New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 245—NO. 39
TUESDAY, MARCH 1, 2011

STATE E-DISCOVERY

Overbroad Demands And Improper Denials

By **Mark A. Berman**

Recent New York state trial court decisions offer detailed guidance on how to properly conduct electronic discovery and use of electronically stored information (ESI) as evidence on summary judgment.

Seeking an overbroad ESI preservation order will be rejected as a court will seek to balance, among other things, the need to preserve relevant ESI with not interfering with the operation of the preserving/producing party's business.

Caution should likewise be used when crafting keyword searches to seek to minimize the likelihood they will be found overbroad. Narrowly tailored searches will not only minimize the risk of having to review significant irrelevant information, but guard against an overly broad request being stricken or reduced in a manner that could potentially prejudice the requesting party's litigation strategy.

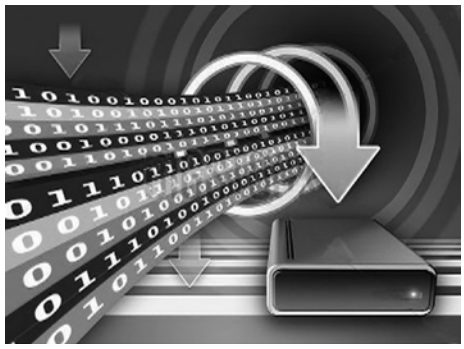
Further, conclusory denials in an affidavit that an individual does not possess ESI will not be condoned and, in response, there is a risk that a court may order an intrusive ESI computer search where the denial is not viewed as credible.

Affidavits should include what specific efforts were made to preserve and search for ESI and consideration should be given to providing an affidavit from a computer forensic expert substantiating the party's position.

Finally, when offering ESI as evidence on summary judgment or at trial, counsel needs to ensure that the proper evidentiary foundation is laid, under not just the CPLR, but also the state Technology Law.

Overbroad Request

In *JFA Inc. v. Docman Corp.*,[1] plaintiff engaged defendants to create proprietary software to assist in its business. Plaintiff alleged, among other things, that defendants: (i) never provided it with actual software in the form of a working server; (ii) poorly crafted the system; and (iii) never instructed plaintiff on how to use the software, and therefore plaintiff was forced to rely upon defendants to operate its business. Plaintiff sought a "preliminary injunction" seeking that defendant:



iSTOCK

- [b]e prohibited from any rotation, alteration, and/or destruction of electronic media that would result in the inability to recover computer data regarding all actual or potential business interests involving defendants;
- [p]rovide [plaintiff's] expert unrestricted access to defendants' computers and data, including all passwords or other necessary means to access the computers and data;
- [b]e prohibited from accessing, using, or booting the defendants' computers until [plaintiff] can secure a backup of defendants' computers and computer storage media; and
- [b]e prohibited from interfering with, accessing, destroying, disseminating, hiding, or in any way impeding the data of [plaintiff's] operations and its software.

Plaintiff's motion also sought an order of seizure of defendants' computers, hard drives, CD-ROMS, and other digital storage media located at defendants' premises, and an order permitting an expert to have unrestricted access to all of defendants' computers.

The court noted that the "bulk" of plaintiff's application seeks "essentially a protective order to preserve relevant electronic evidence."

Noting that plaintiff's motion was "clearly related to discovery, and not in the nature of a provisional remedy," the court stated that "the relevant inquiry is not whether [plaintiff] has met the three part test of injunctive relief, but whether a protective order for the preservation of electronic evidence should be granted."

The court indicated that although it was "inclined to permit the mirror image bit stream backup to preserve electronic evidence (see *Matter of Maura*, 17 Misc.3d 327 (Surr. Ct. Nassau County, 2007) [directing a clone of law firm's hard drive to be made]), [plaintiff] ha[d] not satisfactorily addressed the Court's concerns with the proposed modalities of conducting the electronic discovery."

Plaintiff sought imaging of all defendants' computers, including laptops, as well as handheld devices, such as smart phones.

The court noted that, although a mirror image bit stream backup would seek to preserve the proprietary software at issue, plaintiff did not make a showing that any handheld devices would contain relevant information.

Further, the court found overbroad plaintiff's request that defendants be directed to identify every computer that they "had ever used" for work not only for plaintiff, but also on behalf of non-party companies. The court found that the proposed seizure of defendants' computers to be overbroad, as some computers would be beyond the court's jurisdiction.

The court then balanced defendants' right to run their business with plaintiff's request, and held that removing computers from defendants' premises or ordering defendants not to "power up" their computers until a backup could be made would be too disruptive to defendants' operations.

The court noted that plaintiff failed to "explain how particular files that could contain discoverable electronic information could be affected by the act of powering up defendants' computers."

As such, plaintiff was directed to perform the mirror image bit stream backup at defendants' premises.

MARK A. BERMAN, *a partner at commercial litigation firm Ganfer & Shore, is secretary of the e-discovery committee of the Commercial and Federal Litigation Section of the New York State Bar Association.* ANNE D. TABACK, *an associate at the firm, assisted in the preparation of this article.*

'Mosley'

The plaintiff in *Mosley v. Conte*,[2] a defamation action, sought to have defendant's "computers, hard drives, external memory cards, data files, and external hard drives reviewed by a forensic expert, of [p]laintiff's choice, for data extraction and analysis limited" to plaintiff's proposed keyword search terms (which included names of individuals and companies as well as e-mail addresses) during a specified period of time.

The court noted that:

> [a]s parties serve discovery demands for ESI, they sometimes use keyword searches to focus their demands. However, "[w]hether search terms or keywords will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics." Therefore, "keyword searches work best when the legal inquiry is focused on finding particular documents and when the use of language is relatively predictable." Parties should not "design[] keyword searches in the dark, [or] by the seat of the pants." Instead, they should be able "to explain the rationale for the method chosen to the court" and "demonstrate that it is appropriate for the task."

In support of plaintiff's application, plaintiff noted that defendant had not produced a single e-mail in response to prior document demands, and argued that defendant's position that he "did not have custody or control of the requested materials" was without merit, as defendant's non-party book publisher had produced 7,000 pages of documents, including e-mails, sent to and from defendant.

Defendant stated that "most" of the ESI has been lost and more specifically: (1) he had already disclosed all documents that he was able to locate; (2) he had not communicated with plaintiff or particular non-parties by e-mail and, as to other e-mails, he did not save them for long after he read them so a computer search for same would not be productive; (3) his book publisher has "all pertinent documents" and had produced those documents; (4) a computer search would be futile as defendant's computers had crashed, and had been replaced a number of times; and (5) the government had seized his records as part of an investigation.

With respect to the sufficiency of defendant's affidavit, the court held that it was not "sufficiently comprehensive or persuasive about the existence of ESI and/or the ability to recover lost or deleted" ESI, as defendant: (i) did not state that he ever actually conducted a search for the ESI requested, with the court noting that deleted ESI can "often" be retrieved by a forensic expert; (ii) failed to address whether any of the computers that allegedly crashed had been saved or whether an effort to retrieve or transfer any materials had been made or whether backup drives or discs exist; and (iii) failed to review documents produced by his publisher against his own ESI.

The court noted that an affidavit from a computer forensic expert following his examination of and search through defendant's computer "might have alleviated" the above "problems."

Moreover, the court observed that defendant's statements in his affidavit regarding ESI were "not definitive" and used qualifiers like "most" and "generally." As such, plaintiff, using his own expert, was permitted to conduct a search of defendant's ESI.

The court was very pragmatic in addressing the propriety of the keywords selected to be searched, and permitted a search for references to plaintiff's name and another relevant non-parties' names contained in e-mails, without regard to whether e-mails were sent to or from such individuals, noting that such search is "designed to retrieve documents that are material and necessary to the lawsuit, which turns on the interactions between the two parties."

The court found overly broad a search for the ubiquitous last name of "Hudson," in that it would yield hits irrelevant to the action. As a result, the court held that such term on its own should not be searched for and, to the extent relevant, such name should be found in other search results.

Caution should be used when crafting keyword searches to seek to minimize the likelihood they will be found overbroad. Narrowly tailored searches will not only minimize the risk of having to review significant irrelevant information, but guard against an overly broad request being stricken or reduced in a manner that could potentially prejudice the requesting party's litigation strategy.

Further, as the case involved a claim for defamation, a keyword search seeking to determine, inter alia, whether the subject statements were made, notwithstanding defendant's denial that they were not, or for communications relating to such statements, is proper as it goes to, among other things, credibility.

With respect to the above keyword searches, the court found that since they may reveal: (i) confidential information concerning individuals that are not part of the lawsuit and did not receive notice of the motion and are under investigation by the authorities; (ii) information protected by an attorney-client privilege; or (iii) information that would go to the reputation of a non-party and his business, an in camera inspection was therefore required.

As such, the court ordered plaintiff to conduct a search of all available computers through a forensic expert chosen by plaintiff within 45 days, and submit all documents to the court for an in camera review, and simultaneously provide a second set of documents to defendant, who would be afforded twenty days to provide the court with a privilege log.

Further, the court ordered that to the extent the "defendant does not have access to his old computers and did not preserve any ESI or internet copies of material on the computers, defendant shall provide a detailed affidavit describing his search and explaining what measures if any were taken to preserve computers and/or ESI and shall also provide an affidavit by the forensic expert on this subject."

'American Express'

In *American Express v. Badalamenti*,[3] summary judgment on damages was denied due to a failure to submit "evidentiary proof in admissible form" through a supporting affidavit from a person with "personal knowledge of the care and maintenance" of plaintiff's electronic records.

To determine whether the custodian of records affidavit laid a proper evidentiary foundation, the court reviewed, among other statutes, CPLR Rule 4518 (the Business Record Rule) and CPLR Rule 4539(b), as well as state Technology Law §306.[4]

The court found plaintiff's affidavit insufficient where, while it stated that the copies generated in support of the motion were "exact duplicates of the documents delivered to" defendant, it failed to establish "when, how or by whom" the ESI were created, nor did the affidavit set forth whether the record-keeping system permits "additions, deletions or changes without leaving a record" of them, and how plaintiff prevents "tampering or degradation" of the reproduced records.

1. Index No. 106739/2009 (Sup. Ct. N.Y. Co., Feb. 25, 2010).
2. Index No. 110623/2008 (Sup. Ct. N.Y. Co., Aug. 24, 2010).
3. 2010 WL 5186697 (Dis. Ct. Nassau Co., Dec. 21, 2010).
4. CPLR Rule 4518 provides that "an electronic record… shall be admissible in a tangible exhibit that is a true and accurate representation of such electronic record. The court may consider the method or manner by which the electronic record was stored, maintained or retrieved in determining whether the exhibit is a true and accurate representation of such electronic record."

CPLR Rule 4539(b) adds that "[a] reproduction created by any process which stores an image of any writing, entry, print or representation and which does not permit additions, deletions, or changes without leaving a record of such additions, deletions or changes, when authenticated by competent testimony or affidavit which shall include the manner or method by which tampering or degradation of the reproduction is prevented, shall be admissible in evidence as the original."

State Technology Law §306 provides that "[i]n any legal proceeding whether the provisions of the civil practice law and rules are applicable, an electronic record or electronic signature nay be admitted into evidence pursuant to the provisions of [CPLR Article 45] including, but not limited to [CPLR Rule 4539]."

Ganfer & Shore, LLP
360 Lexington Avenue
New York, New York 10017
212.922.9250
mberman@ganfershore.com