

Safe Harbor: Interpreting Rule 37(f), FRCP

by Gregory Fordham

Under the recently adopted changes to the FRCP, Rule 37(f) provides safe harbor to the inadvertent destruction of Electronically Stored Information (ESI). Specifically, it prohibits sanctions for the destruction of ESI absent exceptional circumstances.

In a recent case, *Doe v Norwalk Community College*, Slip Copy, WL 2066497, D.Conn (July 2007), the Safe Harbor provisions of Rule 37(f) were examined.

In that case, the Plaintiff alleged violations of Title IX as well as other state law claims. Later, she filed a Motion for Sanctions for Discovery Misconduct and Spoliation of Evidence against the college defendants.

The defendants sought refuge under the Safe Harbor provision of Rule 37(f) of the newly implemented FRCP as well as on other grounds. Regarding Safe Harbor, the Court said that, “[T]he Rule only applies to information lost ‘due to the routine operation of an electronic information system . . .’ ” In this case, however, the defendants had not followed their retention policy nor had they consistently followed any policy such that it could be construed as a routine system.

In addition, to take advantage of the safe harbor provision, a party must act affirmatively to prevent the system from destroying or altering information. But, in this case the defendants not only failed to prevent the system from destroying or altering information, there was evidence of tampering.

For example, files that contained Microsoft Outlook e-mail data had gaps in the received e-mail archives, very limited sent e-mail and no deleted e-mail.

In addition, one hard drive that the defendants claimed was failing was actually found to have all sectors overwritten with 0’s. There was also no partition which indicates that the drive was no longer formatted.

Finally, the Plaintiff’s forensic expert found that several files had been accessed and deleted within minutes prior to the investigation. In addition, large volumes of files had been copied onto the computer hard drive on the day of the investigation, which would overwrite and make unrecoverable other deleted data.

Based on the above, the safe harbor provisions were found inapplicable. Perhaps more important was that an adverse inference sanction was warranted.

To receive an adverse inference sanction three criteria must exist. First, there must have been a duty to preserve. Second, there must have been a culpable state of mind. Finally, the destroyed data must be relevant.

For the first prong, the defendants argued that the duty to preserve did not arise until the plaintiff filed her lawsuit and indicated her need for electronic discovery in her Rule (26)(f) Report of Feb 2005.

The Court strongly disagreed, however, and found that the duty to preserve was no later than the demand letter sent by Plaintiff’s counsel in Sept 2004 indicating an intent to sue. The Court noted that it could have also been much earlier, since there was a pending criminal investigation into the offending professor for sexual assault at the time College managers met to discuss the “Doe incident” in Feb. 2004.

For the second prong, the Court found that any destruction after a duty to preserve arises to be negligent. In this case, since the defendants failed to institute a litigation hold on documents and e-mails relevant to the case, they were grossly negligent. Furthermore, the defendant’s selective destruction of data evidenced intentional behavior.

Regarding the third prong, a claimant must generally show that the evidence was relevant to a party’s claims. The Court said the burden is different for gross negligence versus negligence.

After proving gross negligence, as was the case here, no other proof of relevance is necessary. Only when the defendant’s actions are negligent that the claimant must demonstrate that the destroyed evidence would have been relevant and favorable to the claimant’s case.

Clearly, this case provides valuable lessons for lawyers and laymen alike. First, the Safe Harbor provisions of Rule 37(f) are very narrow. A party must have a routine system that is followed exactly.

Second, once the duty to preserve arises the party must take affirmative action to interrupt its routine system relative to the relevant evidence.

Third, notices to preserve are essential to establish the latest date certain when a party’s duty to preserve arises.

Finally, the case demonstrates the importance of forensic analysis in e-discovery cases. Once again, using a computer is like throwing pebbles in a pond. The pebbles may not be recoverable but the ripples on the water and footprints at the shoreline are detectable nonetheless.

§§§

Gregory Fordham has written extensively on this subject. His papers are available for download from the K&F website, www.knfcon.com. He regularly advises clients on how to structure their e-discovery plans in order to minimize cost and maximize return. The Georgia Bar has approved his e-discovery presentation for CLE credit. He has been an expert witness in state and federal cases involving e-discovery and computer forensics. His e-mail is greg@knfcon.com

