Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 6, Issue 1; January-March, 2019, pp. 1-6

http://www.krishisanskriti.org/Publication.html

Information Technology Infrastructure for Managing Costs in Litigation Involving Electronic Evidence

Gautam B. Singh

Professor, Computer Science and Engineering,
Oakland University, USA

Abstract—*As complexity of e-discovery requests and the volume of relevant electronically stored information continues to grow, parties in litigation face numerous challenges related to processing, reviewing, and producing electronic documents in response to discovery requests. A party that incorporates a proactive strategy and an appropriate framework for managing their electronic records reaps benefits of responding timely to discovery requests and minimizing risks of sanctions. The integration of an information management framework for processing electronically stored information also facilitates in authentication of electronic evidence at trial.*

1. INTRODUCTION

Until recently, when the Supreme Court in the United States approved amendments to the Federal Rules of Civil Procedure (FRCP) to accommodate the modern practice of discovery of electronically stored information, courts had been applying the traditional paper discovery rules in situations even when the information sought was electronically stored. Statistics show that roughly 80% of electronic documents are never printed, and that every day over 260-280 billions email messages are exchanged[1];it stands to reason therefore that the impact of e-discovery is expected to besignificant and particularly so for those organizations where e-discovery is an issue.

This paper addresses the interplay of e-discovery and litigation and is organized as follows. Section I presents a summary of the amendments to the U.S. Federal Rules of Civil Procedure that are specifically related to e-discovery. Section II summarizes interpretations of these regulations in cases dealing with discovery sanction, safe harbor, and cost shifting. Section III outlines the Electronic Discovery Reference Model or EDRM, and its role in taking a proactive approach towards e-discovery and the ramifications of using information management strategies for controlling costs and risks associated with e-discovery.

Discovery is intended to yield admissible evidence. Any documentary evidence, including the electronically stored information has to overcome the authentication burden. An appropriate framework for managing electronic documents in an organization's normal course of business further facilitates its use as evidence under the business record exception to the hearsay rule.

2. E-DISCOVERY LEGISLATION

Amendments of the FRCP Electronically Stored Information (ESI) affect all the phases of discovery process beginning with the scheduling order to the format of the actual ESI submitted in response to a request, as well as the safe harbors when ESI is lost. The phrase "electronically stored information" used in FRCP 26, 33, and 34 primarily to acknowledge that ESI is discoverable.("Fed. R. Civ. P. 26, 33, 34,")

The amended FRCP substituted "electronically stored information" for "data compilations" as a category of the required initial disclosures. ("Fed. R. Civ. P. 26(a)(1)(A)(ii).")This expansive phrase is meant to include "any medium from which information can be obtained either directly. after translation;"("Fed. R. Civ. P. 34(a)(1)(A).")the term being broad and flexible enough to cover all types of storage media that is electronically stored today, or in the future.

3. PARTIES TO ADDRESS ESI EARLY IN LITIGATION

The rules encourage the parties address the availability of electronically stored information early in the discovery process, recognizing that such early attention is crucial in order to control the scope and expense of e-discovery and avoid discovery disputes. The amendments to FRCP 16, relating to pretrial conferences, scheduling and management, state that the scheduling order may provide for "disclosure or discovery of electronically stored information" and include any agreement for asserting privilege or protection of information after its production.("Fed. R. Civ. P. 16(b)(3),")

* Gautam B. Singh, PhD, JD, is a Professor of Computer Science and Engineering at Oakland University, Rochester, Michigan, USA. He is also a practicing Technology Lawyer in the Metropolitan Detroit area, Michigan, USA. He is a member of the Michigan Bar, US Patent Bar, Federal Bar, and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). He can be contacted at singh@oakland.edu.

[1] Source: https://www.lifewire.com/how-many-emails-are-sent-every-day-1171210. *Last accessed* January 14, 2019.

4. FORMAT OF ESI PRODUCTION AND ITS USE

FRCP 34 defines the procedures for production of ESI during discovery. Whether the discovery request is made to an opposing party, or to third parties pursuant to a subpoena, amended FRCP 34 defines that ESImust be produced in either *(a)*the form in which the information is ordinarily maintained, or *(b)* in a reasonably usable form.("Fed. R. Civ. P. 34(b)(2)(E),") The rule does not require the requesting party to choose a form of productionsince the requesting party may not know the form the producing party uses to maintain its ESI. Theamended FRCP 33(d)further states that in so far as answering interrogatories are concerned, ESI should be consulted as a business record.("Fed. R. Civ. P. 33(d),")

5. WHEN ESI IS NOT ACCESSIBLE OR IS DESTROYED

The amended rule FRCP 26(b)(2)(B) makes a distinction between ESI that is reasonably accessible, and that which is not. It states that a "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost."("Fed. R. Civ. P. 26(b)(2)(B),")Upon a motion to compel discovery by the requesting party however, the court will order discovery only for good cause shown. The amendments to FRCP 37(e) further direct that "absent exceptional circumstances," a court may not impose sanctions when ESI is lost due to "routine, good-faith operation of an electronic information system." The rules thus recognize that ordinary computer use necessarily involves routine ESI alteration and deletion.("Fed. R. Civ. P. 37(e),")

6. E-DISCOVERY LAWS AND INFORMATION MANAGEMENT

Unless it is stipulated by the parties or ordered by the court, ESI is almost always produced in its electronic form. It is not enough, for instance, to print out hundreds of emails and present them as a product of discovery. The amended rules have in effect created a new *category* of discoverable information. There is discoverable metadata on ESI as well, and to fully appreciate the scope of information discoverable from ESI, the counsel must work closely with the information technology personnel. Attorney should learn about the system, ESI, its encryption, and any metadata encoded therein.

7. SPOLIATION … AND … SAFE HARBOR

Spoliation is defined as the act of destroying or significantly altering evidence. The failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation is constructive equivalent of spoliation.("Reilly v. Natwest Mkts. Group. Inc.," 1999)A party bringing a spoliation claim must demonstrate that:

(i) The party having control over the evidence had an obligation to preserve it at the time it was destroyed;

(ii) The [evidence was] destroyed with a culpable state of mind; and

(iii) The destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.("Residential Funding Corp. v. DeGeorge Fin. Corp.," 2002)

Since civil litigation is likely to encompass relevant electronic data, parties may be tempted to think that consequences of producing such data are avoided by deleting the data, or by employing tools that are designed to erase data. Such an intentional spoliation of evidence is a bad idea indeed since courts impose serious sanctionsin cases of intentional spoliation.

In *Gutman v. Klein*, plaintiff claimed that a defendant had engaged in spoliation of crucial evidence on defendant's laptop. ("Gutman v. Klein," 2008). At some point during the five-year procedural history of this case, a federal magistrate ordered the defendant to make his laptop hard drive available to the plaintiff for examination. When plaintiff suspected that defendant had tampered with the laptop, the court ordered a forensic examination of the hard drive. As a result, it was discovered that defendant had used a file deletion program and numerous files on the laptop were rendered unrecoverable. Given that the defendant action of permanently deleting selective files were in direct contradiction to their duty to preserve relevant evidence, magistrate imposed severest sanctions.

FRCP 37(e) incorporates a safe harbor provision where, absent exceptional circumstances, a court may *not* impose sanctions on a party for failing to provide ESI lost as a result of the routine, good-faith operation of an electronic information system.("Fed. R. Civ. P. 37(e),")This rule recognizes that electronic information systems are generally designed to perform routine modification and deletion of information. Notwithstanding that safe harbor provision protects a party if the ESI is lost in good faith, parties are obligated to preserve ESIreasonably expected to be relevant in a pending litigation. A party may not use the safe harbor provision to evade discovery obligations by failing to prevent destruction of ESI that it is required to preserve.

8. SANCTIONS

The court has a wide discretion in sanctioning a party for discovery abuses, "[w]hether exercising its inherent power, or acting pursuant to Rule 37."("Reilly v. Natwest Mkts. Group. Inc.," 1999) Further, the courts impose the harshest sanctions in cases involving wilfulness, bad faith, where the ultimate sanction of default judgment is imposed against a party engaged in wilful spoliation.("Salahuddin v. Harris," 1986)The court uses this ultimate sanction only in extreme circumstances, usually after consideration of alternative, less drastic sanctions.("West v. Goodyear Tire & Rubber Company," 1999)

In Gutmancase discussed earlier, the court concluded that defendant destroyed evidence in bad faith andany sanction lesser than a default judgment would place the risk of an erroneous judgment on the plaintiff.("Gutman v. Klein," 2008)When the forensic examination uncovered the existence of missing computer files that were irretrievably deleted in folder labeled Privileged, Confidential, Gutman Litigation, and Copy of Gutman Litigation, it was impossible to know what implications of their contents would have if discovery obligations were complied with. Therefore, the magistrate recommended a default judgment for the plaintiff and ordered defendant to pay attorney fees and costs. Id.

Under exceptional circumstances such as those in Gutman, a default judgment appears to be the only appropriate sanction. When compliance with discovery rules results in production of damning evidence, any sanction less than default judgment can not deter destruction of a decisively adverse e-evidence.("Kronisch v. United States," 1998)

Typically however, the court balances the "prophylactic, punitive, and remedial" rationales in imposing sanctions where the purpose of sanctions is to deter parties from engaging in spoliation, to place the risk of an erroneous judgment on party engaging in spoliation, and to restore the prejudiced party to the same position as it would have absent spoliation. Id., ("Hotel Employees & Rest. Employees Int'l Union," 2003)

9. COST OF E-DISCOVERY

Normally the producing party bears the cost of production. However, FRCP 26(b)(2) limits discovery where "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case." ("Fed. R. Civ. P. 26(b)(2),")Considering the potential for unbridled escalation of a simple ESI request, this rule is put to the test in cases of e-discovery.

In *Rowe Entertainment Inc. v. William Morris Agency, Inc*., the court stated that modern day discovery "is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter." ("Rowe Entertainment Inc. v. Willam Morris Agency, Inc.," 2002)The court established an eight-factor test to help courts evaluate whether the costs of production should be shifted. The court came up with a balancing test, or the *Rowe-test*,to decide when cost of e-discovery should be shifted to the requesting party.

A year later, in *Zubulake v. UBS Warburg*, a gender employment discrimination case, the court noted that the application of the Rowe factors may inappropriately result in disproportionate cost for some defendants.("Zubulake v. UBS Warburg," 2003)

In *Zubulake*, the plaintiff requested that defendant produce "[a]ll documents concerning any communication by or between UBS employees concerning the plaintiff."*Id.* at 321. The defendant produced 350 pages of documents, including approximately 100 pages of e-mail. The plaintiff had knowledge that additional responsive e-mail existed on archival media and requested that the defendants produce additional archived e-mails. Claiming undue burden and expense under *Rowe-test*, the defendant urged the court to shift the cost of production to the plaintiff.

While the court stated that consideration for cost shifting is appropriate when electronic data is relatively inaccessible as was indeed the case at bar,the court stated that *Rowe-test* was duplicative and proceeded to modify it by considering the amount in controversy, and the importance of the issues at stake. *Id.* at 324. The court ordered the defendant to produce, at its own expense, all responsive email existing on disks, servers, and backup tapes. In that case, the court decided that a cost shifting analysis would be done after contents of the backup tapes are reviewed and the defendant's costs were quantified. *Id.*

10. E-DISCOVERY: A SHIELD OR A SWORD?

Generally, the individual plaintiff, as for example an employee who is subjected to employment discrimination, will have little ESI to preserve. Whereas the employer, against whom the suit is filed, will have the vast majority of ESIs such as emails exchanged, documents written and reports prepared. Consequently, the plaintiff's attorney will use the ESI request as a sword requiring the employers to bear the burden of searching and producing all relevant ESI. The disparity of the e-discovery burden being so disproportionate, the plaintiff's attorney will generally not be motivated to stipulate to a mutual relief from e-discovery requests.

With the use of appropriate information management framework however, such as the Electronic Discovery Reference Framework, a party can shield itself from becoming a hostage to e-discovery requests. This appears to be the only practical strategy. The employer needs to be proactive in incorporating a framework for managing discoverable ESI with efficient and cost-effective processes for preserving, searching, and producing relevant ESI when called upon to do so.

11. ELECTRONIC DISCOVERY REFERENCE MODEL (EDRM)

Electronic Discovery Reference Model (EDRM) project was created as a conceptual, non-linear, iterative, and extensible framework for "development, selection, evaluation and use of electronic discovery."(Socha & Gelbmann, 2005)EDRM, shown in Figure 1, follows a left to right path starting with the integration of an information management infrastructure for handling ESI and concluding with the presentation of electronic evidence in courtroom.

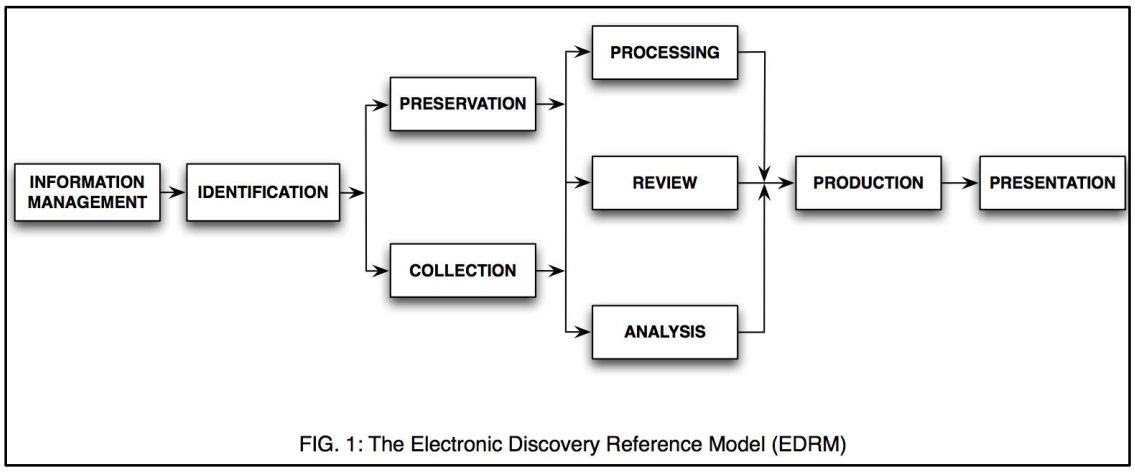

FIG. 1: The Electronic Discovery Reference Model (EDRM)

The first EDRM stage is essentially a prerequisite for all the subsequent stages. It requires that an information management be used as the infrastructure to reduce for supporting e-discovery requests.

The beginning of e-discovery for a specific case occurs during the next phase, which is the identification phase, wherein the location of the ESI artifacts, data-ranges, or transaction-boundaries of relevance are identified. Next, the collection and preservation phaseentails the actual harvesting of ESI using data collection tools, including electronic forensic tools. The harvested information isanalyzed, processed and filtered by type, keywords, concepts, dates, and so on. Attorneys review the processed information, and forensic examiners further analyze relevant documents for evidence of spoliation.

Upon the completion of in-house processing, review and analysis, ESI is turned over to the opposing counsel during the production phase. The form of ESI produced complies with FRCP 34 requiring that the ESI be produced in its native or a reasonably usable form.("Fed. R. Civ. P. 34,") Finally, during the presentation phase, data is presented for legal purposes at depositions or at trial. While ESI is often presented in its native or near native formats for evidentiary purposes, its specific aspects are highlighted for persuasion.

12. INFORMATION MANAGEMENT UNDER THE EDRM

Lessons from case law provides valuable guideposts and make a case for utilizing an EDRM-based, or a similar approach, for managing electronic documents. First, an infrastructure enables a party to preserve evidence as soon as it has notice that the evidence is relevant to litigation, or as soon as it should have known that the evidence might be relevant to future litigation,("Fujitsu Ltd. v. Fed. Express Corp.," 2001)and second, it prevents the preservation of evidence from being sloppy or negligent with respect to ESI.

EDRM helps a party to be prepared to comply with court orders, since where court orders are clear noncompliance is deemed willful("Bambu Sales, Inc. v. Ozak Trading, Inc.," 1995)and is subject to the severest sanctions. Information management procedures with quality control should be put in place as soon as litigation ensues so thata party preemptively prevents court from ruling bad faith conduct.

And judicial opinions clearly enunciate the view that evidence destroyed in bad faith, presumably destroyed after being put on notice, is sufficient circumstantial evidence from which a fact-finder may infer that destroyed evidence was unfavorable to a party. Furthermore, the second judicial circuitheld that ordinary negligence is a sufficiently culpable state of mind for spoliation.("Residential Funding Corp. v. DeGeorge Fin. Corp.," 2002)This clearly implies that appropriate mechanisms for control of ESI need to be proactively put in place.

To avoid from being perceived as negligent, well-defined policies for backing up relevant ESI need to be established. Otherwise, a court may infer that evidence destroyed, albeit through sheer negligence and sloppiness, was relevant. By adopting proactive policies for ESI destruction, a party falls squarely within the safe harbor provisions of the rules as in *U.S. v. Maxxam* where the court declined to impose spoliation sanctions when there was no evidence of intentional destruction of ESI and where, at the time of destruction, there was no duty to preserve.("U.S. v. Maxxam, Inc.," 2009)

Information management procedures also help in situations where a party allegedly destroys evidence due to ordinary negligence. In such a situation, the prejudiced party has the burden of showing that ESI relevant to their claim was included in the files destroyed. ("Byrnie v. Town of Cromwell, Bd. of Educ.," 2001)Such a showing becomes significantly difficult for the prejudiced party when the allegedly negligent party uses well-defined quality control procedures wherein a document pre-screening prevents inadvertent destruction of relevant ESI.

13. DEVELOPING INFRASTRUCTURE TO PRESERVE EVIDENCE

In *U.S. v. Suarez*, the government failed to produce certain electronic SMS messages related to its investigation. The defendants moved the court to either suppresses the electronic evidence, or issue an adverse inference instruction.("United States v. Suarez," 2010)In court's view the inability to produce SMS messages was indicative of government's negligence and granted defendants' motion for an adverse inference instruction.

14. CHALLENGE: ESI BECOMES ALL ENCOMPASSING

*United States v. Suarez*points to the new challenges that IT management divisions are likely to face whereby evidence on PDAs, smart-phones, social-media sites, and other similar ubiquitous computing devices that are becoming commonplace may not be negligently destroyed when a party is put on notice of litigation. The all-encompassing nature of electronic evidence brings forth new challenges in managing and organizing the collection of disparate forms of ESI from various sources at multiple locations. Done properly, evidence collection can serve as the foundation for ensuring fast, accurate and cost-effective response to e-discovery requests.

15. COST OF E-DISCOVERY: ANY OBJECTIVE MEASURES?

It is well accepted that the use of software process models reduces cost and enhances quality of the software development.(Paulk, Curtis, Chrissis, & Weber, 1993) Incorporating a framework for information management will offer the advantages of reducing cost and ensuring quality of ESI produced. Organizations expecting to be subjected to e-discovery requests will therefore benefit from the use of an information management framework.

As provided in FRCP 26(b)(2), and interpreted by *Rowe* and *Zubulake*, cost of electronic discovery is a factor in the court's determination of whether or not the such costs will be borne by the requesting party. The next logical question is likely to be whether these costs are measured using an objective, or subjective standards. While the current opinions of the courts have largely measured it using a subjective yardstick in reference to the producing party, it is quite likely that with ubiquitous and prevalence of electronics, courts will bring some objectivity into the e-discovery cost estimates. A party who expects to be hauled in court might also be expected to incorporate an information management system, such as the EDRM, into the operations and thereby keep a check on the overall cost of e-discovery.

16. AUTHENTICATING AND ADMITTING ELECTRONIC EVIDENCE

Assuming that a party seeks to admit an ESI artifact at a trial, the common hurdles of hearsay and authentication can be overcome if information management guidelines are utilized in controlling ESI. Evidence might be deemed self-authenticating if ESI is computer generated. Further, a party that manages ESI as a regular business practice can make a case for admitting an ESI artifact as evidence under business records exception to the hearsay rule. As to the format of ESI admitted into the evidence, it will most likely need to be in a form that is "reasonable usable" by the trier of facts.

17. CONCLUSIONS

It is clear that electronic evidence will soon be an integral and essential part of any litigation. Corporate counsel should therefore be investigating the use of an appropriate information management infrastructure that proactively protects the organization and offers flexible collection options to meet the unique needs of each e-discovery requests such that privileged and proprietary information is protected. Using a formalized model to proactively manage ESI in an organization is certain to reduce the cost of e-discovery.

BIBLIOGRAPHY

[1] Bambu Sales, Inc. v. Ozak Trading, Inc., 58 849, 852-853 (2d Cir. 1995).
[2] Byrnie v. Town of Cromwell, Bd. of Educ., 243 93, 108 (2d Cir. 2001).
[3] Fed. R. Civ. P. 16(b)(3), 16(b)(3), Federal Rules of Civil Procedure.
[4] Fed. R. Civ. P. 26, 33, 34, 26, 33, 34, Federal Rules of Civil Procedure.
[5] Fed. R. Civ. P. 26(a)(1)(A)(ii). 26(a)(1)(A)(ii). Federal Rules of Civil Procedure.
[6] Fed. R. Civ. P. 26(b)(2), 26(b)(2), Federal Rules of Civil Procedure.
[7] Fed. R. Civ. P. 26(b)(2)(B), 26(b)(2)(B), Federal Rules of Civil Procedure.
[8] Fed. R. Civ. P. 33(d), 26(a)(1)(A)(ii). Federal Rules of Civil Procedure.
[9] Fed. R. Civ. P. 34, 34, Federal Rules of Civil Procedure.
[10] Fed. R. Civ. P. 34(a)(1)(A). 34(a)(1)(A), Federal Rules of Civil Procedure.
[11] Fed. R. Civ. P. 34(b)(2)(E), 34(b)(2)(E), Federal Rules of Civil Procedure.
[12] Fed. R. Civ. P. 37(e), 37(e), Federal Rules of Civil Procedure.
[13] Fujitsu Ltd. v. Fed. Express Corp., 247 423 (2d Cir. 2001).
[14] Gutman v. Klein, 2008 4682208 (E.D.N.Y. Oct 15, 2008).
[15] Hotel Employees & Rest. Employees Int'l Union, 212 178, 230 (S.D.N.Y. 2003).

[16] Kronisch v. United States, 150 112, 126 (2d Cir. 1998).
[17] Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *Software, IEEE, 10*(4), 18-27.
[18] Reilly v. Natwest Mkts. Group. Inc., 181 253, 267 (2d Cir. 1999).
[19] Residential Funding Corp. v. DeGeorge Fin. Corp., 306 107 (2d Cir. 2002).
[20] Rowe Entertainment Inc. v. Willam Morris Agency, Inc., 205 421, 423 (2002).
[21] Salahuddin v. Harris, 782 1127 (2d Cir. 1986).
[22] Socha, G. J., & Gelbmann, T. (2005). The Electronic Discovery Reference Model Project (EDRM). Retrieved August 12, 2011
[23] U.S. v. Maxxam, Inc., 2009 817264 (N.D. Cal. Mar 27 2009).
[24] United States v. Suarez, 2010 4226524 (D.N.J. 2010).
[25] West v. Goodyear Tire & Rubber Company, 167 776, 779 (2d Cir. 1999).
[26] Zubulake v. UBS Warburg, 217 309 (S.D.N.Y. 2003).