New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication

TUESDAY, SEPTEMBER 7, 2010

STATE E-DISCOVERY

Courts Still Wary of Granting Hard Drive Review Requests

By **Mark A. Berman**

Cloning a computer hard drive is a significant tool that should not be overlooked when seeking to uncover electronically stored information (ESI). However, a motion seeking to clone an opposing party's hard drive may likely only be successful upon demonstrating that the information sought could not be obtained any other way.

Courts want more than speculation that the requested ESI would ordinarily have been stored on the hard drive, and may require a substantiated proffer that the failure to voluntarily produce such ESI is due to its unintentional retention or deletion or a more sinister motive.

Cloning to test for the existence of specific ESI may be appropriate where, for instance, there has been a repeated failure to turn over sent e-mails (and, for example, what has been produced were only e-mails received from others); e-mails from a deleted or garbage folder have not been provided; or cause has been shown for the need to examine whether ESI claimed by one side to have been deleted exists in some fashion and/or can be recovered.

While motions seeking to review information stored on a hard drive are being granted more frequently, courts continue to remain circumspect in granting such applications.

Courts are concerned about burden and will not order a wholesale turnover of a hard drive. They will impose limitations to address potential fishing expeditions; privacy concerns as they relate to irrelevant materials; disclosure of competitive materials to ensure that such materials will not be misused; materials protected by the attorney-client privilege, work product immunity doctrine or other privileges; and inconvenience to a non-party owner of a computer. In addition, a court may require a representation that the party requesting the inspection, consistent with New York law, will pay for the costs of the production or review of the hard drive.[1]

iSTOCK

A recent trial court decision on a motion seeking to compel the cloning of a hard drive strongly suggested the need to provide a court with a step-by-step protocol that would address the above concerns, as well as others, when judicial authorization for such a procedure is sought.[2]

Another recent trial court held that a cause of action alleging breach of bailment may encompass the loss intangible information stored on a hard drive.[3]

In *Schreiber v. Schreiber*, plaintiff wife alleged that defendant husband had misrepresented and undervalued his assets and net worth and, in order to prove such allegations, sought "unrestricted turnover" of the hard drive from his law office computer.[4] The husband objected, contending that he had already supplied his wife with the information sought by virtue of an affidavit and through documentary discovery, and characterized the wife's request for inspection of his drive as a "groundless fishing expedition."[5]

After reiterating that in matrimonial actions parties are entitled to disclosure of full financial information concerning marital assets held during the marriage, including both "hard copy and electronically stored data," the court balanced the need for the disclosure of "material and relevant" information with using e-discovery as a "weapon of abuse," commenting that a "computer system or hard drive [is] not a mere thing to produce or copy, which a party has a right to have produced for inspection under CPLR 3120."[6]

Further noting that courts outside the matrimonial context "have been loathe to sanction an intrusive examination of an opponent's computer hard disk drive as a matter of course,"[7] the court found the wife was not entitled to an "unrestricted turnover" of her husband's drive, given that her request was "overbroad as it seeks general—as well as unlimited in time—access to the entirety of [husband's] business and personal data stored on his office computer," with no proposed "discovery/issue resolution protocol."[8]

Accordingly, the court denied the motion with leave to renew, and indicated that upon renewal, such motion should only seek cloning (the original drive would remain in the possession of the husband's counsel), and include a "step-by-stop discovery protocol that would allow for the protection of privileged and private material."[9]

The court suggested that the following areas be included in such protocol and, to the extent possible, they should be agreed upon between counsel:[10]

- **Discovery referee:** An attorney preferably with technical computer expertise;
- **Forensic computer expert:** Expert would execute a confidentiality agreement governing non-disclosure of the contents of the clone;
- **File analysis:** Expert would analyze the clone for evidence of download, installation or use of software that could delete or alter data; extract live files and file fragments; and/or recover deleted files and fragments;

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.*

• **Scope of discovery:** Proposed keyword and other searches conducted by the expert would be subject to a time period for which relevant files or fragments were created and modified;

• **First level of review:** Expert would provide a copy of files and file fragments to opposing counsel for privilege review, and deliver to referee and counsel a report detailing the search results, and indicating evidence, if any, of a data-wiping program;

• **Second level of review:** Within a finite period of time, counsel for the producing party would provide to counsel for the requesting party all non-privileged documents from the extracted files and file fragments in an agreed upon electronic format, along with an appropriate privilege log;

• **Discovery dispute resolution procedure:** Suggestion that the referee's determination on relevance and privilege be final;

• **Cost sharing:** To be borne by requesting party, subject to possible reallocation at the conclusion of the action;

• **Retention of clone:** To remain with the referee until the conclusion of the action.

The court noted that its suggested protocol would seek to achieve the "fundamental goals" of limiting disclosure to relevant documents and preserving applicable privileges.[11]

This decision stands for the proposition that counsel for parties should, at least, discuss and seek to memorialize protocols before engaging in such motion practice, if not specifically include them in any such application, even if they are not all agreed to by counsel. This will help create a pragmatic mechanism for the review and production of ESI and attempt to ensure that court concerns of alleged burdensomeness and the intrusive nature of a request to clone a hard drive are addressed.

Breach of Bailment

The court in *Marchello* held that a breach of bailment cause of action may include "intangible information stored on computer hard drives."[12]

Plaintiff had an oral agreement with defendant for use of its recording studio. When defendant switched from tapes to digital recordings, the studio recommended that plaintiff purchase two hard drives on which to store its music, and which tapes defendant promised to maintain.

Plaintiff temporarily ceased recording music for several years, during which time defendant transferred music made by its "active customers" to a new computer, and deleted the contents of its old computer hard drive that had contained plaintiff's music.

Plaintiff was not advised that defendant was going to delete its music from the studio hard drive, and defendant did not check to see whether plaintiff's two hard drives were in good working order and contained plaintiff's music. When defendant tried to access plaintiff's recordings on plaintiff's two hard drives, one hard drive did not contain the music, and the other permanently crashed.

The court granted plaintiff's motion for summary judgment on its breach of bailment and negligence claims. The court noted that a bailee is responsible for the reasonable value of property lost through its negligence, and since the bailment was gratuitous, the bailee is liable for gross negligence.

The court, however, held that the failure to return the bailed object established a prima facie case of gross negligence. Relying on the New York Court of Appeals decision in *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 832 N.Y.S.2d 873 (2007), which noted that the "tort of conversion[13] must keep pace with the realities of widespread computer use" and includes intangible electronic records, the trial court concluded that "intangible music stored on a hard drive can be subject to a claim of bailment."[14]

> Courts are concerned about burden and will not order a wholesale turnover of a hard drive. They will impose limitations to address potential fishing expeditions, among other privacy concerns.

As such, the court stated that "whether the bailment of the hard drives containing plaintiff's music was gratuitous or for mutual benefit is of no consequence because plaintiff established a prima facie case of negligence through its request for the return of the hard drives containing [the band's] music and defendants' failure to comply."[15]

Conclusion

While courts recognize that ESI contained on a hard drive is appropriately discoverable, if material and relevant, they will require that an appropriate foundation be established in order for a requesting party to be provided with copies of such information, and that safeguards be adopted to ensure that a request for such ESI is not overbroad and unduly burdensome and will not result in the turnover of privileged, irrelevant or confidential material.

Thus, to ensure success when moving to compel disclosure of ESI contained on a cloned drive, counsel for parties should attempt to work together and address protocols upfront that would streamline the review and production process and address the often high costs associated with same.

Further, in addition to the tort of conversion, counsel should consider alleging a breach of bailment cause of action when there has been a loss of electronic data or information.

1. See "Forensic Inspection of Computer Hard Drives Under New York Law," Mark A. Berman, NYLJ, Sept. 1, 2005, at 4, col. 4 (quoted by *Schreiber v. Schreiber*, 904 N.Y.S.2d 886 (Sup. Ct. Kings Co. June 25, 2010)).
2. *Schreiber*, 904 N.Y.S.2d 886.
3. *Marchello v. Perfect Little Productions*, Inc., Index No. 5057/06 (Sup. Ct. Nassau Co. June 15, 2010).
4. *Schreiber*, at 893.
5. Id. at 890.
6. Id. at 890, 891 (citations omitted); see *Etzion v. Etzion*, 7 Misc. 3d 940, 796 N.Y.S.2d 844 (Sup. Ct. Nassau Co. 2005) (permitted mirror imaging of defendant husband's disk drive, but imposed specific limitations and the process was supervised by a referee); *R.C. v. B.W.*, NYLJ, April 23, 2008, at 26, col. 1 (Sup. Ct. Kings Co. 2008) (denied "fishing expedition" into wife's computer where information sought was not limited and "particularly" did "not seek financial documents, records, billing statements or bank statements"); *Byrne v. Byrne*, 168 Misc. 2d 321, 650 N.Y.S.2d 499 (Sup. Ct. Kings Co. 1996) (husband's portable computer kept in the marital residence belonging to husband's employer was "akin to a filing cabinet" and "could be confiscated by [wife] without his consent," and information contained therein regarding "husband's finances and personal business records was discoverable, subject to the attorney-client privilege and any applications for a protective order.").
7. *Schreiber*, at 892.
8. Id. at 893.
9. Id. at 893-94.
10. Id. at 894-95.
11. Id. at 895.
12. *Marchello*, at p. 5.
13. In *New York Racing Ass'n. Inc. v. Nassau Regional Off-Track Betting Corp.*, a trial court also relied on *Thyroff* holding that a party may "maintain an action for conversion where its electronically stored data is misappropriated, regardless of whether plaintiff has been excluded from access to its intangible property." Index No. 021993/09 at 6 (Sup. Ct. Nassau Co. June 14, 2010). The trial court noted that conversion may be predicated upon the "intrinsic value" of information that is stored on the computer and that there was "'very little practical importance whether the tort is called conversion [or unfair competition] because in either case the recovery is for the full value of the intangible right so appropriated.'" Id. (citation omitted) The court concluded that plaintiff "may maintain an action for conversion of its live audio-visual simulcast, even though it was not 'excluded' from access to the electronic data transmission." Id. Thus, although "[defendant's] unauthorized transmission of the simulcast may have been unintended," the court held that it "must give plaintiff the benefit of the possible inference that the simulcast was intentional." Id.
14. *Marchello*, at p. 5.
15. Id.

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