ELECTRONIC DISCOVERY AND TECHNOLOGY-DERIVED EVIDENCE

Presented by:
Technology in the Practice and Workplace Committee

Moderator:

Cynthia N. Sass
Law Offices of Cynthia N. Sass, P.A.
Tampa, Florida

Speakers:

Conor R. Crowley
Law Offices of Conor R. Crowley
McLean, Virginia

Michael J. Gray
Jones Day
Chicago, Illinois

Material Preparation:

James W. Jones
Law Offices of Cynthia N. Sass, P.A.
Tampa, Florida

ABA Section of Labor and Employment Law
Technology in the Practice and Workplace Committee
MidYear Meeting

April 2010
New York, New York

ELECTRONIC DISCOVERY AND TECHNOLOGY-DERIVED EVIDENCE[1]

I. Federal Rules of Civil Procedure and Electronic Discovery

The Federal Rules of Civil Procedure were amended effective December 1, 2006 to focus on the rapidly emerging prevalence of discovery of electronically stored information ("ESI").

A. Rule 26(b)(2)(B) – Discovery Scope and Limits provides: A party need not provide discovery of ESI from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitation of Rule 26 (b)(2)(C). The court may specify conditions for the discovery.

B. Rule 34(E) – Producing the Documents or ESI provides: Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or ESI:

1. A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

2. If a request does not specify a form for producing ESI, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and

3. A party need not produce the same ESI in more than one form.

C. Rule 37(e) – Failure to Provide ESI provides: Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide ESI lost as result of the routine, good faith operation of an electronic information system.

D. Rule 45(d)(1)(A)-(D) – Duties in Responding to a Subpoena Producing Documents or ESI provides:

1. **Documents**: A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

2. **Form for Producing ESI Not Specified**: If a subpoena does not specify a form for producing ESI, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

[1] The materials included in this paper are distributed by the Law Offices of Cynthia N. Sass, P.A., as a service to clients and other interested individuals. The outlines contained herein are provided for informal use only. This material should not be considered legal advice and should not be used as such.

3. **ESI Produced in Only One Form:** The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

4. **Inaccessible ESI**: The person responding need not provide discovery of ESI from sources that the person identifies as not reasonably accessible because of undue burden or cost.

II. Cost-Shifting Cases – Who Pays for the Electronic Discovery?

Given the great expense that electronic discovery can represent, inevitably the question arises of which party should bear the burden of the cost.

A. The *Zubulake* Cases – Seven-Factor Cost-Shifting Test

The lead case on this issue arose out of a series of cases in the United States District Court for the Southern District of New York between Laura Zubulake and UBS Warburg LLC ("UBS"). Zubulake sued UBS for gender discrimination and retaliation and contended that the key evidence in her case was located in various e-mail exchanges between UBS employees that could only be found on backup tapes and archived media. Zubulake requested that UBS produce the archived e-mails. UBS claimed that obtaining and restoring the archived e-mails would cost approximately $175,000 without even counting attorney time. Zubulake moved to compel UBS to produce the archived e-mails at its expense.

In the first case in the series, *Zubulake v. USB Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003), the Court provided guidelines that courts should use when deciding whether cost-shifting is appropriate in cases with extensive electronic discovery. First, the court held that in deciding cost-shifting disputes with electronic discovery, if the data is kept in an accessible format, the usual rules of discovery apply and the responding party should pay the costs of producing responsive data. The court further held that cost-shifting should only be considered when electronic data is relatively inaccessible (i.e., it only exists on backup tapes). Second, since cost-shifting analysis is very fact-intensive, the court reasoned it would be necessary to determine what data may exist on inaccessible media. In most cases it would be reasonable to require a responding party to restore and produce responsive documents from a small sample of archiving medium such as backup tapes in order to show that the sought-after information actually exists. Third, when conducting cost-shifting analysis, the court held that the following factors should be considered and weighted in the following order:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;

3. The total cost of production compared to the amount in controversy;
4. The total cost of production compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

Ultimately the court ordered UBS to produce at its own expense (1) all responsive e-mails from its active servers, and (2) responsive e-mails from a number of backup tapes selected by Zubulake. The court further ordered that UBS should then prepare an affidavit detailing the results and cost of its search and submit it to the court, which would then conduct a cost-shifting analysis based on the factors set forth above.

B. Advisory Committee Notes to Fed. R. Civ. P. 26 (b)(2)(B)

As part of the 2006 amendments to the Federal Rules of Civil Procedure regarding the costs of electronic discovery, the Advisory Committee notes created the following seven-factor test which bears a striking resemblance to the seven-factor test set forth in *Zubulake*:

1. the specificity of the discovery request;
2. the quantity of information available from other and more easily accessed sources;
3. the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
4. the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
5. predictions as to the importance and usefulness of further information;
6. the importance of the issues at stake in litigation; and
7. the parties' resources.

C. Cases Utilizing *Zubulake* and/or Advisory Committee Factors

Semsroth v. City of Wichita, 239 F.R.D. 630 (D. Kan. 2006). Female police officers brought sexual harassment and gender discrimination claims against the City of Wichita, the police department, and the police chief. The officers sought the production of e-mails from backup tapes. Since the city only maintained its backup tapes for disaster recovery purposes, the e-mails on the backup tapes were not easily accessible. The city moved to have part or all of the cost of retrieving any e-mails from the backup tapes charged to the officers. Following the *Zubulake* factors, the court denied the city's motion. The court found that the city's backup tapes were reasonable for disaster recovery and the city would not automatically be required to bear the costs of retrieving the e-mails from the tapes. However, the cost of restoring and searching the single backup tape in question (less than $4,000) was not so much of a financial burden that shifting all or part of the cost to the officers was held to be appropriate. Interestingly, with respect to the sixth *Zubulake* factor (importance of the issues at stake), the court noted that employment discrimination cases are probably not the type of cases that would warrant special consideration with respect to cost-shifting.

Major Tours, Inc. v. Colorel, 2009 WL 3446761 (D. N.J. 2009). Plaintiffs, African-American owned bus companies, claimed that Defendants, the New Jersey Department of Transportation and several individual NJDOT officials, engaged in discriminatory racial profiling by subjecting Plaintiffs' buses to safety inspections en route to Atlantic City, New Jersey. Defendants sought a protective order from Plaintiffs' request for copies of e-mails from backup tapes or archived e-mails maintained by the New Jersey Department of Transportation. Citing *Zubulake*, the court found the requested e-mails were generally considered inaccessible. The cost of reviewing the backup tapes Plaintiffs were requesting were likely to exceed $100,000 independent of any time for attorneys to review them for relevancy and any possible privilege objections. After reviewing both the Advisory Committee and the *Zubulake* factors, the court found that the issue being litigated (whether the NJDOT was engaging in racial profiling) was of paramount public importance, but that the cost of obtaining the requested e-mails from the backup tapes would not be justified since many of tapes would most likely contain evidence that was simply duplicative of other available evidence. Therefore, the court ordered that with respect to backup tapes that were redundant of materials already produced, Plaintiffs would bear the cost of the retrieval and attorney relevancy and privilege review. However, with respect to non-redundant backup tapes, Plaintiffs and Defendants were ordered to split the retrieval costs, but Defendants would bear their own attorney relevancy and privilege review costs.

III. Discoverable Electronic Information

A. Hard Drives and Data Storage Devices

1. Cases Allowing Parties to Make Mirror Images of Computer Hard Drives

Courts may enter discovery orders requiring "the mirror image" of hard drives of any computers that contain documents responsive to an opposing party's request for production of documents. *See Theilen v. Buogiorno USA, Inc.*, 2007 U.S. Dist. Lexis 8998 (W. D. Mich. 2007); *Balboa Threadworks, Inc. v. Stucky*, 2006 U.S. Dist. Lexis 29265 (D. Kan. 2006); *Capital Records, Inc. v. Alaujan*, 2009 U.S. Dist. Lexis 110626 (D. Mass. 2009).

A "mirror image" is a "forensic duplicate, which replicates bit for sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." *See Communications Center, Inc. v. Hewitt*, 2005 WL 3277983 (E.D. Cal. 2005).

Generally, these court orders will set forth a procedure that parties have to follow to obtain the mirror image:

(i) The requesting party will select a computer forensics expert who will create the mirror image;

(ii) The computer expert will execute a confidentiality agreement negotiated by the parties and abide by any protective order put in place by the court;

(iii) The parties will negotiate and agree upon a search protocol that the expert will use to find the relevant documents and information on the mirror image;

(iv) The computer will be made available to the computer forensics expert who will create the mirror image and then inspect the image pursuant to the parties' agreed-upon search protocol; and

(v) The computer expert will then release a report to the parties' counsel regarding the findings of its inspection. The party opposing the production will have a certain amount of time in which to lodge any objections to the expert's report. If the parties cannot resolve their disputes over the report, then the requesting party may file a motion to compel. If there is no dispute, then the expert will release its report and copies of the sought after ESI to the requesting party. *See Bank of Mongolia v. M & P Global Financial Servs., Inc.*, 258 F.R.D. 514 (S.D. Fla. 2009); *Ameriwood Indus. Inc. v. Liberman*, 2006 U.S. Dist. Lexis 93380 (E.D. Mo. 2006); *American Family Mut. Ins. Co. v. Gustafson*, 2009 U.S. Dist Lexis 22685 (D. Colo. 2009); *Frees, Inc. v. McMillan*, 2007 U.S. Dist. Lexis 4343 (W.D. La. 2007); *Cenveo Corporation v. Slater*, 2007 U.S. Dist. Lexis 8281 (E.D. Pa. 2007).

2. Cases Denying Parties' Request to Make Mirror Images of/or Inspect Computer Hard Drives

If a discovery request is too broad and the connection between the ESI and the claims in the lawsuit are vague and unsubstantiated, courts will deny a request for the creation of a mirror images or other inspection of computer hard drives.

McCurdy Group v. Am Biomedical Group, Inc., 9 Fed Appx. 822 (10th Cir. 2001). The mere fact that plaintiff questions whether defendant produced copies of all relevant and non-privileged documents does not warrant compelling production of defendant's computer disc drives where defendant (1) claimed to have produced hard copies of all relevant and non-privileged information, (2) agreed to produce the requested disc drives to a third party for inspection, and (3) asserted attorney-client and trade-secret privileges.

Balfour Beatty Rail, Inc. v. Vaccarello, 2007 U.S. Dist. Lexis 3581, (M.D. Fla. 2007). Court denied motion to seek copies of hard drives where requesting party failed to provide any information regarding what it sought to discover from hard drives and made no contention that defendants had failed to provide requested information contained on hard drives.

Williams v. Mass. Mutual Life Ins. Co., 226 F.R.D. 144 (D. Mass. 2005). Court denied employee's motion to compel discovery and appoint a neutral computer forensics expert in employment discrimination claim. Employee claimed he had possessed a hard copy of an e-mail message describing company's discrimination policy from company officer. Employee was unable to find hard copy and wanted a court-appointed computer forensics expert to search employer's hard drives and electronic communication system for e-mail. Court denied the motion, finding that the missing e-mail was nothing more than a memorandum that employer had already produced. However, court did order employer to preserve all documents, hard drives, and e-mail boxes that had been searched by company's computer expert in response to employee's motion.

At least one court has denied a requesting party's motion to allow its computer forensics expert to make a copy of hard drives where the defending party was willing to have its own computer forensics expert conduct the search.

See Calyon v. Mizuho Securities USA Inc., 2007 U.S. Dist. Lexis 36961 (S.D.N.Y. 2007). Calyon claimed that its former employees had conspired with new employer to transmit its confidential business information to the new employer. There was evidence the former employees had forwarded Calyon's trade secrets to their personal e-mail accounts while working for their new employer. Calyon filed a motion to compel the former employees to allow Calyon's computer expert to make mirror images of the employees' personal home computer hard drives. The former employees objected to allowing Calyon's expert conduct the search of their personal home computer hard drives because other family members used these computers as well and their privacy could be violated. The former employees offered to have their own computer expert conduct the search of the hard drives. The court denied Calyon's motion because it: 1) could not provide any specific reason why the employees' expert could not conduct a thorough search of the hard drives and 2) had not argued that the employees had failed to produce any responsive documents (electronic or otherwise) that had been requested. Moreover, the employees' expert was willing to work cooperatively with Calyon's expert and counsel to refine the search and find all relevant and responsive ESI.

3. Cases Compelling Forensic Imaging

Courts may compel the forensic imaging of hard drives (i.e., making a mirror image) where there are issues as to whether a party has adequately responded to discovery requests. In determining whether to compel forensic imaging, courts will consider whether or not (1) the responding party has withheld requested information, (2) the responding party is unable or unwilling to search for the requested information, and (3) the responding party has complied with previous discovery requests. *See Henderson v. U.S. Bank, N.A.* 2009 WL 1152019 (E.D. Wis. 2009); *Bianco v. GMAC Mtg. Corp*., 2008 WL 4661241 (E.D. Pa. 2008); *Williams v. Mass Mut. Life Ins. Co.*, 226 F.R.D. 144 (D. Mass. 2005).

If the requesting party can demonstrate either that (1) there are discrepancies in response to a discovery request or (2) the responding party has failed to produce requested information, a court will be more likely to order forensic imaging. *See White v. Graceland College Ctr. for Professional Dev. & Lifelong Learning, Inc*., 2009 WL 722056 (D. Kan. 2009); *Diepenhorts v. City of Battle Creek*, 2006 WL 1851243 (W.D. Mich. 2006); *In re Weekly Homes, L.P*., 52 Tex. Sup. Ct. J. 1231 (2009).

B. Courts May Order Servers Be Forensically Searched

Covad Communications Company v. Revonet, Inc., 258 F.R.D. 5 (D. D.C. 2009). Covad brought an action against Revonet, a customer-lead generation service, claiming that Revonet had improperly shared Covad's proprietary customer lead information with its competitors. The court found that Revonet's database servers were evidence and Covad was entitled to a forensic search of them despite Revonet's objection that the servers were old and a forensic search may damage

them. The court further held that Revonet was obligated to take reasonable steps to recover information destroyed due to a crash of its e-mail exchange server.

C. Access to Social Network Sites

1. Cases Allowing Discovery of Information from Social Networking Websites Where it is Relevant to the Claim in Dispute

Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D. Colo. 2009). Ledbetter and Powell were injured while performing electrical work in a Wal-Mart store for their employer and sued Wal-Mart. Ledbetter and Powell claimed to suffer ongoing and permanent physical and psychological injuries. Powell's wife also brought a loss of consortium claim. Wal-Mart subpoenaed FaceBook, MySpace and Meetup social networking websites for information regarding Ledbetter's and Powell's health and Powell's relationship with his wife. While Ledbetter and Powell objected to the subpoenas based on physician-patient and marital privileges, the court allowed the subpoenas to be enforced because their claims for physical and psychological injuries and loss of consortium made the issues the subpoenas were aimed at finding relevant.

Bass v. Miss Porter's School, 2009 WL 3724968 (D. Conn. 2009). School sought text messages from student's Facebook account regarding her alleged teasing and taunting of other students. Parties reached a stipulated agreement whereby Facebook would release "reasonably available data" from student's Facebook profile. Student provided a full copy of the "Facebook documents" (which consisted of 750 pages of wall postings, messages and pictures) to the court but only a subset to the school, claiming the documents she withheld were irrelevant. In reviewing the Facebook documents, the court could find no meaningful distinction between the documents the student had elected to release to the school and those she withheld. As such, the court issued an order stating the school could pick up the remaining Facebook documents from the court.

2. Employers Finding Helpful Evidence on Employees' Social Networking Webpages

Nguyen v. Starbucks Coffee Corp., 2009 WL 4730899 (N.D. Cal. 2009). Nguyen had made complaints to Starbucks that she was experiencing "negativity" from her co-workers because she was Asian, was experiencing "mental pain" and could not return to work. Starbucks placed Nguyen on leave while it investigated her complaints. Before going on leave, Nguyen had informed her Starbucks co-workers of her MySpace page. One of Nguyen's co-workers showed management the page which contained comments about her use of illegal drugs and her thoughts of going berserk and shooting everyone. Based on Nguyen's MySpace comments, Starbucks terminated her for threatening violence to the company and its employees. Nguyen brought claims of sexual harassment, retaliation, and religious discrimination against Starbucks following her termination. Starbucks prevailed on its motion for summary judgment due in part to threatening and inappropriate comments Nguyen made on her MySpace page.

Snyder v. Millersville University, 2008 WL 5093140 (E.D. Pa. 2008) Snyder was a student-teacher enrolled in a public university teacher program and brought a First Amendment claim against Millersville University. Snyder claimed the university violated her free speech rights for failing to certify her as a teacher due to information found on her MySpace page. The university warned its student-teachers not to contact students or teachers on their personal social network web pages and even described an incident in which the university had terminated a student-teacher for doing so. Despite this warning Snyder informed her students of her MySpace page, posted a picture of herself drinking while wearing a pirate hat, and made statements on her MySpace page encouraging students to contact her and criticizing her supervisor. The district court dismissed Snyder's complaint finding that Snyder's Myspace page communications concerned private matters, not matters of public concern.

3. Employees Finding Helpful Evidence against Employers on Social Networking Websites

Williams v. Wells Fargo Financial Acceptance, 564 F.Supp.2d 441 (E.D. Pa. 2008). Williams (African-American) filed a Title VII action against his former employer, Wells Fargo, alleging race discrimination and was able to survive Wells Fargo's summary judgment motion due in part to evidence he discovered on MySpace. Wells Fargo terminated Williams for violating its information security and sexual harassment policies when he sent e-mails containing sexually suggestive jokes and picture attachments. Williams claimed that Wells Fargo enforced these policies in a discriminatory manner by not terminating white employees who sent inappropriate e-mails. Williams was able to survive summary judgment by showing that Wells Fargo had failed to terminate a white employee who e-mailed inappropriate pictures and several personal MySpace e-mails.

4. Limit To Discovery of Employee's Social Networking Webpage

Mackelprang v. Fidelity National Title Agency of Nevada, Inc., 2007 WL 119149 (D. Nev. 2007). Mackelprang brought claims of sexual harassment, negligent infliction of emotional distress, battery, and assault against her former employer, Fidelity based on being sexually harassed and forced to have sex with her supervisors. Mackelprang was so distraught over the harassment, she attempted suicide while at work and then again a few months after she left Fidelity. Fidelity discovered that Mackelprang had two different MySpace accounts: one describing her as married with children and the other describing her as a single woman who does not want children. Fidelity subpoenaed MySpace to seek communications between Mackelprang and others. Fidelity theorized the two different MySpace accounts would tend to show that her sexual relations with her supervisors were consensual. The court denied Fidelity's request to compel production of sexually explicit MySpace emails between Mackelprang and others because Mackelprang had opened the accounts after she had left Fidelity. Thus, even if the accounts showed Mackelprang was engaging in extra-marital affairs, the evidence would not be related to her workplace. The court, however, held that Fidelity could serve limited requests for production for Mackelprang's MySpace pages regarding her emotional distress since she alleged in her complaint that her second suicide attempt (made after she left her employment) was still related to the harassment she suffered at Fidelity.

D. Metadata (Data about Data)

1. Definition of Metadata

"Metadata" is commonly described as data about data and has been defined as "information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location storage requirements and medial information)." *See The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information in the Electronic Age Appendix F*.

A good discussion of the nature of metadata is contained in *Aguilar v. Immigration & Customs, Enforcement Div. of the United States Dept. of Homeland Sec*., 255 F.R.D. 350 (S.D.N.Y. 2008). There are three different types of metadata: (1) substantive metadata, (2) system metadata, and (3)imbedded metadata. *Aguilar* described the three types of metadata as follows:

Substantive Metadata: "Substantive metadata, also known as application metadata is created as a function of the application software used to create the document or file and reflects the substantive changes made by the user." *Sedona Principals 2d Cmt 12a; D Protoeclol 26*. This category of metadata reflects modifications to the document, such as prior edits or editorial comments, and includes data that instructs the computer how to display the fonts and spacing in a document. *Sedona Principals 2d Cmt.12 a.* Substantive metadata is embedded in the document. *Id.* at 354.

System Metadata: "System metadata reflects information created by the user or by the organization's information management system. *Sedona Principles 2d Cmt 12 a.* This data may not be embedded within the file it describes, but usually can be easily retrieved from whatever operating system is in use. Examples of system metadata include data concerning 'the author, date and time of creation, and the date a document was modified.'" *Id*.

Embedded Metadata: "Embedded metadata consists of "text, numbers, content, data or other information that is directly or indirectly inputted into a [n]ative [f]ile by a user and which is not typically visible to the user viewing the output display. Examples include spreadsheet formulas, hidden columns, externally or internally linked files (such as sound files), hyperlinks, references and fields, and database information. This type of metadata is often crucial to understanding an electronic document. For instance, a complicated spreadsheet may be difficult to comprehend without the ability to view the formulas underlying the output of each cell." *Id*. at 355-356.

2. Courts Have Generally Been Uneasy about Compelling the Production of Metadata

Courts have found that most System and Substantive Metadata lack evidentiary value because it not relevant and will not compel its production unless the requesting party articulate a reason why it should be produced. *See Shirley Williams, et al. v. Sprint/United Management Co.*, 230 F.R.D. 640, 651 (D. Kan. 2005) ("Emerging standards of electronic discovery appear to

articulate a general presumption against the production of metadata"), *see also Mich. First Credit Union v. Cumis Ins. Soc'y*, 2007 WL 4098213 at *2 (E.D. Mich. 2007); *Ky. Speedway LLC v. Nat'l Assoc. of Stock Car Auto Racing*, 2006 WL 5097354 at *8 (E.D. Ky. 2006).

Wyeth v. Impax Laboratories, Inc., 248 F.R.D. 169 (D. Del. 2006) Impax sought a motion to compel Wyeth to produce electronic documents in their native format, complete with metadata and not in a Tagged Image File Format (TIFF) in which they were produced. TIFF formats will not provide metadata. The Court stated that if "the requesting party can demonstrate a particularized need for the native format of an electronic document, a court may order it produced. Therefore the producing party must preserve the integrity of the electronic documents it produces. Failure to do so will not support a contention that production of documents in native format is overly burdensome." *Id* at 170. However, since Impax never demonstrated a particularized need for the metadata, the district court denied its motion.

3. Request for Production of Metadata

Courts have denied motions to compel the production of metadata where the underlying discovery request failed to request that documents be produced in any particular format.

Ponca Tribe of Indians v. Continental Carbon Co., 2006 WL 2927878 (W.D. Okla. 2006). ("The original document requests issued by Plaintiffs failed to specify the manner in which electronic or computer information should be produced. [Defendant] elected to use a commonly accepted means of complying with the request. Nothing in the material supports requiring [Defendant] to reproduce the information in a different format. Accordingly, Plaintiffs' request for reproduction of documents in their native electronic format will be denied.").

Ice Corporation v. Hamilton Sunstrand Corporation, 2007 WL 4239453 (D. Kan. 2007). The court denied Plaintiff's motion to compel production of electric versions of all documents already produced in discovery, including metadata, where Plaintiff's discovery requests had never originally sought documents in electronic form. Court refused to compel production of something that Plaintiff's original requests for production had never sought given that the time to file a motion to compel under local rules had long since expired and discovery was about to close.

D'Onofrio v. SFX Sports Group, Inc., 247 F.R.D. 43 (D. D.C. 2008). Court denied motion to compel production of electronic version of business plan documents with metadata where original request failed to request documents in their native format.

Conversely, where the requesting party's original request specified that documents should be produced in their native format, courts have compelled the production of the documents in their native format with accompanying metadata.

Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (requiring production in native format where requesting party asked for it and producing party failed to object).

However, at least one court has stated that parties seeking the production of metadata should focus their requests to specific documents rather than making sweeping requests for metadata.

See Dahl v. Bain Capital Partners, LLC, 2009 U.S. Dist. LEXIS 52551 (D. Mass. 2009). In Dahl, the district court, cited the *Wyeth* and *Williams* decisions as proof of the trend of courts noting their reservations about the utility of metadata. The court noted the Fed. R. Civ. P. Advisory Committee statement that requests for production should be tailored, and stated that "[r]ather than a sweeping request for metadata, the Shareholders should tailor their requests to specific word documents, specific emails or specific sets of mail…"

4. Production of Metadata May Be Compelled Where Requesting Party Can Show Relevance

Sanchez et al., v. Bland Farms, LLC, 2009 WL 2365976 (S.D. Ga. 2009). Plaintiffs were migrant farm workers suing Defendant for unpaid wages. Plaintiffs requested electronic data files for payroll records from 2004 to 2007 in their native format to allow Plaintiffs to review embedded metadata which contained the mathematical formulas used to prepare their pay. Defendants cited *Ky. Speedway LLC, v. Nat'l Assoc. of Stock Car Auto Racing*, 2006 WL 5097354 at *8 (E.D. Ky. 2006) and *Wyeth v. Impax Laboratories, Inc*., 248 F.R.D. 169, 170 (D. Del. 2006) for the proposition that there was a general court trend emerging against production of metadata absent a particularized showing of need. While the district court acknowledge that general trend against metadata production may be emerging, Plaintiffs had shown a particularized need for metadata to determine how their pay was calculated and ordered the production of the data files in their native format so the metadata could be examined.

Hagenbuch v. 3 B6 Sistemi Eletroncici Industiali, S.R.L., 2006 WL 665005 at *3 (N.D. Ill. 2006). Court compelled production of ESI where the system metadata on the ESI was relevant as it would allow the requesting party in patent infringement case to piece together chronology of events including who had received what information and when.

5. Metadata in Public Records

There are few cases concerning requests for public records containing metadata. Thus far, the case law consists of state court cases holding that metadata meets the definition of a public record under the state's respective public records law and should be produced pursuant to a records request.

Lake v. City of Phoenix, 218 P.3d 1004 (Az. 2009). In *Lake*, the Arizona Supreme Court held if a public entity maintains a public record in an electronic format, the electronic version of that record, including any metadata, may be sought through a public records request. David Lake was a Phoenix police officer who filed an administrative complaint and a federal lawsuit alleging employment discrimination by the City of Phoenix. Lake submitted a public records request for copies of his supervisor's notes. After reviewing the notes, Lake suspected his supervisor had backdated a number of the documents which had been created on a computer. Lake then made another public records request for the metadata regarding the file containing his supervisor's

notes which included "the true creation date, access date, the access dates for each time the file was accessed, including who accessed the file as well as print dates."

The trial court and court of appeals supported the City of Phoenix's denial of producing the metadata to Lake on the grounds that "metadata" was not included in the common law definition of public records. The Arizona Supreme Court overturned the appeals court decision with the following rationale:

> The metadata in an electronic document is part of the underlying document; it does not stand on its own. When a public officer uses a computer to make a public record, the metadata forms part of the documents as much as the words on the page. (citations omitted). Arizona's public records law requires that the requestor be allowed to review a copy of the 'real record.' (citations omitted). It would be illogical, and contrary to the policy of openness underlying the public records laws, to conclude that public entities can withhold information embedded in an electronic document, such as the date of creation, while they would be required to produce the same information if it were written manually on a paper public record.

Id. at 1007-1008.

O'Neill v. City of Shoreline, 187 P.3d 822 (Wash. App. 2008). In *O'Neil,* the Washington Court of Appeals held that metadata describing an e-mail's history, tracking and management associated with e-mail from private citizen to deputy mayor alleging improper influence by city council members over zoning was public record. At a public meeting of the Shoreline City Council, the deputy mayor claimed she received an e-mail stating serious allegations of improper influence by members of the city council over a zoning matter from a Mrs. O'Neill. O'Neill was at the public meeting and made an oral request to the deputy mayor to see the e-mail.

After O'Neill's request, the deputy mayor deleted the top four lines of the header on the e-mail when she forwarded it from her personal computer to herself. The deputy mayor had received the e-mail on her personal e-mail account that she sometimes used for official city business. Sometime after that, the deputy mayor deleted the email from her personal computer. O'Neill made repeated oral and written requests to see the e-mail and all information regarding how the deputy mayor had received it, including metadata, following the public hearing. However, the city failed to provide O'Neill with the entire original e-mail or its associated metadata. Not satisfied with the city's responses, O'Neill brought an action against the city under the Washington Public Records Act ("PRA") claiming the city violated the PRA by altering and destroying the e-mail.

The court found that the electronic version of the e-mail met the definition of a public record under the PRA because it was (1) a writing, that (2) related to the conduct of the government, and (3) had been used in the public meeting when the deputy mayor mentioned the e-mail as her source for information regarding the alleged improper conduct of city council members. The court further held that the metadata associated with the e-mail was also a public record because: (1) the metadata fell within the PRA's broad definition of a "writing" and (2) the metadata

contained information that "related to" to the conduct of government. Specifically, the metadata showed the e-mail addresses of persons who may have had knowledge about the alleged improper conduct of city council members on a zoning matter.

IV. Admissibility of E-Discovery

Like any other evidence, ESI must be subjected to the rules of evidence to determine its admissibility. Thus far, the leading case in analyzing the admissibility of ESI is *Lorraine v. Markel Am. Ins. Co*., 241 F.R.D. 534 (D. Md. 2007) in which the court stated:

> Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a serious of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant… (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be), (2) if relevant …, is it authentic… (can the proponent show that the ESI is what it purports to be), (3) if the ESI is offered for its substantive truth, is it hearsay…, and if so, is it covered by an applicable exception, (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, of [sic] if not, is there admissible secondary evidence to provide the content of the ESI, and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice…, such that it should be excluded despite its relevance.

Id. at 538 (citations omitted).

V. Sanctions for Spoliation of Electronic Evidence

A. Employers Responsible for Actions of Their Employees Who Destroy Electronic Evidence

Nucor Corp. v. Bell, 251 F.R.D. 191 (D.S.C. 2008). Nucor sued its former employee, John Bell, and his new employer, SeverCorr, for misappropriation of its trade secrets. The court found that Bell engaged in spoliation of evidence by intentionally destroying and altering evidence stored on a USB thumb-drive and a SeverCorr laptop computer. Bell had used the thumb-drive while working at Nucor, and there was evidence he had connected the thumb-drive to his SeverCorr laptop, thereby making it possible that he transferred data from Nucor to SevereCorr. The court found that SeverCorr could be sanctioned for Bell's continued use of his SeverCorr work laptop since his continued use resulted in the destruction of evidence while Bell was under an obligation to preserve data on its hard drive. In contrast, SeverCorr could not be sanctioned for Bell's destruction of the thumb-drive. The fact that Bell had never informed SeverCorr of the thumb-drive's existence and never discussed discarding the thumb-drive with SeverCorr indicates he was not acting within the scope of his employment with SeverCorr when he threw out the thumb-drive in anticipation of litigation. Bell, however, could be individually sanctioned for destroying

the thumb-drive. The court allowed a jury instruction that the jury could infer the evidence destroyed would have been helpful to Nucor as a sanction.

Connor v. Sun Trust Bank, 546 F.Supp.2d 1360 (N.D. Ga. 2008). Connor sued Sun Trust for taking away a number of her job duties while she was on adoption leave under the Family Medical Leave Act. Connor moved for sanctions against Sun Trust for destruction of evidence, namely an e-mail that set forth the reasons for her termination. The court found Sun Trust could be sanctioned for Connor's supervisor's destruction of the e-mail with a jury instruction instructing the jury to draw a negative inference from the absence of the e-mail.

B. Standards for Finding Spoliation Sanctions – Negligence vs. Bad Faith

1. Negligence

In what may become the leading case regarding the standards of conduct justifying sanctions for spoliation of electronic evidence, the United States District Court for the Southern District of New York set forth a lengthy discussion of what constitutes "gross negligence" where a party fails in its duty to preserve electronic evidence in *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, LLC, 2010 WL 184312 (S.D.N.Y. 2010).

The case concerned an action brought by investors against an investment hedge fund administrator to recover losses from the liquidation of hedge funds in which they owned shares. The administrator made a motion for sanctions against the investors for their failure to preserve various electronic documents. The court held that the investors had a duty to preserve electronic records relating to off-shore accounts because the investors filed a complaint with the British Virgin Islands Financial Services Commission.

For the investors who were "grossly negligent" in their failure to preserve electronic evidence, the appropriate sanction was a jury instruction allowing the jury to presume that the relevance of the missing documents would prejudice the administrator. *Id*. at *12. For the investors who were merely "negligent" in their failure to preserve electronic evidence, the appropriate sanction was a jury instruction permitting the jury to presume the relevance of missing documents. These investors would have the opportunity to try to rebut the presumption. *Id*.

The court held that a party's "gross negligence" in failing to preserve electronic evidence could be supported by a finding that once a duty to preserve evidence had been established, the party failed to: 1) issue a written litigation hold, 2) identify all of the key players and ensure that their electronic and paper records are preserved, 3) cease the deletion of email or to preserve the records of former employees in a party's possession, custody, or control, or 4) preserve backup tapes when they are the sole source of relevant information when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources. *Id*. at *7.

The court also offered further guidance regarding a party's duty to preserve backup tapes. Specifically, the court noted that it was "not requiring that all backup tapes be preserved. Rather,

if such tapes are the sole source of relevant information (e.g., the active files of key players are no longer available), then such backup tapes should be segregated and preserved. When accessible data satisfies the requirement to search for and produce relevant information, there is no need to save or search backup tapes." *Id*. at *12 n. 99.

2. Bad Faith

However, not all courts will be inclined to follow the negligence standard set forth in *Pension Committee*. In *Rimkus Consulting Group, Inc. v. Nickie Cammarata*, 2010 WL 645253, (S.D. Tex. 2010), the United States District Court for the Southern District of Texas addressed whether a negligence or bad faith standard should apply when deciding if sanctions should be levied against a group of former employees who destroyed evidence before suing their former employer to challenge the validity of their non-compete agreements. The court acknowledged the *Pension Committee* decision and its application of a negligence standard but declined to follow it. *Id*. at *7. Instead, the court elected to adhere to a Fifth Circuit precedent requiring a showing of "bad faith" before a court can apply severe sanctions such as adverse jury instructions, striking pleadings or default judgment. *Id*. at *6. The *Rimkus* court found the former employees acted in "bad faith" because (1) they manually and selectively deleted e-mails after they knew they were about to sue their former employer and (2) they failed to disclose their personal e-mail accounts in discovery which were later discovered to contain e-mails showing they had intentionally taken information from their former employer. *Id*. at *30-32. The court decided this "bad faith" warranted an adverse jury instruction as a sanction, but not the more serious sanctions of striking a pleading or entering a default judgment. *Id*. at *32.

See also Swofford v. Eslinger, 2009 U.S. Dist. Lexis 111064 (M.D. Fla. 2009). Swofford was shot on his own property by deputies with the county sheriff's department which was attempting to apprehend a car thief. Swofford moved for sanctions against the county and the individual deputies for spoliation of evidence. The sheriff's department acted in "bad faith" when it failed to take steps to prevent deputies from deleting email messages from their computers after the sheriff's department had received Swofford's counsel's written requests for preservation of evidence. A deputy turned in the laptop computer he had used at time of incident with knowledge that its hard drive would be purged pursuant to the sheriff's department's computer recycling policy. In light of these "bad faith" acts of spoliation, the court awarded a sanction that the jury could be instructed that the e-mails and laptop computer contained evidence that would be detrimental against the sheriff's department and the deputies.

3. Split between the Circuits on Whether "Bad Faith" or "Negligence" is the Proper Standard

The *Rimkus* decision discusses the split amongst the federal appeals court circuits as to whether "negligence" or "bad faith" is the proper standard for courts to use when deciding whether spoliation sanctions should apply. The *Rimkus* court noted the *Pension Committee* decision was based on Second Circuit case law applying a negligence standard to spoliation cases. *Rimkus* at *7. In contrast, the *Rimkus* court noted that the Seventh, Eighth,, Tenth and Eleventh and D.C. circuits require "bad faith" before providing a serious spoliation sanction such as an adverse jury instruction. *Rimkus* at *7 fn 11. *See Faas v. Sears, Roebuck, & Co*, 532 F.3d

633, 644 (7th Cir. 2008) (requiring finding that Sears intentionally destroyed documents in bad faith before drawing an inference that the documents contained information detrimental to Sears); *Greyhound Lines v. Wade*, 485 F.3d 1032, 1035 (8th Cir. 2007) (a spoliation-of-evidence sanction requires a finding of intentional destruction indicating a desire to suppress the truth); *Turner v. Pub. Serv. Co. of Colo.*, 563 F.3d 1136, 1149 (10th Cir. 2009) (mere negligence in losing or destroying records is not enough because it does not support an inference of consciousness of a weak case); *Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1294 (11th Cir. 2003) ("adverse inference is drawn from a party's failure to preserve evidence only when the absence of that evidence is predicated on bad faith"); *Wyler v. Korean Air Lines Co.*, 928 F.2d 1167, 1174 (D.C. Cir. 1991) ("Mere innuendo…does not justify drawing the adverse inference requested.")

The *Rimkus* court noted that the First, Fourth, and Ninth Circuits hold that "bad faith" is not essential to imposing severe sanctions if the spoliation causes severe prejudice to a party's ability to prove its case, but the cases often note the presence of bad faith *Rimkus* at *7 fn. 12. *See Sacramona v. Bridgestone/Firestone, Inc*., 106 F.3d 444, 447 (1st Cir. 1997) (bad faith may be considered but is not essential for sanction regarding spoliation; if evidence is mishandled through carelessness and other side is prejudiced, sanctions may be imposed); *Silvestri v. Gen. Motors Corp.*, 271 F. 3d 583, 593 (4th Cir. 2001) (holding dismissal is "usually justified only in circumstances of bad faith, but even when conduct is less culpable, dismissal may be necessary if prejudice to defendant is extraordinary, denying it the ability to adequately defend its case); *Glover v. BIC Corp*., 6 F. 3d 1318, 1329 (9th Cir. 1993) ("Short of excluding the disputed evidence, a trial court also has the broad discretionary power to permit a jury to draw an adverse inference from the destruction or spoliation against the party or witness responsible for the behavior.")

Rimkus noted that Third Circuit courts balance the degree of fault with the prejudice before applying spoliation sanctions. *Rimkus* at 7 fn. 13 *See Mosaid Techs. Inc., v. Samsung Elecs, Co*., 348 F.Supp.2d 332, 335 (D. N.J. 2004) (three key considerations dictate if sanctions are warranted: (1) degree of fault of the party who altered or destroyed evidence, (2) degree of prejudice suffered by opposing party, and (3) whether there is a lesser sanction that will avoid unfairness to opposing party and serve to deter such conduct by others in the future) (citing *Schmid v. Milwaukee Elec. Tool Corp*., 13 F.3d 76, 79 (3rd Cir. 1994)

VI. Emerging Issues in E-Discovery

A. Public Employees Right to Privacy Regarding Personal Text Messages Sent on Employer-Provided Texting Devices – Pending Supreme Court Case of *City of Ontario v. Jeff Quon*

The Supreme Court is currently reviewing the issue what privacy rights public employees may have with respect to personal text messages they send on employer-provided texting devices. The case, *City of Ontario v. Jeff Quon*, arose out of the Ninth Circuit. The facts, holdings of the Ninth Circuit, and the issues that are before the Supreme Court are set forth below.

Facts: City of Ontario, California, contracted with Arch Wireless to provide wireless text messaging services with each pager having an allotment of 25,000 characters per month, after which the city would be required to pay overage charges. While the city had no policy regarding text messaging, it did have an internet and e-mail policy stating that access and use of e-mail were not confidential and use of inappropriate or derogatory language in e-mail was not allowed. Jeff Quon worked in the city's police department and signed an acknowledgement form regarding the city's e-mail and internet policy before he was issued the two-way pager with text message capabilities. Lieutenant Steve Duke was responsible for procuring the payments from individual police officers for their monthly text overage charges. Although Lt. Duke informed Quon and others that the city's e-mail/internet policy applied to text messages, Lt. Duke also told Quon and other officers that if they paid for their overages, the police department would not read their text messages.

However, after several months of collecting fees from Quon and other police officers for their text overages, the police department requested Arch Wireless to provide it with transcripts of the text messages for the police officers who had exceeded their monthly limit. The police department's goal in reviewing the transcripts was to determine if it needed to negotiate a higher monthly character allotment to account for its employees' official business. The transcripts Arch Wireless provided covered the time period that Lt. Duke had told Quon and others that the police department would not read their text messages if they paid their overage fees. The transcripts revealed that Quon had exceeded the monthly character allotment by over 15,000 characters and many of his texts were personal and sexually explicit. Based on the transcripts, the police department's internal affairs investigated Quon to see if he was wasting time instead of performing his duties during working hours.

Quon and the individuals to whom he was sending text messages filed a court complaint alleging violations of their privacy rights under 4th Amendment, the California state constitution, and federal Stored Communications Act ("SCA"). The case eventually made its way to the United States Court of Appeals for the Ninth Circuit.

1. Ninth Circuit Holdings – *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008)

The Ninth Circuit held that the city's search of Quon and the people to whom he had sent text messages violated their 4th Amendment and California constitutional privacy rights. The Ninth Circuit reasoned that Quon and those he messaged had a reasonable expectation of privacy in the content of the text messages. Furthermore, the city's search was unreasonable in scope due to the fact that Lt. Duke had made it to clear to Quon and other officers that if they paid their monthly overage charges, the police department would not read their texts. The Ninth Circuit supported its holding that the scope of the city's search was unreasonable by finding that the city could have used less intrusive methods such as (1) warning Quon that he could no longer use the pager for personal use and all texts would be subject to review by the police department, (2) providing the text transcripts to Quon and having him count the characters himself, or (3) have him redact the transcript and grant the police department permission to review the redacted transcript.

The Ninth Circuit further held that Arch Wireless's act of turning over the text transcripts to the city violated the Stored Communications Act ("SCA"). Under the SCA, Arch Wireless was considered an "electronic communication service" ("ECS"). As an ECS, Arch Wireless could only release private information (i.e., the transcripts of the texts) of the "addressee or intended recipient of the text communications" to Quon or those to whom he sent text messages. However, as an ECS, Arch Wireless could not release the transcripts to a "subscriber" such as the city without the consent of Quon or those to whom he sent text messages.

2. Issues Before the Supreme Court in *City of Ontario v. Jeff Quon*

a. Whether a police officer has a reasonable expectation of privacy in text messages transmitted on his city-issued pager, where the police department has an official no-privacy policy but a non-policymaking lieutenant announced an informal policy of allowing some personal pager use.

b. Whether individuals who sent text messages from their city-issued pager had a reasonable expectation that their text messages would not be reviewed by their government employer.

c. Whether the Ninth Circuit contravened Supreme Court 4th Amendment precedents and created a split amongst the federal appeals courts by analyzing whether the city's police department could have used a less intrusive method of reviewing the text messages Quon transmitted on his city-issued pager.

B. Employees' Right to Privacy on Employer's Computer Systems

1. Cases Holding Employees Have No Privacy Right on Employer-Provided Computers

Generally, employees will not have a right to privacy regarding files and e-mails on their employer's workplace computers and computer systems where the employer promulgates and enforces a policy telling the employee no such right to privacy exists. *See Muick v. Genayre*, 280 F.3d 741, 743 (7th Cir. 2002); *Thygeson v. Bancorp*, 2004 WL 2066746 (D. Or. 2004); *Kelleher v. City of Reading*, 2002 WL 1067442 (E.D. Pa. 2002).

2. Cases Supporting Employee's Right to Privacy Regarding Attorney-Client Privileged Communication

However, there is emerging case law holding that an employee may still have an expectation of privacy regarding attorney-client privileged communications even if they are made on an employer-provided computer or computer system and the employer has a monitoring policy.

Stengart v. Loving Care Agency Inc., 973 A.2d 390 (N.J. App. Ct. 2009). The New Jersey Superior Court, Appellate Division, held that 1) emails exchanged between an employee and her attorney on employer's company-issued laptop computer through the former employee's personal, web-based email account were protected by the attorney-client privilege, 2) employee's breach of company's

policy regarding use of its computer did not justify company's claim of ownership of employee's e-mail communications to her attorney, 3) it was improper for company's attorney to read e-mails between former employee and her attorney without giving employee opportunity to argue the e-mails were privileged, and 4) the case was remanded for a hearing regarding whether the company's law firm should be disqualified from the case. The court further ordered the company to turn over all e-mails between the former employee and her attorney in its or its attorney's possession to the former employee. In rejecting the employer's argument that its electronic communications policy allowed it to review the employee's e-mails, the court stated

> [a]lthough plaintiff's emails to her attorney related to her anticipated lawsuit with the company, the company had no greater interest in those communications that it would if it had engaged in the highly impermissible conduct of electronically eavesdropping on a conversation between plaintiff and her attorney while she was on a lunch break.

Id. at 400.

The New Jersey Supreme Court recently upheld the Superior Court's decision reasoning that the employee took reasonable steps to keep her e-mails to her attorney confidential by using her personal, web-based e-mail account that was protected by a password she never shared with her employer. *See Stengart v. Loving Care Agency, Inc*., 2010 WL 1189458 at *12 (N.J. 2010).

In *U.S. v. Hatfield*, 2009 WL 3806300 (E.D.N.Y. 2009), the United States District Court for the Eastern District of New York upheld an employee's attorney-client privilege with respect to attorney-created documents stored on his company-issued computer hard drive by using the following five-factor test: (1) Did the employer maintain a computer policy banning personal or other objectionable use, (2) Did the employer monitor the use of the employee's computer or e-mail, (3) Did the employer or third parties have a right to access to the employee's computer or e-mails, (4) Did the employer notify the employee or was the employee aware of the employer's policies regarding computer use and monitoring, and (5) How did the employer interpret its computer usage policy. With respect to each factor, the court found that: (1) the employer's policy did not expressly prohibit employees from using company computers to conduct personal legal matters, (2) the company policy stated it had a right to monitor its employee's e-mails and company computer, but there was no evidence the employer actually did any monitoring, (3) the employer did have a right to access e-mails and its employee's computers, (4) the employee was aware of the employer's policy, and (5) the employer interpreted its own policy to mean that its employees did not waive the attorney-client privilege by maintaining legal documents on their company computers.

Curto v. Medical World, 2006 WL 1318387 (E.D.N.Y. 2006). The court found employer with e-mail monitoring policy went too far when it accessed e-mails an employee had sent to her attorney while working at home via her company-issued laptop computer. Employee had reasonable expectation of privacy where she sent e-mail using a personal web-based e-mail account which did not go through employer's server. *But compare Kaufman v. SunGard Inv. System*, 2006 WL 1307882 (D. N.J. 2006) (holding that employee waived attorney-client privilege by sending e-mails to her attorney on company e-mail system where company policy

clearly notified all e-mails on company system were subject to monitoring, searching, or interception at any time); *Alamar Ranch, LLC. v. County of Boise*, 2009 WL 3669741 (D. Idaho 2009) (citing *Stengart* in finding employee waived attorney-client privilege regarding e-mails sent to attorney because unlike employee in *Stengart*, employee simply used her employer-provided work e-mail instead of web-based password-protected e-mail account); *Convertino v. U.S. Dept. of Justice*, 2009 WL 4716034 (D. D.C. 2009) (upholding attorney-client privilege for e-mails employee sent to his attorney from work computer at the Department of Justice which the Department of Justice later obtained from its e-mail server where the Department of Justice (1) did not have a policy banning personal use of company e-mail, (2) never notified employee it would regularly access and retain e-mails from his account, and (3) employee had attempted to keep e-mails private by deleting them unaware they still existed on e-mail servers).

C. Cloud Computing

Cloud computing is the use of internet services to provide data processing and data storage that would otherwise occur on a user's computer or a company's internal computer network. The "cloud" is the internet.

There are no cases dealing with electronic discovery issues and cloud computing. Currently, the term "cloud computing" is only mentioned in a few cases. *International Business Machines Corp v. Johnson*, 2009 WL 2356430 (S.D.N.Y. 2009) concerned the enforcement of a preliminary injunction to stop a former IBM vice president from working with a new employer, Dell, on any cloud computer projects. *Rearden LLC v. Rearden Commerce, Inc*., 597 F.Supp.2d 1006 (N.D. Cal. 2009) mentioned the term cloud computing in the context of a trademark infringement dispute. The concept of "cloud storage" was mentioned in *Applied Filter Technology, Inc. v. Wetzel*, 2009 WL 2424802 (W.D. Wash. 2009), another case regarding an employer seeking to enforce a preliminary injunction against a former employee. In *Wetzel*, the employer in part sought to prevent its former employee from accessing its electronic information maintained in "cloud storage." In *State v. Bellar*, 217 P.3d 1094 (Or. App. Ct. 2009), a criminal case involving a suspect's possession of child pornography on his personal computer's hard drive, the dissenting opinion made the following statement regarding the concept of an individual's right to privacy with respect to information stored in the cloud:

> Nor are a person's privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another person. Again, in a practical sense, our social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the "cloud" on servers owned by internet service providers. That information can be generated and accessed by hand-carried personal computing devices. I suspect most citizens would regard that data as no less confidential or private because it was stored on a server owned by someone else.

Id. at 1110-1111.

Cloud Discovery Issues

Despite the current lack of cases, one can envision some of the upcoming discovery issues that will arise regarding cloud computing. Since an entity using a cloud service to process or store data will not actually have its data on its premises, entities using a cloud service will need to ensure that the service understands and has procedures to handle electronic discovery in the event of litigation. Some of the key issues that entities utilizing cloud services should review are:

1. Does the service have any routine policies calling for the elimination of documents after a certain period of time? If so, does the service have the ability to put a "litigation hold" on its routine document disposal policies in the event it receives notice of actual or anticipated litigation?

2. Which party, the cloud service or the client using the service, will cover what may be the substantial costs regarding electronic discovery requests?

3. How does the cloud service respond to subpoenas? How quickly will it inform the client- company of its receipt of subpoenas?

4. What does the cloud service agreement say about who owns the data? Is it the cloud service or the client using the service? This may be important if there is a question pursuant to Rule 26 of the Federal Rules of Civil Procedure who has possession, custody, or control of data subject to a discovery request.

In light of the fleshed-out standard of what constitutes "gross negligence" in electronic spoliation cases set forth in the *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, LLC, 2010 WL 184312 (S.D.N.Y. 2010) (See above), one can imagine a "gross negligence" case of spoliation being made against a party utilizing a cloud service that fails to use or enforce litigation holds to preserve relevant and requested information.

VII. Additional Resources for Standards and Practices Regarding Electronic Discovery

A. The Sedona Conference Cooperation Proclamation

The Sedona Conference is a legal think tank dedicated to the advanced study of law and policy. The Sedona Conference has issued guidance on electronic discovery that courts have used to inform its decisions on the topic. You can obtain a copy of *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information in the Electronic Age* at http://www.sedonaconference.com/content/miscFiles/TSG9_05.pdf.

B. The Seventh Circuit Electronic Discovery Pilot Program

The Seventh Circuit has initiated a pilot program to develop principles for effectively handling electronic discovery. The pilot program is currently in Phase I which started on October 1, 2009 and will expire on May 1, 2010. In Phase I, judges who volunteer will

implement a proposed Standing Order in select cases that incorporates the Principles of the Seventh Circuit's Electronic Discovery Committee ("Principles"). These cases will later be evaluated through questionnaires to participating judges and lawyers. The pilot program focuses on having parties cooperate to resolve their common electronic discovery issues.

The Principles set forth in the proposed Standing Order include:

1. The requirement that counsel designate an e-discovery liaison to work towards resolving disputes;

2. The requirement that opposing counsel confer with one another before seeking information regarding preservation and collection efforts to determine if the information is necessary and if there are alternative means to obtain it;

3. The requirement that parties discuss the potential of conducting discovery in states as a method of reducing costs;

4. The requirement that the parties discuss at the Rule 26(f) conference or as soon thereafter as possible methodologies for identifying ESI for production; and

5. At the Rule 26(f) conference, the encouragement that the parties make a good faith effort to agree on the production format(s) of ESI (whether it be the native format or some other reasonably usable form).

Data from Phase I will be used to made adjustments to the Principles and the Standing Order. Those changes may then be tested as a modified proposed standing order is tested during Phase II, which is currently planned to run from June 2010 to May 2011. You can find more details on the Seventh Circuit Electronic Discovery Pilot program at http://www.7thcircuitbar.org/associations/1507/files/Statement1.pdf.

C. Guidelines for State Trial Courts Regarding Discovery of Electronic Information

State court judges will often refer to the Guidelines for State Trial Courts Regarding Discovery of Electronic Information from the Conferences of Chief Justices (the "Guidelines"). The Guidelines provide instructions for state trial courts on a variety of electronic discovery issues such as 1) the scope of electronic discovery, 2) reallocation of discovery costs, 3) form of production, 4) preservation orders, and 5) sanctions.

The Guidelines are at http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf.