

Annual ADFSL Conference on Digital Forensics, Security and Law

2012 Proceedings

May 31st, 1:45 PM

After Five Years of E-Discovery Missteps: Sanctions or Safe Harbor?

Milton Luoma

Metropolitan State University, St. Paul, Minnesota, milt.luoma@metrostate.edu

Vicki Luoma

Minnesota State University, Mankato, Minnesota, vicki.luoma@mnsu.edu

Follow this and additional works at: https://commons.erau.edu/adfsl

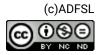
Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

Scholarly Commons Citation

Luoma, Milton and Luoma, Vicki, "After Five Years of E-Discovery Missteps: Sanctions or Safe Harbor?" (2012). *Annual ADFSL Conference on Digital Forensics, Security and Law.* 5. https://commons.erau.edu/adfsl/2012/thursday/5

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.





AFTER FIVE YEARS OF E-DISCOVERY MISSTEPS: SANCTIONS OR SAFE HARBOR?

Milton Luoma

Metropolitan State University 700 East Seventh Street St. Paul, Minnesota 55106 651.793.1481 651.793.1246 (fax) Milt.Luoma@metrostate.edu

Vicki Luoma

Minnesota State University 145 Morris Hall Mankato, Minnesota 56001 507.389.1916 507.389.5497(fax) Vicki,Luoma@mnsu.edu

ABSTRACT

In 2003 the Zubulake case became the catalyst of change in the world of e-discovery. In that case Judge Shira Scheindlin of the United States District Court for the Southern District of New York set guidelines for e-discovery that served as the basis for amending the Federal Rules of Civil Procedure (FRCP) in December 2006. The amendments incorporated a number of concepts that were described by Judge Scheindlin in the Zubulake case. (Zubulake v. UBS Warburg LLC, 2003) Since the Zubulake case and the FRCP amendments, numerous cases have interpreted these rules changes, but one of the main points of court decisions is that of preservation of electronically stored information (ESI). A litigation hold to preserve ESI must be put into place as soon as litigation is reasonably anticipated. The failure to preserve ESI has resulted in the largest number of cases where judges have imposed sanctions, but certainly not the only one. This paper reviews the cases to answer the question – are the courts granting safe harbor protection when litigants failed to follow the rules and best practices rather than imposing sanctions?

Keywords: e-discovery, electronic discovery, sanctions, safe harbor, electronically stored information, ESI, sanctions

1. ELECTRONICALLY STORED INFORMATION AND THE PROBLEM

The biggest problem in complying with discovery requests is the enormous amount of electronically stored information that exists. According to a study conducted at Berkeley in 2003, more than five exabytes of information were stored electronically. Five exabytes of information would be the same as 37,000 libraries the size of the Library of Congress. (Lyman, 2003) They further predicted that based on past growth rates, the amount of ESI doubles every three years. (Lyman, 2003) To put this information in visual terms, one exabyte of information is equal to 500,000,000,000 (500 trillion) typewritten pages of paper. (Luoma M. V., 2011) Beyond the sheer volume of data, other problems include how to determine which of the information is relevant to the litigation at hand, how to retrieve it, in what format it must be provided to the opposing party, and most importantly, to ensure none of the relevant or potentially relevant data has been deleted or lost.

Yet another problem with electronically stored information is that it contains metadata. If the metadata

is not provided in response to a discovery request, court sanctions are a real possibility. Metadata is data about data. So when discovery requests demand data it normally includes the metadata. Litigants must ensure that the metadata is intact and not altered. Metadata will not only provide information concerning the creator, recipient, creation dates and times, but also whether there have been any alterations or deletions and the identity of the person making these changes. It can also provide a timeline. Further, it also includes how and when the alternations were made.

Three types of metadata are of interest, namely, file metadata, system metadata, and embedded metadata. File data includes information about the creator, reviser, editor and data and times. File system metadata is important because if data has been altered this metadata will show that information. Also this is one area in which spoliation occurs. If the collection of data is not done properly, then metadata can be altered or deleted. System metadata is normally recovered from an organization's IT system and will include the path a file took and where it is located on a hard drive or server. The metadata is often in databases in the computer system. Embedded metadata contains the data, content, numbers that are not found in the native format of a document. One example of embedded data would be the formulas used in a spreadsheet. Metadata can also demonstrate an evidence timeline.

In a 2005 case, Williams v. Sprint, the court set the standard concerning metadata when it ruled as follows:

When a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order. (Williams v. Sprint/United Mgmt. Co., 2005)

Metadata is an important element in discovery. The metadata can be used as a search tool to help find relevant documents and it can be used to discover attempts at hiding or deleting information or revealing who knew what when. For example, in the Martha Stewart case in which she was found guilty of four counts of obstruction of justice and lying to investigators about a stock sale, it was the metadata that showed she had made alterations to her electronic calendar, (Securities and Exchange Commission vrs Martha Stewart and Peter Bacanovic, 2003) and in the Qualcomm case metadata helped to locate emails that Qualcomm had denied receiving. (Luoma M. &., 2009) The pure volume of information and the layers of information available to a litigant make discovery a difficult dilemma. When does a party have enough information?

2. PRIOR TO THE CIVIL RULE CHANGES

The former version of the FRCP required litigants to comply with discovery requests in an effort to prevent surprises at trial and to ensure a fair trial. Although some courts interpreted the rules to include electronic data as well as paper data, there were no well-established guidelines in this matter. The case that was the catalyst for change in electronic discovery was the Zubulake case. The Zubulake case began as a gender discrimination case, but became the first authoritative case in the United States on electronic discovery issues. (Zubulake v. UBS Warburg LLC, 2003)

The Zubulake case forced the legal community to review the rules of civil procedure and make the necessary changes to the Federal Rules of Civil Procedure to include specific instructions concerning electronically stored information. In 1999 Laura Zubulake was hired as the director and senior salesperson of the UBS Asian Equities Sales Desk and was told that she would be considered for her supervisor's position when he left. When Laura's supervisor took another position, another male was given that position without consideration of any other candidates, including Laura Zubulake. Her new supervisor made it clear that he did not feel a woman belonged in Laura's position and earning \$650,000 a year. Laura Zubulake complained that her new supervisor made sexist remarks, excluded

her from office activities and demeaned her in the presence of her co-workers. In response to this treatment Laura Zubulake filed a gender discrimination claim with the EEOC against her employer UBS Warburg LLC. She lost the case and was fired. She then brought suit against her employer under federal law, New York state law, and New York City law for both gender discrimination and retaliation. (Zubulake v. UBS Warburg LLC, 2003)

This case was atypical in that there were five pre-trial motions dealing with discovery issues. When Warburg could not produce the desired emails and other electronic documents requested, Zubulake brought a motion requesting access to UBS backup media. UBS responded by asking the court to shift the cost of restoring the backup tapes to the plaintiff. What followed were four more motions to resolve discovery issues. During the restoration effort it was determined that many backup tapes were missing and some were erased. The court ordered a sampling to be done of the backup tapes. In these results it was evident that Zubulake's supervisor had taken steps to conceal or destroy particularly relevant emails. As a result of this action, the court set standards for retention and deletion requirements, litigation holds and cost shifting. It became clear after the Zubulake case that the old rules of civil procedure were no longer adequate. Clarification had to be made concerning electronic discovery. The guidelines forged by the judge in the Zubulake case were debated in setting new rules with trial adoption of the rule changes in December 2006 and permanent adoption one year later. (Zubulake v. UBS Warburg LLC, 2003)

3. NEW FEDERAL RULES

In April of 2006 the U.S. Supreme Court determined the amount of electronically stored information involved in discovery requests required clarification and standards. Changes in the Federal Rules of Civil Procedure that dealt with ESI issues that took effect in December 1, 2006 included Rules 16, 26, 34 and 37. Rule 26 provided that parties must provide an inventory, description and location of relevant ESI and required the parties to meet and develop a discovery plan. Rule 34 sets out rules for document requests and Rule 37 addresses the safe harbor provisions.

Rule 26 (A) (1)(ii) requires the litigants to provide the following:

(ii) a copy — or a description by category and location — of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment; (Federal Rules of Civil Procedure, 2006)

This revision now requires a party to reveal all of its information without requiring the opposing party to ask for the information. This provision requires attorneys who have always been adversaries to cooperate. In addition, Rule 26(f) requires that the parties must confer as soon as practicable or at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b). (Federal Rules of Civil Procedure, 2006)

4. SANCTIONS

Since the Zubulake case it has been clear that parties must put a litigation hold in place as soon as litigation is known and anticipated. That one issue has been the primary reason for courts imposing sanctions on a party. However, there are other reasons for sanctions that have arisen since the Federal Rules of Civil Procedure were modified. Those reasons have included data dumping, data wiping, intentional destruction and certainly failure to have a litigation hold.

4.1 Data Dumping

If an opposing party provides too much information it may be guilty of data dumping while demanding too much information can result in cost shifting and a litigation nightmare. Failure to retain electronic data in a retrievable format for litigation that a litigant knew or should have known might be imminent can result in sanctions.

In a 2008 case, ReedHycalog v. United Diamond, a Texas court found that in discovery the producing party must cull out irrelevant information from document production and must not engage in data dumping. (ReedHycalog v. United Diamond, 2008) The court ruled that "there are two ways to lose a case in the Eastern District of Texas: on the merits or by discovery abuse." (ReedHycalog v. United Diamond, 2008) The court stated, "While these provisions generally ensure that parties do not withhold relevant information, a party may not frustrate the spirit of discovery rules — open, forthright, and efficient disclosure of information potentially relevant to the case — by burying relevant documents amid a sea of irrelevant ones." (ReedHycalog v. United Diamond, 2008)

In a 2010 case of data dumping the court did not award sanctions even though the defendant dumped the computer hard drive on the plaintiff because the plaintiff did not make the motion in a timely fashion. However the court did sanction the defendant for other discovery violations and warned if the motion on dumping had been timely there would have been additional sanctions. (Cherrington Asia Ltd. v. A & L Underground, Inc, 2010)

In yet another data dumping case, a third party produced three servers in response to a subpoena and court orders without conducting a review for either privilege or responsiveness. Later the party asked the court for the right to search the 800 GB and 600,000 documents for relevant materials at their cost in exchange for the return of any privileged documents. The court found that the party had made voluntary disclosure and resulted in a complete waiver of applicable privileges. The court pointed out that in nearly three months the party had not flagged even one document as privileged, so the court rejected its "belatedly and casually proffered" objections as "too little, too late." (In re Fontainebleau Las Vegas Contract Litig., 2011)

In a 2011 District of Columbia case, the defendants had produced thousands of e-mails just days before trial and continued to "document dump" even after the trial ended. The court found that "repeated, flagrant, and unrepentant failures to comply with Court orders" and "discovery abuse so extreme as to be literally unheard of in this Court." The court also repeatedly noted the defendants' failure to adhere to the discovery framework provided by the Federal Rules of Civil Procedure and advised the defendants to invest time spent "ankle-biting the plaintiffs" into shaping up its own discovery conduct. (DL v. District of Columbia, 2011)

4.2 Failure to Maintain a Litigation Hold

Failing to maintain a litigation hold when litigation can be reasonably anticipated is another ground for court-imposed sanctions. Kolon executives and employees had deleted thousands emails and other records relevant to DuPont's trade secret claims. The court fined the company's attorneys and executives reasoning they could have prevented the spoliation through an effective litigation hold process. Three litigation notices sent that were all deficient in some manner. (E.I. du Pont de Nemours v. Kolon Industries, 2011) The court issued a severe penalty against defendant Kolon Industries for failing to issue a timely and proper litigation hold. The court gave an adverse inference jury instruction that stated that Kolon executives and employees destroyed key evidence after the company's preservation duty was triggered. The jury responded by returning a stunning \$919 million verdict for DuPont.

4.3 Data Wiping

In a recent shareholders' action in Delaware extreme sanctions were ordered against the defendant Genger. Genger and his forensic expert used a wiping program to remove any data left on the unallocated spaces on his ESI sources after a status quo order had been entered and after the opposing side had searched his computer and obtained all ESI. The sanctions included attorney fees of \$750,000, costs of \$3.2 million, changing the burden of proof from "a preponderance of the evidence" to "clear and convincing evidence," and requiring corroboration of Genger's testimony before it would be admitted in evidence. On appeal, the defendant argued the sanctions were disproportionate and excessive since he erased only unallocated free space and did not erase this information until after the

plaintiff had searched all of the data sources. Further, the status quo order did not specifically mention preserving the unallocated space on the computer. The defendant also argued that normal computer use would likely cause overwriting of unallocated space to occur. Further, if this order were affirmed by the court computer activities would have to be suspended every time a discovery order issued. In 2011 the Supreme Court of Delaware upheld the sanctions. (Genger v. TR Investors, LLC, 2011)

In a patent infringement case, plaintiffs asked for sanctions against the defendants for their failure to produce relevant electronic documents. The defendants' excuse was that their e-mail servers were not designed for archival purposes. The company policy was that employees should preserve valuable e-mails. The court refused to grant safe harbor provision citing the forensic expert's declaration that failed to state the destruction was a result of a "routine, good-faith operation." (Phillip M. Adams & Assocs. LLC v. Dell, Inc., 2009)

In another case, almost every piece of media ordered to be produced was wiped, altered or destroyed. In addition, the last modified dates for critical evidence were backdated and modified. The court found the plaintiff guilty of "bad faith and with willful disregard for the rules of discovery" and ordered a default judgment, dismissed the plaintiff's complaint with prejudice and ordered \$1,000,000 in sanctions. In addition, the plaintiff's counsel was ordered to pay all costs and attorney fees for their part in the misconduct. (Rosenthal Collins Grp., LLC v. Trading Tech. Int'l Inc., 2011)

4.4 Social Media

In a social media case an attorney was sanctioned when the attorney had his client purge unflattering posts and photos on his Facebook account. The court found that the attorney, Murray, told his client, the plaintiff in a wrongful death suit brought after his wife was killed in an auto accident, to remove unflattering photos including one in which the distraught widower was holding a beer and wearing a t-shirt emblazoned with "I [heart] hot moms." (Lester v Allied Concrete et al, 2012)Murray instructed his client through his assistant to "clean up" his Facebook account. Murray's assistant emailed to the client "We do not want blow ups of other pics at trial, so please; please clean up your Facebook and MySpace!!" (Lester v Allied Concrete et al, 2012) The attorney was fined \$522,000 even though he argued he did not consider the social media site an ESI site. (Lester v Allied Concrete et al, 2012)

In another interesting case, several key employees intentionally and in bad faith destroyed 12,836 emails and 4,975 electronic files. The defendant argued that most of these files were recovered and thus the plaintiffs were not harmed. Declaring these deletions significant in substance and number, the court imposed an adverse inference instruction and ordered payment of attorney fees and costs incurred as a result of the spoliation. (E.I. Du Pont De Nemours & Co. v. Kolon Indus., Inc., 2011)

In another case, the plaintiff sought a default judgment sanctions alleging the defendants intentionally deleted relevant ESI by lifting a litigation hold, erasing a home computer, delaying preservation of computers hard drives and deleting files, defragmenting disks, and destroying server backup tapes, ghost images, portable storage devices, e-mails and a file server. The court determined that a default judgment was appropriate given the defendants' "unabashedly intentional destruction of relevant, irretrievable evidence" and egregious conduct. (Gentex Corp. v. Sutter, 2011)

4.5 Egregious Behavior

After five years of case law, rules, and The Sedona Conference best practices principles there are still cases that so blatantly flaunt the rules and good practices that all can be said is what were they thinking? In an intellectual property dispute, the plaintiff and third-party defendants appealed the district court's decision to grant default judgment as a sanction for ESI spoliation. The court found that the plaintiff willfully and in bad faith destroyed ESI. The plaintiff and his employees videotaped the employees talking about their deliberate destruction of the potentially harmful evidence. In addition, the employee state one laptop off a building and drove a car over another one. In addition, one employee said '[If] this gets us into trouble, I hope we're prison buddies." Finding this behavior

demonstrated bad faith and a general disregard for the judicial process, the court affirmed the default judgment and award of attorneys' fees and costs. (Daynight, LLC v. Mobilight, Inc, 2011)

In a products liability case, the plaintiff sought to re-open a case and asked that sanctions be ordered against the defendant for systematically destroying evidence, failed to produce relevant documents and committed other discovery violations in bad faith. The plaintiff's attorney uncovered documents requested in the litigation nearly a year after trial ended when conducting discovery in another case. The court determined the unproduced e-mails were extremely valuable and prejudiced the plaintiff. Further, the court found the defendant's discovery efforts were unreasonable. The defendant put one employee who was admittedly "as computer literate —illiterate as they get" in charge. In addition, the defendant failed to search the electronic data, failed to institute a litigation hold, instructed employees to routinely delete information and rotated its backup tapes, thus permanently deleting data. The court ordered that defendant was to pay \$250,000 in civil contempt sanctions. The unusual part of the order was that the court imposed a "purging" sanction of \$500,000, extinguishable if the defendant furnished a copy of the order to every plaintiff in every lawsuit proceeding against the company for the past two years and to file a copy of the order with its first pleading or filing in all new lawsuits for the next five years. (Green v. Blitz U.S.A., Inc., 2011)

5. THE SAFE HARBOR

The court has great leeway in imposing sanctions on litigants who fail to produce relevant materials to the opposing party or who has tampered with or destroyed information or metadata. Sanctions can vary from fines, attorney fees, an award of costs, and adverse-inference instructions to outright dismissal of the case. However, in an effort to distinguish between inadvertent mistakes and outright obstruction, Federal Rule 37(f) provides: "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.' (Federal Rule of Civil Procedure, 2006)

This rule indicates that parties could implement and rely on their document retention and deletion policy that provides for the routine and frequent destruction of electronic evidence and still be protected from civil sanctions when they were unable to produce relevant electronic evidence. However, case law has not always followed that simple interpretation. With all this information from rules to cases to think tanks on best practices, the question that remains is whether the safe harbor provision protects litigants and does it matter if the failure is based on ignorance, mistake or willfulness?

5.1 Ignorance

In a 2011 case the defendants sought sanctions alleging the plaintiff failed to produce relevant information and further was guilty of spoliation of evidence by donating her personal computer to an overseas school after commencing the action. The court found that the plaintiff did not act in bad faith and unlike corporate parties, the plaintiff in this case was unsophisticated and unaccustomed to preservation requirements. Further, the court stated the e-mails were withheld under the good faith misconceptions of relevance and privilege. Therefore, the court found no evidence of prejudice or bad faith and their court declined to impose sanctions. (Neverson-Young v. Blackrock, Inc, 2011)

5.2 Mistake

In another 2011 case, the plaintiff brought a motion for sanctions in a wrongful termination case alleging the defendants failed to: (1) issue a prompt litigation hold resulting in the destruction of electronically stored information (ESI); and (2) provide emails in their native file format, producing them in paper instead. The court denied the plaintiff's motion for sanctions holding that FRCP 37(e) grants safe harbor for the defendants' automated destruction of emails based on their existing document retention policy. (Kermode v. University of Miss. Med. Ctr, 2011)

5.3 Lack of Good Faith

In a 2008 case, the defendants sought a spoliation jury instruction alleging the plaintiff failed to preserve and produce requested copies of critical e-mails. Further, the plaintiff failed to notify the defendants that evidence had been lost prior to the defendant sending an employee out to the plaintiff's site to inspect it. The court determined there was an absence of bad faith and denied both requests for sanctions. (Diabetes Ctr. of Am. v. Healthpia Am., Inc, 2008)

In a 2011 products liability litigation case, the plaintiffs sought ESI sanctions against the defendants for failure to preserve data. Despite the discovery violations alleged by the plaintiff, including the failure to preserve and produce relevant e-mails, the court noted that procedural defects and the Rule 37(e) safe harbor provision barred the imposition of sanctions as the e-mails were deleted as part of a routine system

5.4 Not enough Evidence

In another 2011 case the court refused to compel data restoration or a finding of bad faith in an employment law case. The defendant requested damages from the plaintiff (the former employee) for damages for erasing data from his company-issued laptop. The employee claimed that he did not have any way of removing his personal data. The court found that it was far from clear whether plaintiff deleted the files in bad faith and that there was a lack of evidence that the defendant was harmed.

6. EXTREME MEASURES

In September, 2011 Chief Judge Randall R. Rader introduced a Model Order to be used in Patent cases which basically eliminated e-discovery and metadata. For example, item 5 of the Model Order read "General ESI production requests under Federal Rules of Civil Procedure 34 and 45 shall not include metadata absent a showing of good cause." In addition this model order severely limited electronic discovery. (Rader, 2011)

This order is contrary to the Sedona Principle 12 that holds the production of data should take into account "the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case." (Sedona, 2009)

7. CONCLUSION

In conclusion both federal and state courts have had an increasing number of cases where they have determined that sanctions are appropriate since the new Federal Rules of Civil Procedure were enacted in 2006, especially Rule 26(f). The probability of receiving sanctions seems to depend on the harm the missing information has caused or can cause as well as the bad faith involved in the failure to provide discovery. The severity of bad faith conduct increases the severity of the sanction imposed. Often the litigant has had numerous acts of misconduct that will result in negative-inference jury instructions and summary judgment.

In a landmark case decided by Judge Paul Grimm, the defendant responded to discovery using boilerplate objections. Judge Grimm ruled that use of such broad objections violates FRCP 33(b)(4) and 34(b)(2). Judge Grimm stated that the parties must have a meet-and-confer conference prior to discovery, discuss any controversial issues – including timing – costs, and the reasonableness of the discovery request in proportion to the value of the case. (Mancia v. Mayflower Textile Servs. Co, 2008)

Lawyers have been trained to be advocates and adversaries and to represent their clients zealously. However, with the volume of ESI today, lawyers must redefine what zealous representation means. Cooperation in the discovery process by full disclosure of the ESI and cooperation in devising a discovery plan will save the client money in the long run, avoid sanctions, and allow a full and fair

trial on the merits.

REFERENCES

Securities and Exchange Commission vrs Martha Stewart and Peter Bacanovic, 03 CV 4070 (NRB) Complaint (United States Disct Court Southern District of New York 2003).

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y 2003).

E.I. du Pont de Nemours v. Kolon Industries, 3:09cv58 (E.D. VA July 21, 2011).

Cherrington Asia Ltd. v. A & L Underground, Inc, WL 126190 (D. Kansas January 8, 2010).

Daynight, LLC v. Mobilight, Inc, WL 241084 (Utah App Jan 27, 2011).

Diabetes Ctr. of Am. v. Healthpia Am., Inc, WL 336382 (S.D. Texas Feb 5, 2008).

DL v. District of Columbia, No. 05-1437 (D.D.C. May 9, 2011).

E.I. Du Pont De Nemours & Co. v. Kolon Indus., Inc, WL 2966862 (E.D. VA July 21, 2011).

Federal Rule of Civil Procedure, 37(f) (2006).

Federal Rules of Civil Procedure, Rule 26 (A)(1)(ii) (2006).

Federal Rules of Civil Procedure, Rule 26(f) (December 2006).

Genger v. TR Investors, LLC, WL 2802832 (Del Supreme July 18, 2011).

Gentex Corp. v. Sutter, WL 5040893 (M.D. PA October 24, 2011).

Green v. Blitz U.S.A., Inc., WL 806011 (E.D. Tex March 1, 2011).

In re Fontainebleau Las Vegas Contract Litig., WL 65760 (S.D. Fla Jan 7, 2011).

Kermode v. University of Miss. Med. Ctr, 3:09-CV-584-DPJ-FKB (S.D. Jul 1, 2011).

Lester v Allied Concrete et al, CL108-150 (CC Virgina 2012).

Luoma, M. &. (2009). Qualcomm v. Broadcom: Implications for Electronic Discovery. Proceedings of the 7th Australian Digital Forensics Conference. Perth: Edith Cowan University School of Computer and Information Science.

Luoma, M. V. (2011). ESI a Global Problem. International Conference on Technology and Business Management, Dubai. UAE.

Lyman, P. V. (2003). How Much Information? Retrieved August 6, 2010, from University of California Berkley School of Information Management and Systems: www.sims.berkeley.edu/how-much-info

Mancia v. Mayflower Textile Servs. Co, WL 4595275 (D. MD October 15, 2008).

Neverson-Young v. Blackrock, Inc, WL 3585961 (S.D.N.Y. August 11, 2011).

Phillip M. Adams & Assocs., LLC v. Dell, Inc, WL 910801 (D. Utah March 30, 2009).

Rader, R. (2011, September). Model Order. Retrieved January 21, 2012, from An E-Discovery Model Order.

 $http://memberconnections.com/olc/filelib/LVFC/cpages/9008/Library/Ediscovery\%\,20 Model\%\,20 Order.pdf$

ReedHycalog v. United Diamond, Lexis 93177 (E.D. Texas October 3, 2008).

Residential Funding Co. v. DeGeorge Financial Co, 306 F.3d 99 (2d Cir 2003).

Rosenthal Collins Grp., LLC v. Trading Tech. Int'l Inc., WL 722467 (N.D. Ill Feb 23, 2011).

Sedona. (2009). Commentary on Achieving Quality in the E-Discovery Process. Sedona conference.

ADFSL Conference on Digital Forensics, Security and Law, 2012

Sedona: Sedona Publishers.

Victor Stanley, Inc. v. Creative Pipe, Inc., WL 3530097 (D. MD 2010).

Williams v. Sprint/United Mgmt. Co., . LEXIS 21966 (U.S. Dist Kansas September 20, 2005).