthermore, emails along with many other forms of electronic documents are difficult to erase.

What is referred to in both Canada and the United States as

“eDiscovery” can result in a gold mine of evidence. The problem is that getting to the gold, if it indeed exists, is fraught with potentially huge effort and cost, issues of confidentiality and privilege, and problems of document loss.

Courts in Canada are struggling with the unique issues posed by electronic documents during the discovery process. Several provinces, such as Ontario, British Columbia and Quebec have taken the lead by assembling judges, lawyers and experts to study the issues and propose solutions. Revisions to existing rules have begun as a result of these initiatives. On a national level, a Canadian version of the Sedona Conference recently issued “The Sedona Canada Principles” as a guide on eDiscovery matters (for more information, visit www.thesedonaconference.org).

This article provides a quick overview of eDiscovery in Canada, as it exists at this moment in time. It identifies the general rule of discovery, and then discusses how courts have departed from this standard to deal with the unique problems that arise in the context of electronic documents. In particular, this article reviews what

must be disclosed, who pays, how inadvertent disclosure of privileged and confidential documents are handled, and the issue of document preservation.

The General Rule in Canada

All documents in the power, possession or control of a party, that may be relevant to the issues in the legal proceeding, must be disclosed to the opposing party (or parties). Such disclosure is usually done shortly after the close of pleadings and before examinations for discovery.

This rule is not universal across the country. But it is generally applicable. The precise rule governing document discovery in Canada varies based on the court or tribunal in question. Typically, there are specific written rules of procedure governing the disclosure of documents for each provincial court, the Federal Court of Canada (whose jurisdiction is more limited than US federal courts), and the many tribunals that have been established by governments to administer specific subject areas, such as human rights, international trade, or labor matters. Further differences in document disclosure practice can be found between those Canadian juris-

(Continued on page 12)

ESI and the Discovery Rules (Continued)

(Continued from page 1)

production; and how best to produce it in response to discovery requests. Metadata has increasingly become important in the everyday practice of law, and the practitioner should have at minimum a basic working knowledge of metadata in ESI, and what to do – and as importantly, what not to

The New eDiscovery Rules

do – when considering ESI issues in the litigation context.

On December 1, 2006, after years of comments and modifications,

the amendments to the Federal Rules of Civil Procedure regarding electronic discovery became effective. The amendments affecting electronic data

“The Amendments Affecting Electronic Data Include Federal Rules 16, 26, 33, 34, 37 and 45”

include Federal Rules 16, 26, 33, 34, 37 and 45, and this section will briefly discuss the amendments to each.

Rule 16(b), which addresses pre-trial conferences, scheduling and

planning, adds two topics, in subsections (5) and (6), to be addressed in the scheduling order. The scheduling order now may include “(5) provisions for disclosure or discovery of electronically stored information,” and “(6) any agreements the parties reach for asserting claims of privilege or protection as trial preparation material after production.”

The amendments to Rule 16(b) require the parties to discuss electronic discovery at their initial Rule 16 “meet and confer” conference.

The amendments to Rule 26(b)(2) (B) regarding discovery scope and

(Continued on page 7)

ESI and the Discovery Rules (Continued)

(Continued from page 6)

limits provide that “a party need not produce electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost,” except upon an order compelling such production.

The “not reasonably accessible” amendment allows a party to identify “inaccessible” ESI, and the court can, upon proper motion, then make an informed determination as to whether the ESI is in fact “not reasonably accessible,” and assess the perceived

burden and likely cost of production. If the requesting party prevails in a motion to compel production, the amendment gives the court the option of imposing conditions, including shifting some or all of the costs of production to the requesting party.

New Rule 26(b)(5)(B) relates to information produced, which is subject to a privilege claim, and allows a party, under certain circumstances, to produce documents to the opposing side without waiver of the attorney-client privilege or waiver of work-product protection by use of what is commonly referred to as a “clawback”

provision.

This amendment took into consideration of the volume of stored ESI subject to production in litigation, and in response to and recognition of the substantial cost of reviewing the ESI for privilege and relevancy, loosened the prior rules on inadvertent production of privileged information to address the cost issues and promote quicker initial production.

The amendments to Rule 26(f) add three topics to be discussed at the parties’ initial discovery confer-

(Continued on page 8)

Let the Lawyer Beware (Continued)

(Continued from page 1)

mous.

Qualcomm alleged patent infringement by Broadcom based on its manufacture, sale and offers to sell “H.264-compliant products.” A key issue was whether and when Qualcomm participated in and communicated with an industry standard-setting body, the JVT. It claimed it did not do so until late 2003. Participation in 2002 or early 2003 would provide evidence of patent waiver that would have been grounds for a dispositive pre-trial motion by Broadcom.

Over the course of discovery, Broadcom served several discovery requests for information regarding Qualcomm’s JVT participation. Qualcomm replied that responsive documents would be produced if found after a reasonable search. However, Qualcomm never conducted a reasonable search.

Despite serving an expert declaration confirming the absence of any JVT records, Qualcomm never searched the computers of key company witnesses, and did not search for obvious keywords, like “H.264.” In fact, even when 21 responsive JVT emails from 2002 were discovered while preparing a witness for trial, the Qualcomm trial team did not produce them. Most shocking to the court was that even with this discovery, neither Qualcomm nor their retained counsel conducted any inquiry into why the emails had not previously been discovered or into the reasonableness of its document collection procedure. On cross-

examination, Qualcomm’s witness admitted that she had received these emails, and the company was forced to produce them.

The jury returned a verdict for Broadcom. At the close of trial, Broadcom moved for sanctions. In response, Qualcomm agreed to search the current and archived emails of five trial witnesses using the search terms “JVT, avc_ce, and H.264.” In fact, they searched the email archives of 21 em-

“Every Meaningful Security Program Starts by Determining Your Organization’s Appropriate Balance of Usability and Security”

ployees and located more than 46,000 documents (300,000 pages) that were inconsistent with the arguments they made at trial about JVT participation.

In his comprehensive order, the trial judge found that Qualcomm had actively and wrongfully concealed the JVT information and actively hidden this concealment from the Court and opposing counsel. He further found that “counsel

(Continued on page 14)

ESI and the Discovery Rules (Continued)

ence: (1) the preservation of discoverable information; (2) discovery and form of production of ESI; and (3) whether the court should enter an order allowing privileges to be asserted post-production. These amendments require the parties and the court to consider eDiscovery issues very early in the case, and make specific provisions related to ESI discovery and production of ESI.

The amendments to Rules 33 and 34 regarding interrogatories and production allow a party to answer an interrogatory by referring to specific ESI, and add the term “electronically stored information” to the production list of Rule 34. The amendments to Rule 34(b) outline the actual procedure for eDiscovery, and provide that a document request “may specify the form or forms in which electronically stored information is to be produced.”

The producing party is allowed to object to the requested form, and propose an alternative form of produc-

***“The Amendments to
Rules 33 and 34 Regarding
Interrogatories and
Production Allow a Party to
Answer an Interrogatory by
Referring to Specific ESI”***

tion. If an agreement cannot be reached between the parties, the court must decide the method and form in which the parties will produce the ESI. If no particular form is specified in the document request, the producing party may produce in the “form or forms in which it is ordinarily maintained” or in “electronic forms that

are reasonably usable.” The rule also provides that “a party need not produce the same electronically stored information in more than one form” in the absence of an agreement of the parties or a court order to the contrary.

Rule 37(f) was amended to include a safe harbor: “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

Disputes have already begun regarding the undefined terms “exceptional circumstances” and “good-faith” contained in the amendment. Much of the recent press received regarding eDiscovery disputes

(Continued on page 9)

GET PUBLISHED IN DIGITAL MATTERS!

Digital Matters seeks articles relating to technology and the lawyer for publication in future issues. To discuss publication opportunities, please contact Rich Stockton, Digital Matters Editor-in-Chief, at rstockton@bannerwitcoff.com or (312) 463-5000.

**Digital
Matters**

WRITER-EDITOR WANTED FOR LITIGATION NEWS

If you are a lawyer with a journalism degree or journalistic experience and would like to join the Litigation News editorial board, send your resume, three writing samples, and references to Doug Motzenbecker at DMotzenbecker@podvey.com

APPLY TODAY!!!

ESI and the Discovery Rules (Continued)

(Continued from page 8)

has centered on sanctions imposed on parties for failing to produce ESI or for spoliation of ESI. These sanctions have included dismissal of claims and defenses, as well as adverse instructions. Other recent cases address when a “litigation hold” notice should be employed, and steps that should be taken to ensure preservation and production of ESI.

The amendments to Federal Rule 45 incorporate the changes made to Rules 26 and 34 for subpoenae, and provide that “a subpoena may specify the form or forms in which electronically stored information is to be produced.” Similar to the Rule 34(b) amendment provisions, a producing party responding to a subpoena may object to the requested form of production.

Of particular importance to the litigator are the amendments to Rules 16 and 26 regarding conferences. The attorney must immediately communicate with the client regarding the client’s electronic data, and must gain at least a basic understanding of the client’s systems, including where the ESI is or could be located and how it can be accessed, in order to be adequately prepared to discuss ESI with opposing counsel at the initial Rule 26 (f) conference. The lawyers on both sides must be able to discuss and agree on eDiscovery issues at the Rule 26(f) conference, including identification, collection, production, review and clawback. The lawyers are then able to go to the court at the Rule 16 conference with fewer discovery disputes and less likelihood of

The Zubulake Decisions — A Primer

subsequent spoliation accusations and sanctions requests.

There are now a number of cases discussing the Federal Rules applicable to electronic discovery to give

guidance to the practitioner. Of those, the six (to date) separate opinions arising from the *Zubulake v. UBS Warburg* litigation authored by United States District Judge Shira A. Scheindlin of the Southern District of New York have extensively discussed eDiscovery issues, are widely consid-

“The Six (to Date) Separate Opinions Arising from the Zubulake v. UBS Warburg Litigation . . . are ‘Must Reads’ for Anyone Practicing in the Federal Courts”

ered authoritative and are “must reads” for anyone practicing in the federal courts.

In *Zubulake I*, Judge Scheindlin sets out seven-factor test for determining whether to shift the cost of discovery. *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D. N.Y. 2003) (“*Zubulake I*”). *Zubulake II* addresses the plaintiffs’ reporting obligations regarding electronic discovery. *Zubulake v. UBS Warburg, LLC*, 230 F.R.D. 290 (S.D. N.Y. 2003) (“*Zubulake II*”). In *Zubulake III*, Judge Scheindlin requested evidence of the costs and results of an initial test sample, data restore, and then ordered restoration of back-up tapes, applying the seven-point test from *Zubulake I*.

Judge Scheindlin then ordered the plaintiff to pay 25% of the costs of restoring data and conducting word searches for relevant information. *Zubulake v. UBS Warburg, LLC*, 216 F.R.D. 280 (S.D. N.Y. 2003) (“*Zubulake III*”). In *Zubulake III*, Judge Scheindlin also held that the defendants’ attorneys fees for reviewing restored data for relevancy and privilege should not be shared.

In *Zubulake IV*, Judge Scheindlin addressed litigation holds and when

the obligation to impose a hold arises, and determined that the obligation to preserve relevant documents arises “once a party reasonably anticipates litigation.” *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D. N.Y. 2003) (“*Zubulake IV*”). Once litigation is reasonably anticipated, a party “must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.” *Id.* at 218.

In *Zubulake V*, Judge Scheindlin held that once litigation is reasonably anticipated, “a party and her counsel must make certain that all sources of potentially relevant information are identified and placed ‘on hold’ to the extent required in *Zubulake IV*.” *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422, 432 (S.D. N.Y. 2004) (“*Zubulake V*”). The court further noted: “To do this, counsel must become fully familiar with her clients’ document retention policies, as well as the clients’ data retention architecture.” *Id.* *Zubulake V* additionally requires that counsel must not only make the client aware of the obligation, but must also monitor compliance and facilitate production.

Finally (so far), Judge Scheindlin held in *Zubulake VI* that evidence of discovery sanctions were not admissible at trial, with the exception of an adverse inference instruction arising out of discovery violations. *Zubulake v. UBS Warburg, LLC*, 382 F.Supp.2d 536 (S.D. N.Y. 2005) (“*Zubulake VI*”). Judge Scheindlin outlined her decision in *Zubulake V*, noting that “[the defendant] acted willfully in destroying potentially relevant information, which resulted either in the absence of such information or its tardy production.” *Id.* at 546 (quoting *Zubulake V*, at *12).

The court concluded that the appropriate remedy was an adverse inference instruction of whether the jury

(Continued on page 10)

ESI and the Discovery Rules (Continued)

was satisfied that the defendant's failure to produce this information was reasonable. *Id.*

Judge Scheindlin also allowed the plaintiff to introduce correspondence between counsel regarding discovery matters, but only if the defendants first opened the door by introducing evidence that their failure to produce was reasonable. *Id.* There are many other eDiscovery cases handed down daily by the federal district courts, and it is beyond the scope of this paper to discuss even a representative sampling (for a more detailed discussion, see, for example, H. Hunter Twiford, III and Adam H. Gates, "Beware the Rocky Shoals: Navigating the Uncharted Waters of Electronic Discovery," *The Mississippi Lawyer*, Vol. LIII, No. 3, February-April, 2007).

The *Zubulake* opinions are, however, the starting point for any eDiscovery research and analysis.

What Type of ESI is Discoverable?

Based on the amended rules and the recent case law, the question arises, "What is discoverable?" The short answer is, "Everything relevant." In the *Zubulake* opinions, the principal ESI at issue was email. ESI can, however, include virtually any form of electronic communications, including emails, instant messages, text messages and voicemails, and any electronically created or stored documents, including Word or WordPerfect documents, spreadsheets, databases and any customized electronic information which may be used.

The eDiscovery amendments to the Federal Rules place strong emphasis on the ability to review files in their "native formats," the associated file structure as defined by the original application creating the ESI. For example, Microsoft Word documents in their native format are created as ".doc" files. The native format of a

Microsoft Word document thus is not the printed or scanned document produced in printed format or electronically as a .pdf or .tiff image, but the original .doc format. While native file format may be unfamiliar territory for many litigators, some familiarity with the concept is important, because the

"The eDiscovery Amendments to the Federal Rules Place Strong Emphasis on the Ability to Review Files in Their Native Formats"

native file format of ESI is where metadata is found.

What Is Metadata?

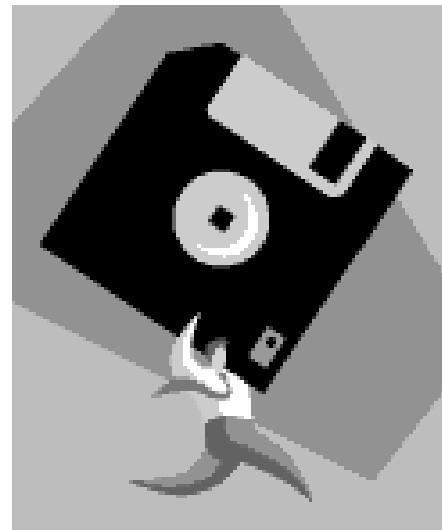
When a document is created on a computer, the particular computer program used creates certain information about what the user is doing. The program automatically tracks in the background who created the document, when it was created, how long the user worked on the document, how many words are in the document, who has edited it, when it was last edited, and much more. This computer-created information is called "metadata." The simple definition of metadata is "information about information."

A more precise definition is provided by The Sedona Conference, a legal think tank consisting of judges, attorneys and others experienced in electronic discovery matters:

Metadata is information about a particular data set or document which describes how, when and by whom it was collected, created, accessed, modified and how it is formatted. Can be altered intentionally or inadvertently. Can be extracted when

native files are converted to image. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed (see <http://www.thesedonaconference.org/content/miscFiles/tsglossarymay05.pdf>).

Although metadata is contained in most documents created on a computer, the user cannot ordinarily readily see much of it. Metadata is embedded in computer files tied to the specific document. A technologically proficient user who knows what she is looking for and how to find it though, can "mine" the metadata to discover a potential goldmine of useful information.



The file containing the specific metadata is called an OLE ("Object Linking and Embedding storage) file. OLE files travel with a document wherever it goes (in native format), and generally contain information such as the user's name and initials, the company name, the computer name, the server name, previous authors and

(Continued on page 11)

ESI and the Discovery Rules (Continued)

(Continued from page 10)

revisers, the number of revisions or versions, hidden text, comments and other file properties and summary information.

At first glance, this metadata

“At First Glance, This Metadata Might Appear Relatively Harmless. In the Litigation Context, However, Metadata Can Potentially Provide the ‘Smoking Gun’ in a Mountain of Documents.

might appear relatively harmless. In

the litigation context, however, metadata can potentially provide the “smoking gun” in a mountain of documents. In the expert’s hands, metadata provides an electronic paper trail of each person that “touched” a particular document and what that particular person did to it. For example, a witness might testify that a document was created and sent on a particular date, or that she was the only person who worked on that particular document, while the metadata tied to the particular document would reveal the document’s true origin and edits, and possibly provide counsel with powerful cross-examination ammunition.

Specific Dangers

Two standard features in Microsoft Word® create significant metadata risks: “Versions” and “Track

Changes.” The “Versions” feature in Microsoft Word saves a new version of the document in the OLE automatically, without giving the user notice of the changes. The risk is that the “Versions” feature, if activated, automatically records all of the user’s prior versions, including any revisions by

“Two Standard Features in Microsoft Word® Create Significant Metadata Risks”

any clients or other counsel, with the attendant risks of inadvertently disclosing confidences. This information, if simply linked to an email, would then be accessible by the receiving attorney, who may well be counsel opposite.

(Continued on page 17)

Business and Commercial Litigation in Federal Courts

EDITED BY ROBERT L. HAIG



Covering the most common commercial litigation subjects, the new edition of *Business and Commercial Litigation in Federal Courts* takes readers through a step-by-step analysis of the entire litigation process. With 16 new chapters and more than 500 pages of forms and jury charges on CD-ROM, the set is an indispensable resource for the commercial litigator.

SPECIAL SAVINGS FOR LITIGATION MEMBERS

The eight-volume set is now available at a 40% discount to Section of Litigation members.

www.abanet.org/litigation/books

 SECTION of LITIGATION
AMERICAN BAR ASSOCIATION

eDiscovery in Canada (Continued)

dictions that follow either the English common or French civil law system.

In Canada there is usually a two stage process to document disclosure. The first is the delivery of a list to the opposing party (usually sworn in affidavit form) of all relevant documents, including privileged documents. The expense of assembling documents for the purpose of making disclosure is generally not recoverable.

Thereafter, all documents, except those that are privileged, may be inspected by the opposing party and/or their attorney. A copy of the documents may also be obtained at that party's cost. In reality, most parties simply copy and bind their own documents, deliver them to the opposing party, and seek the cost of this production later in the litigation. The copying and binding of documents is considered a disbursement that, in most Canadian courts, is recoverable by a party if they are successful at trial (administrative tribunals are less likely to award costs in a proceeding, however).

Historically, the kinds of documents that had to be disclosed were not restricted to paper based records. For example, they could be sound recordings or film. The requirement to disclose electronic documents is therefore not novel. What is different now is the volume and nature of electronic documents. Documents such as emails or mobile device data, which are recent technological phenomenon, have proven to be difficult to apply to existing rules of disclosure and production.

Electronic Documents

There is little doubt that an electronic document must be disclosed. In an era where most evidence is stored in electronic format, to exclude such documents from the litigation process would be absurd. A more difficult question is whether or not the

item in question is a document that carries with it a disclosure requirement.

Canadian courts have held that electronic information such as database records (see *Sourian v. Sporting Exchange Ltd.*, 2005 CanLII 4938 (Ont.S.C.)), and records created by or stored on mobile devices such as BlackBerries or iPods, are documents that must be disclosed (see *CIBC v. Genuity*, 2005 CanLII 3944 (Ont.S.C.)),

“Canadian Courts Have Held That Electronic Information Such as Database Records . . . And Records Created by or Stored on Mobile Devices Such As BlackBerries or iPods, are Documents that Must be Disclosed”

para. 3). Moreover, data must be disclosed in its electronic (or native) format. Where necessary, software to be able to access or understand the data may be ordered disclosed (see *Jorgensen v. San Jose Mines et al.*, 2004 CanLII 1653 (B.C.S.C.)). Metadata, which is information generated not by a person but by software (for example, a record of the date and time that the document was created), is also a document that must be disclosed (see *Logan v. Harper*, 2003 CanLII 15592 (Ont.S.C.)).

In some circumstances, “deleted” documents must be disclosed. In the world of electronic documents, “deleted” does not necessarily mean the document has been destroyed. In many cases, where a document has been “deleted” on a storage device like a hard drive, it in fact continues to exist. However, the document has been tagged so that it may be overwritten by other documents at some

point in the future. The document is also difficult to access and for most people, will require expert assistance to retrieve.

Courts have typically refused to order parties to produce storage devices like hard drives (see *Desgagne v. Yuen et al.*, 2006 CanLII 955 (B.C.S.C.)), unless there is some evidence of the concealment of potentially relevant documents (*Rhodia UK Ltd. v. Jarvis Imports (2000) Ltd.*, 2005 CanLII 1628 (F.C.T.D.)). The theory behind this approach is that a storage device is like a filing cabinet, which would normally not be accessible for search by an opposing party. Following this theory of disclosure, courts have also resisted ordering a party to “reconstruct” documents.

Proportionality and Cost

Where obtaining electronic records is unduly difficult and/or expensive, as a result for example of the volume of documents, or their dispersal among other records unrelated to the litigation, significant challenges arise. On the one hand, the disclosing party does not want to undertake a massive document hunt that may ultimately be fruitless. On the other hand, the party seeking disclosure will not want to be deprived of a document that could make the difference between a win or a loss (the proverbial smoking gun).

The issue of the burden of disclosure becomes more acute where the size of each party is disproportionate. For example, where one party is an individual and the other is a large corporation. In such a case, the individual, who typically has documents that are few in number and easy to access, can make broad and onerous demands on the opposing party without fear of being subjected to a similar burden. In such a case, electronic disclosure may become more than a

(Continued on page 13)

eDiscovery in Canada (Continued)

(Continued from page 12)

procedural step in the litigation, it can be an end in itself that serves to pressure a corporation to settle at nuisance value. As class actions and mass litigation become more common in Canada, this problem has assumed increased importance.

In response to this issue, courts have departed from the traditional notion that any document that “may”

**Canadian “Courts Have
Departed from the
Traditional Notion That
Any Document That ‘May’
Be Relevant Should be
Disclosed.”**

be relevant should be disclosed. The courts have instead been guided by a principle of “proportionality.” In other words, they have begun to look to the effort and cost involved in seeking the documents, and to weigh these factors against the expected value of the documents to the litigation, should they be obtained (see *Dominey v. Cosmetology Assn. of N.S.*, 2004 CanLII 116 (N.S.S.C.)).

In some cases, the interim cost of seeking the documents may be shifted. For example, the cost of hunting for documents may be split between the parties, or ordered to be carried by one of the parties. There is no specific rule that exists regarding cost-shifting in Canada. It remains one of court discretion, guided by the specific facts of the situation (see, for example, *Barker v. Barker*, 2007 CanLII 13700 (Ont.S.C.) and *JDS Uni-*

phase Inc. v. Metconnex Canada Inc., 2006 CanLII 34432 (Ont.S.C.)).

Privileged and Confidential Documents

Where large volumes of documents are disclosed, the risk of inadvertent disclosure of privileged or confidential information is heightened. This problem is of particular concern to Canadian counsel following the recent Supreme Court of Canada decision in *Celanese Canada Inc. v. Murray Demolition Corp.*, 2006 CanLII 36 (S.C.C.). In this case, the Court held that where legal counsel came into possession of the opposing parties privileged documents, the attorneys and their law firm had to be removed from the case. Other recent cases from lower courts have similarly

(Continued on page 16)

ESI Triage: A Method for Strategically Deploying Resources for the Large Case

By Michael Kelleher and
Jeff Ghielmetti

The growing importance of electronically stored information (“ESI”) in litigation and regulatory proceedings has created unprecedented demands on legal and IT resources. In large cases (defined for this article as cases involving 20 or more custodians), legal and IT teams are frequently called upon to deal with huge volumes of ESI under severe time and budget constraints. Meeting these demands requires an understanding of how ESI can be “triaged” by deploying resources to acquire and analyze the most critical ESI first, processing that initial data inexpensively and then using the understanding of the case from the early ESI to guide the review

and processing of the remainder of the ESI. This article discusses the need for triage and proposes a series of steps that can be used in this “ESI triage” process.

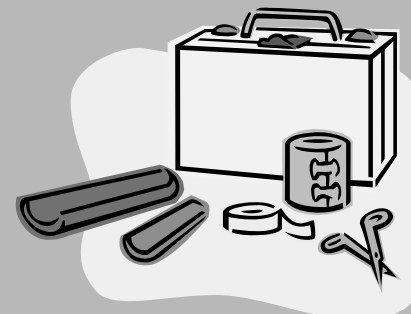
The Pressures Creating the Need for ESI Triage

Volume: The volume of ESI in litigation and regulatory proceedings has exploded beyond anything that could have been imagined a decade ago. Less expensive storage technology has made it routine for businesses and individuals to store multiple gigabytes or even terabytes of data. The ease of copying, transmitting, and storing ESI means that ESI is now found with more custodians and in more places and forms than

ever. As the volume, locations and formats of ESI have expanded, the burden and cost of finding, collecting, processing, reviewing and producing this data has also grown.

Time: Unfortunately, as the volume of ESI has increased, the time for legal and IT teams to deal with the ESI has been collapsed by numerous factors, including “rocket dockets”, amended Federal Rules requiring early and detailed meet and confer sessions about ESI, and aggressive case management by judges. Another

(Continued on page 20)



Let the Lawyer Beware (Continued)

(Continued from page 7)

participated in an organized program of litigation misconduct and concealment throughout discovery, trial and post-trial.” He referred the motion for sanctions to the magistrate.

In determining whether sanctions were appropriate, Magistrate Judge Major found clear and convincing evidence that Qualcomm intentionally engaged in conduct designed to prevent Broadcom from learning of its JVT participation. Qualcomm and its retained counsel also failed to heed several warnings signs that should have alerted it to the fact that its document search and production were inadequate. For example, neither Qualcomm nor retained counsel searched the computer of its first 30(b)(6) witness for relevant files, nor did they provide her with relevant documents to ensure that she was knowledgeable about the key JVT issues. Even when she was impeached and Qualcomm agreed to produce a second 30(b)(6) witness on the JVT issues, Qualcomm and retained counsel did not search his computer, “nor take any other action to prepare him.” The court found that an adequate 30(b)(6) investigation “should include an analysis of the suffi-

ciency of the document search conducted to date and, when electronic documents are involved, an analysis of the sufficiency of the search terms and locations.”

The court ordered Qualcomm to reimburse Broadcom for all of its attorneys’ and expert fees. It reasoned that had Qualcomm produced the responsive emails, Broadcom would have obtained a pre-trial adjudication and would not have had to spend the significant amounts it did to try the case.

However, what is most significant is that the court did not stop at sanctioning Qualcomm. Instead, the court found that six of Qualcomm’s retained lawyers were also responsible for the concealment. These lawyers had good reason to suspect there was additional responsive information, but chose to ignore the evidence and warning signs and accept Qualcomm’s unsubstantiated assertions regarding discovery. Had any of the attorneys insisted on reviewing Qualcomm’s records regarding the locations searched and terms utilized, they would have discovered the gross inadequacy of

(Continued on page 15)



Powerful Ideas, Straight from the Source.

If you’re like most lawyers, time is at a premium. While in-person CLE programs are great for networking, it can be difficult to make time to travel to a seminar.

With the Litigation Series Teleconferences, you get the programming you need, wherever you are. Featuring nationally known lawyers and judges, the programs offer a lively and balanced examination of the issues litigators care about. It’s as easy as picking up the phone. No plane ticket required.

Get connected today at
www.abanet.org/litigation/teleconferences/

 SECTION of LITIGATION
AMERICAN BAR ASSOCIATION

Let the Lawyer Beware (Continued)

(Continued from page 14)

the search and the suppressed documents. Because the six retained attorneys either intentionally or recklessly ignored this responsibility and then used the lack of evidence to repeatedly and forcefully make false statements to

“Because the six retained attorneys either intentionally or recklessly ignored this [eDiscovery] responsibility and then used the lack of evidence to repeatedly and forcefully make false statements to the court and jury, Judge Major . . . referred them to the State Bar of California for an Appropriate Investigation.”


the court and jury, Judge Major suspected a violation of their ethical duties. She referred them to the State Bar of California for an appropriate investigation. She did not impose monetary sanctions, although she found them appropriate, because of the possibility that Qualcomm would seek contribution from the attorneys, and because referral to the Bar would have a sufficient deterrent effect.

In what should become required reading for attorneys conducting electronic discovery, the court clearly set forth the responsibility that the attorneys failed to meet. Attorneys must work with their clients to “ensure that both understand how and where electronic documents, records and emails are maintained and to determine how

best to locate, review and produce responsive documents. Attorneys must take responsibility for ensuring that their client’s conduct a comprehensive and appropriate document search.” She even went so far as to explain that if the attorneys “were unable to get Qualcomm to conduct a competent and thorough document search, they should have withdrawn from the case or taken other action to ensure production of the evidence.”

Finally, the court ordered Qualcomm and retained counsel to participate in a comprehensive Case Review and Enforcement of Discovery Obligations (“CREDO”) process. The purpose of this process is to identify the failures in case management and discovery protocol. This was to include a

detailed analysis of the factors that contributed to the discovery violations, such as insufficient communication (between client and counsel, counsel and counsel and senior and junior attorneys), inadequate case management, and inadequate discovery plans. Qualcomm would then be required to create a protocol to prevent such violations in the future.

The clear lesson from this case is that it is crucial for retained counsel to be an active and informed participant in discovery and in particular, the electronic discovery process. 

Melissa Klipp is a partner at Drinker Biddle & Reath LLP in Florham Park NJ. Kate Seib is an associate at Drinker Biddle & Reath LLP in Florham Park NJ.

EDISCOVERY TIP

Look before you leap. The file format your opponent touts as the “standard” for email, for example, may not be the “standard” after all. Indeed, your client may be using POP, IMAP or MAPI, all of which could be called the “standard,” and conversion to another format could be very difficult. Plan ahead, or consult your (and your client’s) IT personnel before agreeing to produce ESI in a particular “standard” file format.

**Digital
Matters**

eDiscovery in Canada (Continued)

(Continued from page 13)

found that the inadvertent disclosure of documents can result in the disqualification of opposing counsel (see, for example, *Dublin v. Montessori Jewish Day School of Toronto*, 2006 CanLII 7510 (Ont.S.C.); *Chan v. Dynasty Executive Suites Ltd.*, 2006 CanLII 23950 (Ont.S.C.); *Doust v. Schatz*, 2002 CanLII 129 (Sask.C.A.)). Therefore, steps must be taken to ensure that documents are reviewed for privileged information. This will necessarily add to the cost and effort of a large electronic disclosure situation.

The protection of confidential or business sensitive documents is treated differently. Such documents are typically protected against inadvertent disclosure by an agreement between the parties. Furthermore, in the event of inadvertent disclosure, there is added protection through a general rule that parties are deemed to undertake that they will not use documents they receive as part of the litigation for any purpose collateral to the immediate proceeding.

Destruction of Documents

An additional disclosure problem regarding electronic documents is their propensity for destruction. The word "destruction" may sound sinister, but in many cases, the destruction of electronic documents is part of an innocent and necessary policy to automatically purge huge volumes of data that accumulate every day. Such purging is often done without human intervention. Furthermore, in cases where litigation arises, relevant documents may be lost through scheduled purging, and despite efforts to preserve.

In Canada, a party is required to preserve documents that may be relevant to the litigation (see *Doust v. Schatz*, 2002 CanLII 129 (Sask.C.A.)). The obligation arises once they become aware of the litigation. In addi-

tion, a party is required to implement policies, whether litigation is contemplated or not, to preserve documents for a reasonable period of time. Case law suggests that documents should be preserved, at a minimum, for any relevant limitation periods for an action against the party (see *Moezzam Saeed Alvi v. YM Inc. (sales)*, 2003 CanLII 15159 (Ont.S.C.)).

A party must err on the side of

"A party must err on the side of caution when deciding what electronic records to preserve"

caution when deciding what electronic records to preserve. Where documents have not been preserved, or destroyed, courts may draw an adverse inference.

Historically, the destruction of documents, also referred to as spoliation, was an evidentiary doctrine (see *St. Louis v. R.* (1895) S.C.R. 649 which stands for the proposition that where one party destroys evidence there is a rebuttable presumption that the evidence destroyed would have been adverse to that party's interest." (at para. 17)). A finding of spoliation resulted in an adverse inference by the court against the party responsible for the destruction. In other words, the court would find that the evidence destroyed contained information that would have assisted the opposite party's case.

In extreme circumstances, where there was willful destruction of evidence, a person could be found in contempt of court. Contempt is a criminal matter. However, while the sanction against the offender is extreme (criminal conviction, fines and/or imprisonment), a finding of contempt is difficult to obtain. Canadian

(Continued on page 17)




(Continued from page 16)

courts are reluctant to convict civil parties for contempt, prosecutors are busy with other cases, and the standard of beyond a reasonable doubt applies (see *Dreco Energy Services Ltd. v. Wenzel*, 2005 CanLII 185 (Alta.C.A.)).

Recently, Canadian courts have considered treating spoliation as an independent tort. However, the law on whether or not spoliation is a tort remains unsettled in Canada (see *Logan v. Harper*, 2003 CanLII 15592 (Ont.S.C.)).

The Way Forward

As in the United States, the law and practice regarding electronic documents in Canada is relatively sparse and in flux. Judges, attorneys and experts continue to work towards introducing national guidelines to the process of electronic discovery, to assist courts and tribunals, and to bring consistency to the practice. Fresh court decisions are providing further guidance. However, new forms of technology will continue to pose unique discovery challenges. Furthermore, the inherent conflict between small and large parties, each with their own opposing views as to whether broad or limited eDiscovery should be permitted, will likely result in much more litigation. This will lead to further court decisions that will help define a relatively new practice area. 

Peter Mantas is a litigation partner with Heenan Blaikie LLP and a member of the bars of Ontario and New York. He can be reached at pman-tas@heenan.ca.

Genevieve Pellerin is a paralegal with Heenan Blaikie LLP and a member of the bars of Ontario and Quebec.

ESI and the Discovery Rules (Continued)

(Continued from page 11)

The “Track Changes” feature allows multiple parties to work in collaboration on documents, and permits a user to send drafts of documents, with edits and comments, to others, including co-counsel, the client, and opposing counsel. The receiving user can then review the specific changes made by each user, and either accept or reject them. The risk with using “Track Changes” is that changes may be hidden.

If, for example, the “Hidden Text” option is turned on, the user editing the document may make changes without realizing that those changes are automatically being recorded in the background without any action by the editing user. This is but a single example of the metadata created by a single software application. Such software package has its own way of recording and saving metadata, although industry experts agree that metadata is significantly more prevalent in Microsoft products than in those of its competitors.

Finding Metadata

“Simple” metadata can be accessed by a minimally-proficient user, while more complex or extensive metadata is likely the province of the computer forensic expert.

In order to access general metadata about a specific document, the Windows user need only open Windows Explorer. Once Windows Explorer is open, the user can navigate to the particular folder that contains the document of interest. Once in the desired folder, the document can be displayed in “Details” view.

To arrange the documents in “Details,” the user simply clicks on “View” on the menu bar, and selects “Details” in the dropdown list. The screen will then display a list of all of the documents contained in that particular folder, with headings that include name, size, type, date modified,

and similar information. The user can then right click on the caption bar and obtain a list of the most commonly used metadata. The last option in the dropdown list is “More.” By selecting “More,” the user receives a list of all of the metadata that Microsoft creates about the particular file.

Dates are always important for litigation purposes, and there are three main dates that can be selected

***“Dates Are Always
Important for
Litigation Purposes,
and There Are Three
Main Dates That Can
Be Selected from
Microsoft’s Metadata”***

from Microsoft’s metadata list, including the date created, the date modified and the date accessed. For photographs, there is metadata which lists the actual date on which the photo was taken.

When navigating in specific documents, the user can also view metadata about a particular document by clicking on the “File” menu. Under the “File” menu, there is a selection entitled “Properties,” which provides general metadata about the specific document.

The metadata provided about the document will depend on the type of document, and whether it is a text document, a spreadsheet or another format. Within Microsoft Word, the user can also choose the menu options “View” and “Mark-up.”

This particular feature within Microsoft Word is the equivalent of the “Track Changes” feature discussed above, and can show the user the

(Continued on page 18)

ESI and the Discovery Rules (Continued)

(Continued from page 17)

original document, the original with any mark-ups, and the final document with all mark-ups. This tool can also show each user's or reviser's identity, comments, insertions and deletions, and is a powerful tool to discern the origin of a particular Microsoft Word document.

Why Should Attorneys (and Their Clients) Be Concerned?

In the past several years, metadata has become a concern to anyone who transmits electronic documents. Given the pervasive role of technology in everyday life, an attorney must understand how to properly integrate electronic evidence into each case in order to effectively, competently and zealously represent the client. The attorney must exercise at least basic competency in the representation of the client, and such competency, at least for the litigator, now involves being at least moderately well-versed in electronic discovery.

Some "horror stories" regarding metadata: in 2005, an anonymous, unsigned Microsoft Word document was circulated referring to the "anti-civil rights and anti-immigrant rulings" of Judge Samuel A. Alito, Jr., shortly after his nomination

to the Supreme Court by President Bush. A review of the document's metadata disclosed that the memo was drafted by two authors who were, in actuality, members of the Democratic National Committee. The metadata revealed both

"[A]n Anonymous, Unsigned Microsoft Word Document Was Circulated Referring to the 'Anti-Civil Rights and Anti-Immigrant Rulings' of Judge Samuel A. Alito, Jr. . . . A Review of the Document's Metadata Disclosed That the Memo Was Drafted by . . . Members of the Democratic National Committee."

the authors' names and the date of creation of the document, which was, interestingly (but perhaps not coincidentally), prior to Judge Alito's nomination.

In another example, the New England Journal of Medicine found metadata revealing that Merck & Company had deleted certain data in a study about Vioxx concerning heart attacks. Merck attempted to dismiss the finding, stating that the Vioxx data uncovered by the New England Journal had been deleted because the heart attacks occurred after a cut-off date for information collection in the study.

Another example somewhat closer to home and which has been floating around the internet for some time involves a large law firm partner who passed off an assignment for a corporate client to an associate. A memo was drafted, supposedly by the partner, and transmitted to the client via email without having the metadata scrubbed from the document. The client examined the memorandum's metadata, and determined that it was the associate, not the partner, who was the document's author.

The metadata also showed only minor edits by the partner. The principal embarrassment came, however, when the partner billed the client as if he had drafted the document, charging the client the partner's rate. This example has not been confirmed, but if true, would likely destroy the relationship as well as raise a myriad of ethical concerns.

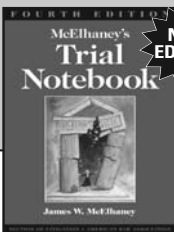
Is It Ethical to Peek at Metadata?

As with any other facet of the law, counsel must exercise at least minimum competency in the representation of a

(Continued on page 19)

www.ababooks.org

FOURTH EDITION



McElhaney's
**Trial
Notebook**

James W. McElhaney

**NEW
EDITION**

**McElhaney
is back – and
better than ever**


A new edition of the ABA's all-time best-selling book on trial practice. Expanded, updated and revised by the author, this new edition of *Trial Notebook* includes 30 years of James McElhaney's clear, lively and memorable prose from *Litigation Journal*. Nearly a third larger than the previous edition, the book now includes 90 chapters that cover everything from discovery through rebuttal and provides you with techniques, tactics and strategies for every stage of trial. James McElhaney knows his subject better than anyone, as a practitioner and as a professor. The result is information, grounded in actual courtroom experience, that you will understand, enjoy and use daily in court. Used again and again by thousands of trial lawyers, *Trial Notebook* is certain to make your trial work more effective. Bulk discounts available.

2005 792 pages
6 x 9 Paper
ISBN: 1-59031-503-0
Product Code: 5310348
Regular Price: \$64.95
LT Member Price: \$54.95

SECTION of LITIGATION
AMERICAN BAR ASSOCIATION

AMERICAN BAR ASSOCIATION

Phone: 1-800-285-2221
 Fax: 1-312-988-5568



www.ababooks.org

ESI and the Discovery Rules (Continued)

(Continued from page 18)

client. Basic competency now involves being versed in electronic discovery. However, most attorneys involved in electronic discovery are under duties not listed in their state's Rules of Professional Conduct – duties of which they may not even be aware.

As Judge Scheindlin warned in the “Postscript” of *Zubulake V*, “Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully

**“Most Attorneys
Involved in
Electronic Discovery
Are Under Duties
Not Listed in Their
State’s Rules of
Professional
Conduct—Duties of
Which They May
Not Even Be Aware”**

on notice of their responsibilities to preserve and produce electronically stored information,” *Zubulake V*, 229 F.R.D. 422, 440 (S.D. N.Y. 2004), and recognized several duties incumbent on counsel engaged in eDiscovery. *Id.* See also *Kleiner v. Burns*, 2000 WL 1909470 (D. Kan. Dec. 15, 2000) (ordering the parties to “continue to preserve data that they know, or should know, is relevant to the ongoing litigation, including preservation of all data compilations, computerized

data and other electronically-recorded information”).

At least one court has held that a lawyer’s duty of fundamental competence now encompasses that same level of competency as it relates to digital technology, especially the information technology systems used by one’s client. See, *G.T.F.M., Inc. v. Wal-Mart Stores, Inc.*, 2003 WL 22439791, No. 01 Civ. 6595VM (S.D. N.Y. October 27, 2003) (not reported).

On August 5, 2006, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 06-442 regarding metadata, concluding that “the Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party or an agent of an adverse party.” ABA Standing Comm. on Ethics and Prof’l Responsibility, Formal Op 06-442 (2006).

The Committee pointed out in its opinion that Rule 4.4(b) is the only provision in the ABA Model Rules of Professional Conduct which addresses the lawyer’s obligations regarding inadvertently-received information. Rule 4.4(b), added in 2002, states that a lawyer who receives information that she knows or should know was sent inadvertently “shall promptly notify the sender.” ABA Model Rule of Professional Conduct 4.4(b). The Committee’s notes to Rule 4.4 state, “Rule 4.4(b) is silent as to the ethical propriety of a lawyer’s review or use of such information.” *Id.*

The ABA Model Rules serve as a model for the rules of professional conduct in 47 states, but are not followed in California, Maine and New

York. The states considering the issue have split on whether it is permissible for counsel to examine metadata in documents transmitted by counsel opposite, with a distinction made by some as to whether the production was inadvertent.

The Maryland State Bar Association’s Committee on Ethics has issued an opinion regarding metadata, holding, like the ABA opinion, that it is not an ethical violation to look at metadata received from opposing counsel. Maryland State Bar Association Committee on Ethics Opinion 2007-09 (October 19, 2006).

The New York State Bar Association’s Committee on Professional Ethics, taking a different approach, determined that an attorney’s attempt to glean metadata from an adversary’s document may violate New York’s ethics rules. Opinion 749, issued December 14, 2001, prohibits counsel from using computer technology to “surreptitiously obtain privileged or otherwise confidential information” of an opposing party. New York State Bar Ass’n Formal Op. 749.

The opinion cites New York’s ethics rule, which prohibits a lawyer from engaging in conduct “involving dishon-

(Continued on page 24)



ESI Triage (Continued)

(Continued from page 13)

internal time constraint is the advantage conferred by allowing counsel to know and understand the case earlier. Mastering the ESI as early as possible allows counsel and the party to understand the strengths and weaknesses of a case and to chart a course to guide the case to a desired outcome.

Cost: The soaring cost of ESI has created sticker shock among clients and imposed budgetary constraints on legal and IT teams. Legal and IT teams are now asked to do more with fewer people and at lower cost. In order to meet budget constraints, teams must think creatively about what tasks can be automated, what tasks can be performed by people with lower billing rates (perhaps in less expensive regions of country or even the world), and how the time of the core legal team can be used and leveraged most effectively.

Finding the Key Custodians

A core observation that can guide deployment of ESI resources is that in a typical case, a few key custodians have

the bulk of responsive documents. We have observed that even in cases with a hundred or more custodians, as much as 90% of the responsive documents can come from just

“We have observed that even in cases with a hundred or more custodians, as much as 90% of the responsive documents can come from just five to ten custodians”

five to ten custodians. The concentration of responsive ESI among a few key custodians dictates that an effective ESI triage must identify the key custodians and deal with their data first (both in terms of collection and review). When the ESI of the key custodians has been collected, processed, and partially reviewed, counsel will have a much better understanding of the case. Armed with this new data, counsel can make more informed decisions on what else to process and review.

Plan, Coordinate, Communicate and Document

Effective ESI triage requires planning, coordination, communication and documentation to make sure that ESI is identified, preserved and collected in a thorough and defensible process.

ESI triage should include an early case kick-off meeting attended by inside and outside counsel, paralegals and representatives from IT to educate the team, establish lines of communication, and plan for success. The kick-off meeting agenda should include a review of the case and claims, identification of the key witnesses/custodians, and an introduction to the company's culture, organizational structure, data sources and contacts within the company. This meeting provides an opportunity for counsel and IT to share information, to ensure that custodians and data sources are identified, and to set realistic and achievable goals and to do items.

Data preservation requires careful attention early in the case to avoid the loss of data and the inevitable resulting accusations of spoliation. At the case kick-off meeting, the status of data preservation efforts should be reviewed (e.g., any litigation hold /document preservation memoranda sent to custodians and any preliminary data collections). After the kick-off meeting, newly identified custodians must re-

**WRITER-EDITOR WANTED
FOR
LITIGATION NEWS**

If you are a lawyer with a journalism degree or journalistic experience and would like to join the Litigation News editorial board, send your resume, three writing samples, and references to Doug Motzenbecker at DMotzenbecker@podvey.com

APPLY TODAY!!!

(Continued on page 21)

ESI Triage (Continued)

(Continued from page 20)

ceive the document preservation memorandum, and counsel should follow up with each custodian with a phone call or visit to ensure that the notice was received and understood. These preservation steps should be tracked by the litigation team in a simple database that will also be used for tracking collections. Should discovery disputes arise later, this preservation and collection database can be critical evidence for establishing that counsel and the party diligently sought to meet their discovery obligations.

Over-Collect ESI

Our recommended ESI triage strategy is to over-collect ESI and later narrow the collected data through computer processing and review. We err toward over-collection because data is too easily lost – corporations are fluid, employees and servers come and go, tape backups are moved, stored and moved again, and trying to control that environment has proven to be impossible or impractical. Murphy's Law dictates that if a "hot" document is accidentally deleted by the custodian, opposing counsel will learn of the document from another source. Another common scenario is that two years after the collection, the case changes direction and a key employee is gone, or data has been lost or moved to off-site tape backup storage. Once lost, ESI can become the center of a very expensive spoliation fight that can end up determining the outcome of the litigation.

In collecting data, the ESI should be copied and stored on dedicated litigation computers to prevent inadvertent loss. Internal corporate IT employees are often relied upon for collections because they are much

less expensive than outside attorneys or consultants. However, because the proper collection and preservation of data can become central to the outcome of the litigation, it is critical that internal IT resources have the supervision, training and expertise necessary to become witnesses if necessary. In particular, the collection must be performed in a standardized way by

“[I]t is critical that internal IT resources have the supervision, training and expertise necessary to become witnesses if necessary.”

trained personnel and carefully documented to establish a chain of custody.

Machine Processing of the ESI

Despite the risks of lost ESI, an over-collection strategy has not historically been the norm for eDiscovery because large volumes of data drastically increased costs. Over-collection increased costs in a world where most eDiscovery vendors charged by the gigabyte and armies of attorneys were required for brute force review of each page of ESI.

However, as ESI technology has developed and companies and their counsel have become more experienced with the processing and review of ESI, alternatives to “per-gigabyte”

pricing and brute force review have emerged. In particular, several eDiscovery companies have developed programs that can quickly process the majority (about 80%) of ESI without human intervention and prepare it for review. (The remaining 20% of ESI that the tools cannot automatically process typically consists of uncommon file types or corrupt or secure files – these files can be set aside for later processing while triage of the remainder of files continues).

These sophisticated computer programs for ESI processing are a key component in the success of ESI triage. ESI triage calls for using these computer programs to process the ESI from the five to ten key custodians, then using common sense to filter out (but not delete) non-essential files by file type, location, or topic. Large volumes of data, up to fifty gigabytes per day, can be processed and readied for review with these programs.

Delivering Key Custodian Data to Counsel ASAP

ESI triage focuses on getting the most relevant ESI into the hands of the attorneys as soon as possible. Early access to the documents is critical for developing an understanding of the case and a strategy. Using the process described above of prioritizing the ESI collection from key custodians and using machine processing of the ESI, counsel can have documents to search and review electronically in just a few days from the start of the process.

Completing the Review

Once counsel has received the most critical ESI for initial review, the

(Continued on page 22)

ESI Triage (Continued)

(Continued from page 21)

ESI team must transition to a structured and thorough review of the entire ESI data set as necessary to satisfy discovery obligations. This should involve the following tasks and considerations:

Continuing Collections and Processing: The IT staff will continue collecting from other custodians and data sources, processing ESI and documenting the effort.

Electronically Categorizing the ESI for Efficient Review: Computerized searching, sorting and pre-marking of ESI can make the ESI easier and quicker to review. For example, one technique is to collect the names of all inside and outside counsel, search the data for those names, and pre-mark those documents as potentially privileged so that those documents receive careful review. Another possibility for targeting and accelerating the review is the use of concept search engines that identify groups of related documents by analyzing patterns in the language used in the responsive documents.


Using a First Pass Review Team to Narrow the ESI Population: Using a "first pass review team" of inexpensive contract attorneys can be an effective way to triage ESI by quickly reducing its volume. First pass reviewers use computer searches to look for large groups or patterns of documents, marking those documents that are clearly not relevant for suppression (not deletion) and marking potentially responsive documents for further review. In our experience, first pass review can quickly reduce the total volume of data that must be reviewed more thoroughly by up to 92%. Once first pass review is about 30% complete, outside counsel's associates can be added to the review team for second pass review of the potentially responsive documents.

Incorporating Your Learning into the Review: As the review progresses, the ESI team will learn additional information that should be incorporated into the review. For example, the reviewers will usually identify new custodians who must then receive the litigation hold memorandum and have their ESI collected. It is possible that these later collections may be more targeted and focused than the first collections because the team now understands what types of issues arose in review of the early collections.

Limiting the Scope of ESI Production: As counsel and IT begin to understand the ESI in a case, the team can work to limit the scope of ESI search and production through agreements with opposing counsel and/or court orders. For example, the parties may agree that they will only review documents for production if certain keywords are found in those

documents. In negotiating which keywords to include in such a list, the knowledge of the document population gained through ESI triage can be very valuable.

Using ESI Triage to Your Advantage

Handling ESI efficiently and well can provide an enormous advantage in litigation and regulatory proceedings. The party that has the best early understanding of the ESI evidence can often control the scope, direction, and ultimately the outcome of a dispute. Conversely, failing to deal with ESI effectively can be expensive and disastrous. The principles of ESI triage can help guide parties and their counsel through this process toward the best outcome. 

Michael Kelleher is a partner at Folger, Levin & Kahn LLP.

Jeff Ghielmetti is the Director of Legal/Discovery Technology at Qulas, Inc.

***Visit the Technology for the
Litigator Committee's Web
Site!***

***[http://www.abanet.org/
litigation/committees/
technology/home.html](http://www.abanet.org/litigation/committees/technology/home.html)***



Be Careful What You Wish For—Wading Deep in eDiscovery

By Alfred A. (“Al”) Malena, Jr.

The advent of the recent modifications to the Federal Rules of Civil Procedure to implement rules for electronic discovery were much anticipated and discussed. The new rules were designed to govern the preservation, collection and production of electronic records, which of course is a huge issue with our increasingly technological society. The combination of complex and difficult to understand technological aspects (metadata, anyone?) for the uninitiated, the inevitable growing pains as new rules are adapted to meet real life situations, and the distaste for discovery disputes in general, have made for interesting results as judges sort out eDiscovery. (The cases discussed here necessarily include those that began or had opinions issued prior to enactment of the new rules.)

How Does It Feel to be Tasered?

The only players in litigation who hate discovery disputes more than attorneys are judges. Generally, judges are happiest when the parties can keep the discovery disputes to themselves and not come to the court for resolution. Of course, lawyers being who they are, that often does not happen.

In *Williams v. Taser Intl., Inc.*, 2007 WL 1630875, (N.D. Ga. 2007), a federal District judge was called on to resolve a discovery dispute regarding searching of databases for electronic documents. The judge initially ordered the parties to list specific deficiencies they alleged existed with the other parties’ discovery responses,

ordered them to confer on the record, and then provide the court with a list of remaining issues.

The court held a hearing and ordered the parties to each create a specific protocol to govern how electronic discovery would proceed in the case. The court then issued the opinion cited above. It begins with an orderly consideration of requests for additional interrogatories and an analysis of how they should be counted, and continues with a scolding for boilerplate objections.

The court then gets to the heart of the dispute – a disagreement over how Taser would search its databases for responsive discovery documents. The parties’ dispute included the timing of the production, what specific search terms would be used and how much participation the plaintiffs would have in the process. The plaintiffs demanded to actively participate in the search, including having an attorney

“The plaintiffs demanded to actively participate in the search, including having an attorney sit with the tech person doing the search . . .”

ney sit with the tech person doing the search, providing exact search terms to be used, having a defense attorney immediately review the results for privilege, and then have the plaintiff’s attorney immediately review the result.

As you might imagine, the defendant strongly disagreed – it wanted to receive the requested search terms by e-mail, perform the searches itself, notify the plaintiff of how many documents were returned in the search results, and if the plaintiff liked that

number, then review them for privilege. The Court disliked both proposed approaches, wisely stating that putting the attorneys in a room together was a recipe for disaster, and concluding a remote procedure was a recipe for delay.

The court went on to issue a jaw-droppingly specific order: it lists 21 specific search terms to be run on Taser’s databases. These terms range from “fibrillation” to “‘multipl*’ within 10 words of ‘discharg*’”. Taser would then review the results for privilege, under a very limited definition of privileged claims specified by the Court, and Taser was ordered to provide a written description of the protocol used.

Taser was ordered to conduct the search and produce the results and a privilege log within 30 days. It is clear that the judge had lost his patience with the parties, as the issuance of such a specific list goes further than most judges would want to go into the swamp of discovery disputes.

The opinion includes an additional notable item. The court specifically criticizes Taser’s argument that the eDiscovery demands of the plaintiffs placed a burden upon it, stating that “... Taser implies that because it has elected to hire and train only a single technology employee, and because it has chosen to retain only a handful of attorneys to conduct document review, it is somehow relieved from its obligations to timely respond to Plaintiffs’ discovery requests. That is not the case.” *Taser* at 7.

While there is no way of knowing from the opinion whether Taser’s position was reasonable, the implications of the use of eDiscovery demands as a club are evident.

Napster’s Effects Live Long After the Original Site

One of the biggest issues in eDiscovery is the question of the “litigation

(Continued on page 29)

ESI and the Discovery Rules (Continued)

(Continued from page 19)

esty, fraud, deceit or misrepresentation” or that is “prejudicial to the administration of justice.” *Id.* New York State Bar Opinion 782 specifically addresses metadata, and concludes that “lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets . . . [and] use of computer technology to access client confidences and secrets revealed in metadata constitutes ‘an impermissible intrusion of the attorney-client relationship.’” New York State Bar Ass’n Formal Op. 782. This opinion seems to be premised on the attorney’s affirmative use of software to recover metadata in order to rise to an ethical violation, and may now be somewhat dated.

The Florida Bar prohibits a lawyer from looking for metadata in a document sent inadvertently. Florida Bar Op. 06-2. The Alabama State Bar’s ethics panel advised in a recent opinion that the unauthorized mining of metadata to uncover confidential information in electronic documents constitutes professional misconduct. Alabama State Bar Office of Gen. Counsel, Op. RO-2007-02.

A recent opinion was handed down in September 2007 by the Legal Ethics Committee of the District of Columbia Bar. Ethics Opinion 341 addresses the review and use of metadata in electronic documents. D. C. Bar Opinion 341. The D. C. Bar examined other states’ ethics opinions, and reached the compromise position that a receiving lawyer is prohibited from reviewing metadata sent by an adversary only where the receiving lawyer has actual knowledge that the metadata was inadvertently sent. In such instances, the receiving lawyer should not review the metadata before consulting with the sending lawyer to determine whether the metadata includes work product of the sending lawyer, or confidences or secrets of the sending lawyer’s client.

Scrubbing Metadata

There is an important distinction to be drawn between the day-to-day transmission of electronic documents, both between attorneys, and with their clients, and the production of ESI pursuant to discovery requests. As to the former, the lawyer must always consider attorney-client privilege in communications, and when appropriate, “scrub” metadata

(Continued on page 25)

eDiscovery in State Courts (Continued)

(Continued from page 5)

mation is lost in the regular course of business. FED. R. CIV. P. 37(f).

eDiscovery Guidance Documents for States

Uniform Rules Relating to the Discovery of ESI

On August 2, 2007, the National Conference of Commissioners on Uniform State Laws adopted the *Uniform Rules Related to the Discovery of Electronically Stored Information*. These model rules are based on the Federal Rules of Civil Procedure. They do not, however, contemplate a mandatory conference amongst the parties early in the litigation as called for in Federal Rule of Civil Procedure 26. Rather, the *Uniform Rules* suggest

that a conference occur, but allow parties to opt out.

Guidelines for State Trial Courts on Discovery of ESI

The Conference of Chief Justices recently published *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* (see Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* (Aug. 2006) (available at <http://www.ncsconline.org>). The *Guidelines* are not binding, nor are they model rules, but are simply an additional tool to assist state court judges “in identifying the issues and determining the decision-making factors to be applied” in electronic discovery disputes. The *Guidelines* make several recommendations to judges

that are substantially similar to the Federal Rules, but differ in some respects. For instance, they recognize that not all states have adopted civil rules that require counsel to confer early in a litigation. Thus, courts in those states are advised to “encourage” counsel to meet and confer if electronic discovery is likely to be an issue in a case. The *Guidelines* also provide a list of factors to be considered when deciding a motion to protect or compel discovery of electronically stored information.

State Court Rulemaking

At least 14 states have adopted electronic discovery rules in all or part of their judicial systems. Many more are contemplating rules or watching to see how the Federal Rules and other

(Continued on page 26)

ESI and the Discovery Rules (Continued)

(Continued from page 24)

from documents sent to opposing counsel to avoid potential liability for disclosure. Failure to remove metadata from documents created or revised by an attorney prior to transmission outside the firm will likely become a fertile source of future attorney malpractice claims. Conversely, scrubbing metadata from documents produced in discovery, particularly when the metadata is requested to be produced and is potentially relevant, is probably a violation of the new Federal Rules, and according to the *Zubulake* opinions, will expose both the attorney and the client to potentially severe sanctions.

Once the distinction is made between scrubbing metadata contained in day-to-day communications between counsel and properly requested discoverable metadata, the issues can be more easily parsed. Many lawyers use scrubbing programs which

“Many Lawyers Use Scrubbing Programs Which Eliminate Metadata from Electronic Documents Sent from Their Offices”

eliminate metadata from electronic documents sent from their offices – in fact, some commentators posit that it may be malpractice not to routinely scrub such metadata.

There are multiple methods of scrubbing metadata from documents transmitted from the attorney’s office. One, and perhaps the simplest, option is to convert the document to Adobe

Acrobat PDF format, which turns the document into a “flat” image, with some basic (and relatively harmless) metadata which might still be accessed if the recipient has the full version of Adobe Acrobat. (The new Acrobat 8.0 Professional software, for example, contains a built-in metadata removal and redaction tool that can search for and permanently remove selected metadata.)

Another method to permanently remove metadata is to print the document, and then scan it into a pdf document. Recipients cannot alter or even access the original document. Corel has included metadata removal functions in its WordPerfect program, and Microsoft has recently joined Corel by including a similar metadata removal function in its Office Suite programs.

The most widely-used tools, however, are third-party products which integrate with Microsoft Word and Outlook. These products are set to automatically initialize upon the user sending an email, and search attachments for metadata, both identifying and requesting user confirmation of metadata deletion.

Finally, there is always the sure-fire method of eliminating metadata altogether: printing and then, faxing or mailing the printed document. This method, however, is rapidly disappearing as a result of client demands, time constraints and storage and access concerns.

It is important to note that whichever method is chosen, there should be a standard scrubbing procedure throughout the firm. Attorneys and staff should be trained on the standard protocol, and the process should be automated to the maximum extent possible to avoid the inadvertent transmission of “unscrubbed” documents, particularly by untrained or unaware lawyers.

Form of Production of ESI

Amended Federal Rule of Civil Procedure 34(b), effective December 1, 2006, permits a party seeking production of electronic documents to “specify the form or forms in which electronically stored information is to be produced,” and requires that “[u]nless the parties otherwise agree, or the Court otherwise orders,

(i) a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request; (ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable.” (Fed. R. Civ. P. 34(b)).

Amended Rule 34(b) permits the requesting party to specifically request the documents in their native format. The native format includes the related metadata. The responding party may oppose producing the documents in that format, but must make a formal objection to the specific form requested on a basis conforming with the Federal Rules. The objection should be for reasons ordinarily recognized by the courts, such as cost, inconvenience or breadth of the request. There is no valid objection to the production of documents simply because the requested ESI in native format may contain harmful or embarrassing metadata.

The rules regarding production of ESI again underscore the importance of early and frequent communication between the lawyer and the client to determine the breadth and scope of ESI in order to be prepared for the

(Continued on page 27)

eDiscovery in State Courts (Continued)

(Continued from page 24)

states' rules are implemented and received. A list of online resources relating to these state rules is included on page 29.

Early Rulemaking Efforts

Texas, the first state to adopt eDiscovery rules, enacted Texas Rule of Civil Procedure 196.4 in 1999. The rule requires the requesting party to specifically request production of "electronic or magnetic data" and to specify the format of production. The producing party must produce "reasonably available" information, but may object to producing information that it cannot retrieve through "reasonable efforts." If the court still orders production, the cost of any extraordinary methods needed to retrieve and produce the information *must* be borne by the requesting party. Cost-shifting in this instance is mandatory.

In 2003, Mississippi enacted a rule that is virtually identical to the Texas rule, but does not require mandatory cost shifting. See Miss. R. Civ. P. 26(b)(5).

Adoption of the Federal Rules of Civil Procedure

Arizona, Idaho, Indiana, Minnesota, Montana, New Jersey and Utah have all recently enacted sweeping changes that are modeled on the new Federal Rules, although only Utah has adopted an early "meet and confer" requirement. Arizona does not require an early conference amongst the parties, but does require disclosure of a list relevant ESI 40 days after a responsive pleading is filed. As part of its new rules, Idaho has adopted the approach taken by Texas

and Mississippi, although mandatory cost shifting is not required.

Limited eDiscovery Rules Enacted

On January 10, 2008, the Supreme Court of Arkansas approved a new civil rule and a new evidence rule that provide limited protection against inadvertent disclosure of privileged information. See Ark. R. Evid. 502; Ark. R. Civ. P. 26(b)(5). The civil rule amendment is similar to Federal Rule of Civil Procedure 26(b)(5) and allows a producing party to "take back" inadvertently produced privileged information. The new rule of evidence is modeled on Proposed Federal Rule of Evidence 502, and protects from waiver attorney-client communications and attorney work product that has been inadvertently disclosed. The amendments are effective immediately.

In June 2007, Louisiana adopted limited new rules that are modeled on the Federal Rules. The Louisiana Code now sets forth protections against the waiver of inadvertently disclosed information, allows for the withholding from production ESI that is not reasonably accessible, and requires parties to specify the form of production. See LA Code of Civ. P. Art. 1424, 1425, 1460, 1461, 1462.

In March 2007, New Hampshire enacted a statewide civil rule mandating that the parties meet and confer shortly after the lawsuit is filed to discuss, among other things, the scope of electronic discovery, the extent to which ESI is reasonably accessible, the likely costs of obtaining access to such information and who shall bear said costs, format of production, preservation of ESI, and protections against the waiver of attorney-client privilege contained in ESI. See N.H. Superior Ct. R. 62.

In 2006, New York adopted a new rule for the Commercial Division of the trial courts. The new rule requires counsel in commercial disputes to consult about ESI prior to a mandatory preliminary conference, including but not limited to: (i) implementation of a data preservation plan; (ii) identification of relevant data; (iii) the scope, extent and form of production; (iv) anticipated cost of data recovery and proposed initial allocation of such cost; (v) disclosure of the programs and manner in which the data is maintained; (vi) identification of computer system(s) utilized; (vii) identification of the individual(s) responsible for data preservation; (viii) confidentiality and privilege issues; and (ix) designation of experts. See 22 N.Y.C.R.R. 202.70(g), Rule 8.

North Carolina has also adopted electronic discovery rules in its specialty business courts. See General Rules of Practice and Procedure for the N.C. Business Court 17.1(i); 17.1(r); 17.1(s); 17.1(t); 17.1(u); 18.6(b); Form 2. The Business Court Rules require that counsel meet and confer very early in the litigation to discuss the scope of ESI that may be involved in the case, preservation of information, potential cost-shifting for discovery of ESI that is not reasonably accessible, format of production, discovery of metadata, and security measures required to protect ESI that is produced in the discovery process.

Rule Changes Contemplated

As noted above, other states around the country have either proposed amendments, or are contemplating changes. For instance, on January 14, 2008, Alaska released proposed changes to its Civil Rules

(Continued on page 28)

ESI and the Discovery Rules (Continued)

(Continued from page 25)

eDiscovery “meet and confer” with opposing counsel. Ideally, any issues regarding form of production can be agreed upon prior to the initial conference with the court to deter later discovery disputes regarding metadata. The rules and judicial decisions to date also contemplate continuing communications between client and counsel regarding retention and continuing implementation of the litigation hold.

The Federal Rules of Evidence

The Advisory Committee on the Federal Rules of Evidence has approved for publication proposed Rule of Evidence 502 for publication. The proposed Rule would codify waiver of privilege and work product protections by allowing exceptions to waiver by inadvertent disclosure of ESI. Both the Advisory Committee’s Report and proposed Rule 502 are available online at <http://www.uscourts.gov/rules/Reports/EV05-2006.pdf>.

The proposal of Rule 502 shows the Advisory Committee’s concerns about the ever-increasing cost of privilege and work product review of ESI. The draft rule provides that the disclosure of privileged documents will not result in a waiver, provided the producing party took reasonable precautions to prevent disclosure, and once the party learned of the disclosure, took reasonably prompt measures to rectify the error. Proposed Rule 502 also allows waiver to be avoided by making party agreements regarding inadvertent disclosure binding on the parties to the agreement.

There are some concerns as to whether such agreements between the litigators are binding on third parties, but that concern could probably be alleviated and the agreement be made binding on third parties if incor-


porated into a subsequent court order. Rule 502 would allay the risks currently facing parties conducting privilege reviews, and would be another positive step toward bringing the legal world up to speed with the business world.

Expert Help

There is a growing satellite industry of expert consultants available to assist with ESI evaluation and production. A forensic computer expert is likely required to fully extract all available metadata, and would certainly be helpful to the practitioner in evaluating metadata prior to disclosure. It may well be beyond the abilities both functional and capacity of both the litigator and her staff to sort through hundreds of thousands or more files in their native format to determine relevance and privilege, and again, the consultant’s time and expertise may well be worth the expense.

Conclusion

Although eDiscovery is in its infancy, a body of law is rapidly developing, which requires the federal practitioner (and the state-court practitioner, as well, in those states which have adopted ESI discovery rules) to be familiar with both the concept of eDiscovery and ESI production, and the client’s systems, practices and procedures. Read the amendments to the Federal Rules of Civil Procedure. Read the decisions, including the *Zubulake* opinions. Talk to your clients, and become familiar with their technology platforms and protocols. The trend stems to be developing among the courts to place at least part of the burden of ensuring client compliance with litigation holds and discovery orders on the attorney, and the sanctions and penalties for a failure to do so can be extremely expensive. It behooves the wise practitioner to become familiar with at least the

basics of e-discovery and, as with other specialty areas, to know when to bring in outside expert assistance. And watch the developing case law as the courts hand down their opinions on this topic in order to be able to more accurately predict the scope and outcome of future eDiscovery battles. Talk to your own consultants regarding metadata in documents sent from your system, and make sure that you have adequately addressed any potential concerns in that regard. And join your state bar’s technology committee (or befriend someone who is already a member), and learn more about this rapidly-developing area of the law. 

H. Hunter Twiford, III is a member and the managing partner of McGlinchey Stafford’s Jackson, Mississippi office, where he also heads up the firm’s Mississippi Commercial Litigation section.

John T. Rouse is an associate in the Commercial Litigation section of McGlinchey Stafford.



eDiscovery in State Courts (Continued)

(Continued from page 26)

that would bring the state rules in line with the Federal Rules. Public comments are due by February 29, 2008.

After rejecting changes in 2006, California recently released proposed amendments to its Civil Discovery Act and Court Rules. The proposed rules are modeled on the *Uniform Rules Related to the Discovery of Electronically Stored Information*. They also seek to incorporate two case management rules that would encourage parties to identify and discuss electronic discovery issues early in the litigation and to encourage courts to address the issues in case management orders.

Ohio released proposed amendments and accepted public comment up to November 14, 2007. The proposed changes are mostly based on the Federal Rules amendments, but provide a list of factors courts should consider in determining sanctions when a party has destroyed potentially relevant electronically stored information, including:

- (1) Whether and when any obligation to preserve the information was triggered;
- (2) Whether the information was lost as a result of the routine alteration or deletion of information that attends the ordinary use of the system in issue;
- (3) Whether the party intervened in a timely fashion to prevent the loss of information;
- (4) Any steps taken to comply with any court order or party agreement requiring preservation of specific information;

(5) Any other facts relevant to its determination under this division.

Ohio R. Civ. P. 37(f) (Proposed). If approved, the changes will become effective on June 1, 2008.

Maryland's Standing Committee on Rules of Practice and Procedure submitted proposed amendments to the Maryland Court of Appeals on September 26, 2007. The proposed amendments are modeled on the Federal Rules and also draw from the



Sedona Conference, *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production*, the Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information, and the Maryland Business and Technology Case Management Program, Electronic Data Discovery Guidelines.

In March 2007, Iowa released for public comment a series of potential amendments that are based on the new Federal Rules. The deadline for

comment was May 1, 2007.

The public comment period for Nebraska's proposed limited changes closed on August 31, 2007. Nebraska has proposed adopting the phrase "electronically stored information" and some other terminology revisions to its rules related to interrogatories, requests for production, and subpoenas. Also included in the proposed amendments are provisions dealing with format of production of ESI that mirror the Federal Rules.

The District of Columbia is reportedly in the process of revising its local rules to adopt the amendments to the Federal Rules of Civil Procedure. A subcommittee of the Washington State Bar Association is currently circulating to stakeholders proposed amendments to that state's civil rules. Florida, Kansas, New Mexico, South Carolina, and Virginia are all currently contemplating the adoption of rules relating specifically to electronic discovery. Several other states, such as Missouri, Oregon, and Vermont, are in the very early stages of exploring whether they need or want to amend their civil rules.

No Changes Contemplated, or Changes Rejected

Several states, like Delaware and Nevada, are taking no action at all to adopt eDiscovery rules, preferring to "wait and see" how the Federal Rules

(Continued on page 29)




eDiscovery in State Courts (Continued)

(Continued from page 28)

amendments and other states' rules are received.

Rationale for Adoption of State Rules

Electronic discovery is now a fact of life for litigators and courts. The proliferation of computer usage, inexpensive data storage, and developments in communication technology have changed modern discovery practice tremendously over the past several years. Courts around the country have been promulgating *ad hoc* case law, rules, and procedures to deal with electronic discovery which pro-

vide little guidance or assistance to litigants. The Federal Rules amendments, along with the *Uniform Rules Related to the Discovery of Electronically Stored Information* and the *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* provide a strong backbone upon which states can build a comprehensive, uniform set of rules to address electronic discovery in their courts. 

Gregory D. Shelton is Of Counsel in the Seattle office of Williams Kastner. He is a frequent author and speaker on eDiscovery and products liability issues.

On the Internet...

Enacted/Proposed State eDiscovery Rules

Arizona Enacted Rules:

159.87.239.100/rules/ramd_pdf/r-06-0034.pdf

Arkansas Proposed Rules:

www.lexisnexis.com/applieddiscovery/lawLibrary/ArkansasPrivilege.pdf

Indiana Enacted Rules:

www.in.gov/judiciary/orders/rule-amendments/2007/trial-091007.pdf

Iowa Proposed Rules:

www.judicial.state.ia.us/wfdata/frame5416-1022/File11.pdf

Ohio Proposed Rules:

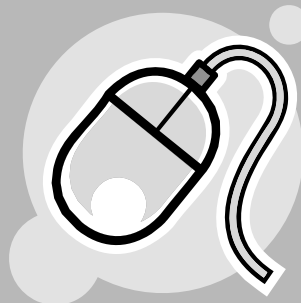
www.sconet.state.oh.us/Rules/amendments/practiceProcedureOct07.pdf

Maryland Proposed Rules:

www.courts.state.md.us/rules/reports/158thReport.pdf

Nebraska Proposed Rules:

www.supremecourt.ne.gov/rules/proposedarchive/DiscoveryRulesCivilCases.pdf



Wading Deep (Continued)

(Continued from page 23)

hold” – at what point does a party have the obligation to preserve electronic records above and beyond their normal retention policy (if any)? *In re Napster, Inc. Copyright Litigation*, 462 F.Supp.2d 1060 (N.D. Cal. 2006), provides a detailed autopsy of the timeline of when a party would be obligated to preserve, and a dire warning: an individual or corporation may be obligated to preserve documents not only when litigation is pending, or when it is imminent, but even when there are indirect threats that do not materialize for years.

Napster, as all may well be aware, was an incredibly popular and controversial file sharing web site, known mostly for the sharing of music files. It was the subject of several ultimately effective lawsuits for copyright infringement. *Napster* concerns a lawsuit by a record company, UMG Recordings, against Hummer Winblad Venture Partners (Hummer), a venture capital investor in Napster.

Hummer made an investment in Napster after it was already in litigation, in May 2000, and signed a “Common Interest and Defense Agreement” at that time. Two days later, a Hummer employee sent what later became the “smoking gun” e-mail, instructing Hummer employees to, among other things, continue the company policy of deleting e-mails.

Soon thereafter, in a scene that might be straight from a movie, Universal Music Corp. CEO Edgar Bronfman told John Hummer of Hummer Winblad in a meeting that he would sue investors in Napster if the copyright infringement continued. Hummer was sued by different parties the next month, and that case was eventually dismissed. The instant suit was filed three years later.

The key question considered by the court in *Napster* was at what point

(Continued on page 31)

Wading Deep (Continued)

(Continued from page 29)

Hummer should have been on notice to preserve electronic records for litigation. To make that determination, the court went through a detailed analysis of what Hummer knew when, at what stage various pieces of litigation were at various times, and what effect that knowledge should have had. As with the *Taser* case discussed above, the Court went deeper into factual issues that it likely would have been comfortable in a discovery dispute.

The Plaintiffs in *Napster* were seeking sanctions against Hummer of, in increasing severity: (1) exclusion of testimony; (2) adverse inference and (3) dismissal. The court came down extremely hard upon Hummer, particularly for a long delay in producing the “smoking gun” e-mail.

The court found that Hummer had the duty to preserve evidence from the date of the Bronfman threat, which continued throughout the next several years, regardless of whether litigation was actually pending against it or not at any given time. The court found that “even if Hummer’s ‘long standing policies’ included deleting emails, Hummer was required to cease deleting e-mails once the duty to preserve attached ...”. *Napster* at 1070. Thus, the duty to preserve began when the CEO was threatened with litigation at a meeting, and continued thereafter.

Ultimately, the court found that Hummer ordered its employees to delete Napster related e-mails through its order to delete all e-mails. Such action constituted at least gross negligence by Hummer, according to the court, even if it was not willful. The court ruled that it would not enter a dismissal, but would order some level of evidence preclusion and adverse inference instructions, the exact nature of which would be determined at the summary judgment or trial stage. *Id.* at 1079. Given the results

of this case, it would be very prudent to consider preserving all electronic records if even the hint of litigation is in the air.

The Mother of All eDiscovery Opinions

For a lengthy (51 pages in double columns) and detailed précis on eDiscovery, you cannot beat *Lorraine v. Markel American Ins. Co.*, 241 F.R.D.

“For a lengthy (51 pages in double columns) and detailed précis on eDiscovery, you cannot beat Lorraine v. Markel American . . .”


534 (2007)(*Markel* for ease of reference). While some judges treat discovery disputes with hesitation, here the judge jumped in with both feet. In *Markel*, the Chief Magistrate of the U.S. District Court, District of Maryland, considers a case where e-mails are the key to determining the intent of the parties in a dispute over an arbitration agreement.

The parties agreed to arbitrate the dispute over the cause of damage in a lightning strike on a boat; the arbitrator returned an award including damages midway between what was claimed and zero; and the plaintiff contested the arbitration award as being beyond the scope of the arbitrators’ authority, claiming it should have only concerned a question of law and did not include the authority to alter the amount of the claim.

The judge in *Markel* performs a detailed analysis of the admissibility of electronic evidence. Generally, the examination includes whether the electronic evidence is: (1) relevant under Federal Rule of Evidence 401; (2) authentic under FRE 901(a); (3) hearsay under FRE 801 or an exception under FRE 803, 804 or 807; (4) is an original or duplicate, or admissible secondary evidence to prove its contents; and (5) would it cause unfair prejudice under FRE 403? *Markel* at 538.

The opinion goes through a rule by rule analysis of each rule that may apply to each of these factors, discussing how they apply to different types of electronic evidence, including e-mail, internet website postings, text messages and chat room postings, computer stored records and data, computer animation and computer simulations, and digital photographs. If you are looking for an overview of the admissibility of electronic evidence or need the application of specific rules to your situation, *Markel* is the place to start.

Conclusion

There is no question that the momentum of issues regarding electronic discovery has only quickened with the enactment of the new Federal Rules. New opinions appear to be coming out almost daily. It is a complicated and increasingly important area of the law that is causing more, not less, involvement by judges in the intricacies of discovery disputes. While judges and attorneys may wish otherwise, that involvement will only increase. 

Alfred A. (“Al”) Malena, Jr. is a litigator and partner with Thompson, Slagle & Hannan, LLC in suburban Atlanta, Georgia.



The Section of Litigation, the largest specialty section of the American Bar Association, is dedicated to helping litigators become more effective advocates for their clients. The Section is a legal publisher, a provider of CLE programming, a source of news and analysis, and a strong national voice in discussions concerning the profession. Simply put, the Section helps lawyers be better lawyers.

Mission

Who more than litigators have the responsibility to secure the vitality of the American system of justice and equal justice for all?

The mission of the Section of Litigation is to dedicate its efforts to accomplishing these critical objectives while, at the same time, providing our members the resources and opportunities to help them be effective, competent and ethical advocates on behalf of their clients and in the eyes of the public.

*Visit the Technology for
the Litigator
Committee's Web Site!*

*[http://
www.abanet.org/
litigation/committees/
technology/home.html](http://www.abanet.org/litigation/committees/technology/home.html)*

