SUMMER 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics, and cybersecurity needs. For this E-Newsletter, we focus on the topic of cloud storage technologies and the impact on legal, compliance, and investigations.

FINE LINES FROM RULE 37(E) AMENDMENTS

Seven months have passed since the amendments to the Federal Rules of Civil Procedure ("FRCP") Rule 37(e) were adopted. Already, we're getting a read from the courts on how the rule is going to be interpreted, and, the fine lines along which decisions will be made. Considering the near ubiquitous nature of electronically stored information and e-discovery as part of legal proceedings, reviewing trends relevant to Rule 37(e) makes sense.

A Brief Recap

In December 2015, FRCP Rule 37(e) was amended specifically to address the expansion of ESI. The previous 2006 amendment was found lacking in the face of increasing ESI capability and capacity. The 2006 rule read:

> 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.

The revised rule reads:

(e) FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

Rule 37(e) applies only to ESI; and, its inherent differentiation from tangible evidence is not only important, but also instructive. The rule acknowledges that ESI is a form of evidence in its own right, and not merely a digital facsimile of tangible documentation. Whether this acknowledgement arises in part from a demonstrated importance of metadata, the progress made toward increasing paperless-ness, or simply from the well-established body of rules already governing tangible data, we may not know for certain, but we can infer a nod of gravitas to ESI from the amended rule that was previously absent.

A Question of Intent

The word "intent" missing from the 2006 version of Rule 37(e) may seem innocuous at first glance. However, spoliation determinations hinge on intent. Prior to the intent requirement, the rule lacked provisions on adverse inference and remedy. However, while the courts appear to have gained guidance in Rule 37(e) with regard to intent, a recent decision supports the idea that the court may look beyond 37(e) in exercising the court's inherent authority.

When evidence of intentional destruction or failure to preserve is not clear and convincing, the courts may still find that ineffective ESI practices are near analogous to intentional spoliation. In *Freidman v. Philadelphia Parking Authority, 2016 U.S. Dist. E.D. Pa. March 10, 2016*, the court found that an email storage system that didn't adequately preserve ESI, while not rising to the definition of intentional destruction under Rule 37(e), did meet the test for abuse or misconduct. In this instance, the Court found:

> "Without limitation, litigation misconduct may be otherwise sanctioned by the Court's inherent power. We are vested with broad discretion to fashion an appropriate remedy under our inherent powers to stop litigation abuse."

The takeaway for remote data storage users? Ineffective or sloppy ESI management practices may be just as damaging as intentional destruction in the eyes of the court. While intent to deprive negates the need to over-preserve, lack of intent is not a free pass to negligent data management.

Now You See It, Now You See It Again

Another addition to Rule 37(e) is the defining of lost ESI "because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery." The conjunction between the two clauses set up a conditional test: can the data be located from another source? In the Advisory Committee notes on Rule 37(e), the committee writes, "Because electronically stored information often exists in multiple locations, loss from one source may be harmless when substitute information can be found elsewhere."

If the ESI is located, the court can take a "no harm, no foul" approach, as they did in *Carlson v. Fewins, 2015 U.S. App. 6th Circuit.* In this case, the court ruled that spoliation of evidence did not occur when recordings of 911 calls were destroyed because the duplicate recordings of the calls were produced from another source. The perceived loss was in fact, harmless, as foreseen in the Advisory Committee note. It's important to note here that while the amendments to Rule 37(e) did

not take effect until December 1, 2015, Chief Justice Roberts ordered in April 2016 that the amendments be applied “insofar as just and practicable, all proceedings then pending.”

Just because evidence is produced from a secondary source, the courts are not restricted to finding that “substitute information” is just as good as the original. Slight alterations can become material, as in *Cat3, LLC v. Black Lineage, Inc. Dist. Court, SD New York 2016*. In Judge Francis’ January 12, 2016 Memorandum and Order, an interesting, albeit minor manipulation is at the heart of the issue.

Plaintiffs' email production revealed that each email message appeared in two versions within the production. The "top" level version of each email shows the message in full, as well as sender and recipient information and the date and time each message was sent/received.

However, behind each email message is a near-duplicate copy of the message containing the identical message, with the identical date and time. The only pieces of information that are altered from the top version of the email message to the near-duplicate version beneath are the certain email domains that appear for a number of the senders and recipients of the emails.

[According to expert testimony] this anomaly is the result of Plaintiffs having initially copied the version of the emails that contained the true and correct email addresses/domain names, and then deleting the true and correct versions prior to production. The deleted emails were then replaced with a second, altered version of the email correspondence, which was then produced to Defendants. (Emphasis added.)

In this case, the Plaintiffs, against whom the spoliation claim was made, argued that since they were able to produce the information in the emails from another source, they met the Rule 37(e) test for harmless loss and reproduction of ESI. Not so, according to Judge Francis, who wrote, “the fact that there are near-duplicate emails showing different addresses casts doubt on the authenticity of both.” Judge Francis determined the emails could not be used by Plaintiffs in the presentation of their case, showing that the line between lost and not lost can be very fine indeed.

A Word to the Wise

Legal history shows that the law tends to be cautious, reactive, and slow to change. Technology development demonstrates a proactive, daring, and ever-evolving environment. While the amendments to Rule 37(e) clarify much of what the 2006 version of the same rule did not, there’s clearly room for interpretation by the courts. As we’ve demonstrated in the above examples, the courts have not shied away from interpreting.

Some commenters point to the language in section (1) of the rule as non-specific when determining “measures no greater than necessary to cure the prejudice.” The wisdom of Solomon may be required to determine the extent of the prejudice in the case of lost ESI. Others question how egregious does the level of intent have to be to justify dismissal of an action under the amended Rule 37(e)? From what cases we’re seeing, it may be a while before we find out. Until then, our best bet is to take a lesson from the law when it comes to ESI and proceed with caution.

UPCOMING INDUSTRY EVENTS

July 2016
The Masters Conference, Managing the E-Discovery and Social Media Minefield,
New York: July 19

August 2016
HTCIA 2016 International Conference & Training Expo,

Las Vegas: August 28-31

ILTACON 2016,
National Harbor: August 28-Sept. 1

September 2016
CSA Congress and IAPP Privacy Academy 2016,
San Jose: September 15-16

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: