

LITIGATION

Web address: <http://www.nylj.com>

TUESDAY, OCTOBER 10, 2006

In the Mirror Image?

Courts have allowed access to opponent's hard drive only in specific situations.

BY ARTHUR S. LINKER

ACCESSING a "mirror image" of an opposing party's computer hard drive has become an increasingly popular aspect of litigants' discovery plans. Such access raises a number of unique discovery issues. As recent cases demonstrate, courts will only allow such access in a few very specific situations. This article will delineate the ground rules governing attempts to gain access to an opponent's hard drive.

Accessing Data

Data contained on a "hard drive," which is a storage device within a computer, consists of "bits" of information in binary form stored in defined locations (called "sectors") of the hard drive. The computer's operating system software (typically, Microsoft Windows) organizes the data by referencing these sectors to named "files," which are listed in a "directory" maintained by the operating system. When the data contained in a file is accessed through use of an

Arthur S. Linker is a litigation partner with Katten Muchin Rosenman in New York. **Evan Newman**, a Katten summer associate, assisted in the preparation of this article.

application program (such as a word processor or a spreadsheet, database or e-mail program), a text document, spreadsheet or e-mail is displayed, which can be viewed, copied or printed.

Hard drives also contain data that has been left intact, in whole or in part, after files have been modified or "deleted," either in the ordinary course of business or to thwart discovery. Such deleted data "remains...in whole or in part until it is overwritten by ongoing usage or 'wiped' with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer."¹ Often, such "deleted" data, although not accessible using the computer's operating system, can be recovered by forensics experts, either directly from the hard drive, or preferably from a "mirror image" of the hard drive.

"A 'mirror image' is generally described as 'a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space...on a computer hard drive.'" *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, *3 (D. Kan. March 24, 2006). Forensics experts



ART BY NEWS/COM/MICHELE STEINBERG

use specialized software to capture all of the data on the hard drive without altering any of its contents.

Viewed as Document Request

While "electronic documents are no less subject to disclosure than paper records," *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317 (S.D.N.Y. 2003), the real issue is access, either onsite or through a mirror image, to an opponent's entire hard drive. Such access raises concerns regarding relevance, overbreadth, undue burden, privilege and privacy.

While access to a hard drive is sometimes considered to be a form of "inspection" of property, e.g., *Eugene J. Strasser, M.D., P.A. v. Bose Yalamanchi, M.D., P.A.*, 669 So.2d 1142 (Fla. App. 1996), courts usually view a request for such access as a document request, analogizing a hard drive to "an electronic filing

cabinet.” *Menke v. Broward County School Board*, 916 So.2d 8, 10 (Fla. App. 2005). Courts thus ordinarily view requests for wholesale access to hard drives as improper, because, as explained in *Menke*, “we have never heard of a discovery request which would simply ask a party litigant to produce its business or personal filing cabinets for inspection by its adversary to see if they contain any information useful to the litigation. Requests for production ask *the party* to produce copies of the relevant information in those filing cabinets for the adversary.” (emphasis in original) *Id.* Thus, Rule 34 contemplates that the responding party will search for and produce the relevant data; it “does not give requesting party the right to conduct the actual search.” *Floeter v. City of Orlando*, 2006 WL 1000306, *3 (M.D. Fla. April 14, 2006) (quoting *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003)).

Strong Grounds

In light of the extremely intrusive nature of access to an adverse party’s hard drive and overbreadth, privilege and burdensomeness concerns, a request for production of a “mirror image” will be denied absent strong grounds.² Courts require production of a “mirror image” only in certain well-defined circumstances. These include cases where the computer itself allegedly was used to commit the wrong that is the subject of the lawsuit, and those where there is evidence that computer files that should have been but were not produced improperly were deleted or destroyed.

In the recent case, *AutoNation, Inc. v. Hatfield*, 2006 WL 60547 (Fla. Cir. Ct. Jan. 4, 2006), for example, defendant was accused of stealing trade secrets in an attempt to gain a competitive advantage for his probable new employer. Because evidence demonstrated that he had improperly downloaded confidential proprietary information from plaintiff, he was required to produce for examination by a forensic computer expert a computer to which he had sent e-mails, to determine whether those e-mails had been forwarded and whether any other material belonging to plaintiff existed on the computer. Similarly, in *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 (D. Kan. March 24, 2006), an action for copyright infringement, plaintiffs claimed that defendants wrongfully copied digital embroidery designs and then sold the designs to at least one third party. Because the alleged infringement was claimed to have

occurred through use of computers to download copyrighted material, the court found that computer evidence was particularly important, and ordered that all of defendants’ computers be made available for mirror imaging, at plaintiffs’ expense.

Likewise, in *Physicians Interactive v. Lathian Systems Inc.*, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003), plaintiff alleged that defendants hacked its Web site by sending “electronic robots” to steal its customer list, computer code and confidential data. Plaintiffs proffered evidence that defendants launched three “attacks” on its file servers to surreptitiously steal confidential data. The court granted plaintiff limited expedited discovery to enter the premises where the computers used in the alleged attacks were located and to obtain a “mirror image” of the computer equipment containing electronic data relating to the alleged attacks on plaintiff’s file server. See also *Computer Associates International, Inc. v. Quest Software, Inc.*, 2003 WL 21277129, *1 (N.D. Ill. June 3, 2003) (defendants did not dispute having had possession of plaintiff’s source code in copyright infringement and trade secret case, “making it likely that a thorough search of the drives will lead to the discovery of some relevant information”).

In other cases, courts have required production of a “mirror image” where there was an unexplained failure to produce relevant documents, or evidence of improper deletion or destruction of computer files. Thus, in the recent case *Leviton Mfg. Co., Inc. v. Nicor, Inc.*, 2006 WL 1305036 (D. N.M. Jan. 6, 2006), e-mailed documents produced by other parties tended to show that defendant had not produced all responsive documents and he had not offered an excuse for not producing documents that existed. Also, although defendant contended that he had not retained e-mails because his only communications were through the equivalent of a “Hot Mail” account which precluded retention of e-mails, there was evidence that he in fact operated his own Web site to which e-mails were sent. The court therefore ordered defendant to make his computers available for inspection.

In *Etzion v. Etzion*, 7 Misc.3d 940, 943 (Sup. Ct. Nassau Cty. 2005), a matrimonial action, the court granted the wife’s application to clone or copy the husband’s hard drive based on his alleged history of past fraudulent conduct, stating that it was required to insure complete discovery where “it is suggested that some files may have been deleted or altered.” In *Renda*

Marine, Inc. v. U.S., 58 Fed. Cl. 57 (Fed. Cl. 2003), plaintiff was granted access to defendant’s hard drive where defendant admitted that it routinely deleted e-mails even after the lawsuit commenced. In *GTFM, Inc. v. Wal-Mart Stores, Inc.*, 2000 WL 335558 (S.D.N.Y. March 30, 2000), the court ordered defendant to make its computer facilities available for on-site inspection for the purpose of allowing plaintiff’s expert to ascertain whether and how it was possible to extract information about the purchase of trademark-infringing goods, where defendant had misrepresented that its computer system did not maintain the relevant records.³

Mere Suspicion Is Insufficient

Absent “evidence of intentional deletion of data,” courts usually deny requests for discovery of hard drives. *Menke*, 916 So.2d at 12 (access to hard drive denied because “no evidence of any destruction of evidence or thwarting of discovery”).⁴ “[A] party’s suspicion that another party has failed to respond to document requests fully and completely does not justify compelled inspection of its computer systems.” *Bethea v. Comcast*, 218 F.R.D. 328, 329-30 (D. D.C. 2003). In *Bethea*, an employment discrimination case, plaintiff found “incredulous” defendant’s assertion that it had created no documents regarding plaintiff except for a single organizational chart, arguing that she “just can’t believe that an organization of that magnitude could go through a reorganization and would not create one single document” and therefore seeking access to defendant’s hard drives to determine whether there were additional documents that were not produced. (Emphasis in original). The court ruled, “plaintiff is speculating, and such conjecture does not warrant the compelled inspection of a computer system that contains voluminous information relating to many topics other than plaintiff’s employment discrimination claim.” *Id.* at 30.⁵

A recent case illustrates the limitations on the discovery of a “mirror image” that can be imposed by a court in order to ascertain whether relevant documents have been withheld and to prevent a party from pursuing an inappropriate “fishing expedition.” In *Liturgical Publications, Inc. v. Karides*, 2006 WL 931892 (Wis. App. April 12, 2006), plaintiff alleged that defendants, former employees who resigned and began working for a competitor, misappropriated

computer information, programs and data. The court ordered the making of mirror images of defendants' personal and business computers under the supervision of a referee, but limited the inspection of the mirror images to a "hash value search, comparing hash values of materials on the defendants' computers to hash values on [plaintiff's] computers." *Id.* at *5. The court explained that "hash values" were "alphanumeric identifiers of files," *id.* at n.7, i.e., essentially digital fingerprints.

When the hash value search did not result in any matches, plaintiffs sought a second inspection of the mirror images with defined search parameters, including a search for specified words and evidence of various forms of computer activity. The court denied this additional request, finding that the request "essentially amounted to a fishing expedition" and would be unreasonable in light of the negative result of the "hash value" search. *Id.* at *6.

Protocol

An order for imaging of a hard drive that sets "no parameters or limitations" notwithstanding the presence of confidential and privileged information is improper. *Southern Diagnostic Associates v. Bencosme*, 833 So.2d 801, 803 (Fla. App. 2002). When courts grant access to a party's entire computer hard drive, they typically establish or approve a "protocol" to protect the party's privacy and any privileged documents. In *Playboy Enterprises, Inc. v. Welles*, (see endnote 3) an early case establishing such a protocol, the court appointed a neutral expert who would produce a mirror image of the defendant's hard drive. The expert would serve as an officer of the court and any "disclosure" to him of documents on the hard drive would not result in a waiver of the attorney-client privilege. Defendant's counsel would then review any recovered documents, produce those that were responsive

and create a privilege log for any documents withheld on a claim of privilege. Defendant's counsel would be the sole custodian of and would retain the "mirror image" and copies of all retrieved documents. *Playboy*, 60 F.Supp.2d. at 1055.

Most cases have followed this or other similar protocols. In *Balboa*, for example, the court ordered the parties, with the assistance of their respective computer experts, to agree on a search protocol, whether one using key word searches and/or other search procedures, that would adequately protect confidential and irrelevant personal data. *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 at *5.

Who Bears the Expense?

As noted above, in some of the cases in which creation of a "mirror image" was ordered, the requesting party proposed to perform the imaging at its own expense. Generally, however, "the presumption is that the responding party must bear the expense of complying with discovery requests." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978). Courts, however, have developed a fairly uniform set of factors that are employed when considering whether there are grounds to shift the cost of production to the requesting party. The factors include the extent to which the request is specifically tailored to discover relevant information; the availability of such information from other sources; the total cost of production, compared to the amount in controversy and to the resources available to each party; the relative ability of each party to control costs and its incentive to do so; the importance of the issues at stake; and the relative benefits to the parties of obtaining the information. *Zubulake*, 217 F.R.D. at 322. Presumably, these factors may apply in some cases so as to require a requesting party (which otherwise is unwilling to do so) to pay for all or some of the costs associated with imaging.

One court, however, in addressing the cost-shifting issue, held that a producing party's costs for hiring a computer consultant to image hard drives and to search for privileged communications contained in the images so that they could be removed prior to production should not be shifted to the requesting party, because they were "costs of...preventive measures undertaken before the actual disclosure of the information" and were "analogous to the review of documents for privileged information and should not be shifted to the requesting

party." *Computer Associates*, 2003 WL 21277129 at *2.

In sum, litigants seeking access to a "mirror image" of an adversary's hard drive should be prepared to show either that the computer in question was used to commit the alleged wrong or that relevant documents that have not been produced existed and likely were deleted or destroyed. They should also be ready to propose a suitable protocol for imaging using the services of a nonparty expert to limit disclosure to relevant documents and to preserve any applicable attorney-client privilege.

.....●.....

1. "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production," Appendix A at 51 (The Sedona Conference 2004).

2. See, e.g., *BG Real Estate Services, Inc. v. American Equity Ins. Co.*, 2005 WL 1309048, *5 (E.D. La. May 18, 2005) ("request for the entire 'computer hard drive'...is overly broad and seeks much that is irrelevant and not likely to lead to the discovery of admissible evidence"); *Galvin v. Gillette Co.*, 19 Mass.L.Rptr. 380, 2005 WL 1476895, *4 (Mass. Super. May 19, 2005) (state official's request to have access to and search "hard drives (of all computers of Gillette and Gillette personnel)" denied as "nearly impossible to comply with"); *Dikeman v. Mary A. Stearns, P.C.*, 560 S.E.2d 115, 117 (Ga. App. 2002) (request to produce full and complete copy of hard drive denied because "overbroad, oppressive, and annoying and to require undue burden and expense").

3. See also *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) ("mirror image" ordered to permit plaintiff at its own expense to attempt to recover deleted files, based on showing of "some troubling discrepancies with respect to defendant's document production"); *Playboy Enterprises, Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D. Cal. 1999) ("mirror image" ordered to attempt to recover deleted files where defendant produced very few e-mails or hard copies of computer files and admitted that it was her custom and practice to delete e-mails); *Alexander v. F.B.I.*, 186 F.R.D. 78, 96 (D. D.C. 1998) (discovery of nonparty witness' hard drive granted where his conduct in deleting files prior to receiving subpoena was "highly unusual and suspect" in light of pending government investigation).

4. See also *Floeter*, 2006 WL 1000306 at *3 (denied where no showing that plaintiff requested information contained on hard drive that defendant failed to produce); *Williams v. Mass. Mutual Life Ins. Co.*, 226 F.R.D. 144, 146 (D. Mass. 2005) (denied where plaintiff "provided no reliable or competent information to show that [d]efendants' representation [regarding completeness of production]...are misleading or substantively inaccurate"); *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 169 (S.D.N.Y. 2004) ("widespread destruction or withholding of relevant information" not shown); *Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc.*, 2003 WL 1809465 (N.D. Ill. April 4, 2003) (denied where there was no evidence of withholding of or tampering with evidence).

5. See also *McCurdy Group, LLC v. American Biomedical Group, Inc.*, 9 Fed.Appx. 822, 831 (10th Cir. 2001) (mere skepticism that adverse party produced all relevant and nonprivileged documents from hard drives was insufficient to warrant "drastic discovery measure" of physical inspection of hard drives); *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 533 (1st Cir. 1996) ("mere speculation" that document was fabricated after its ostensible date was insufficient to require forensic examination of hard drive to attempt to determine creation date of file).

