

The Jurisprudence of Hard Disk Inspections: Protection by Protocol

By Adam I. Cohen and Gina A. Dombosch

[Editor's Note: Adam I. Cohen is a partner with David J. Lender and Gina A. Dombosch is an associate in the litigation department of Weil, Gotshal & Manges LLP. Mr. Cohen is the co-author of the treatise *Electronic Discovery: Law and Practice*, published by Aspen Publishers. Copyright 2004 by the authors. Replies to this commentary are welcome.]

Hard disks represent a tantalizing potential source of discovery because information computer users intended to “delete” often can be recovered from hard disks through computer forensics techniques. Accordingly, it should come as no surprise that several judicial opinions have issued exploring hard disk inspections as a discovery mechanism. Federal courts have derived their authority to order these inspections from the Federal Rules of Civil Procedure. Rule 26(b) permits a party to obtain discovery of relevant information “reasonably calculated to the lead to the discovery of admissible evidence” so long as the respondent is not subjected to undue burden, expense or invasion of privileged matter.ⁱ Rule 34 governs the scope and procedure for the production of documents, specifically, subsection (1) allows a party to copy and inspect the documents and things of another party.ⁱⁱ

In denying discovery requests for hard disk inspections, courts have cited the absence of protocols or safeguards to address confidentiality and evidentiary concerns associated with unbridled access to original digital media. Furthermore, access to a hard disk typically will be refused where the request is based on mere suspicion that relevant information might be uncovered. As more fully discussed below, hard disk inspection guidelines have emerged from recent judicial opinions.

Antioch

The District Court of Minnesota recently addressed the issue of a request to copy and inspect a hard disk in a copyright infringement case, *The Antioch Co., v. Scrapbook Borders, Inc. et. al.*ⁱⁱⁱ Antioch sought an order compelling the production of computer equipment for inspection by a court-appointed computer forensics expert.^{iv} Antioch argued that since data “deleted” but recoverable from the computer might be irretrievably overwritten by continued use of the equipment, a court order was appropriate to maximize preservation and recovery.^v Antioch offered to bear the costs of this discovery.^{vi}

Noting that the Federal Rules of Civil Procedure clearly state that electronic data is discoverable and indicating that a party has an obligation to search available electronic systems for information requested in discovery, the court found that deleted information on the defendants’ computer equipment might be relevant and discoverable.^{vii} In connection with Antioch’s request for the appointment of a neutral expert in computer forensics to search the defendants’ hard disks for information responsive to Antioch’s requests, Antioch proposed two alternative procedures to be implemented after the data was retrieved: (a) the expert would forward the responsive documents to both parties marked “Attorneys’ Eyes Only;” the defendants would have ten days to review the information and assert any privilege; Antioch would be required to return any document subject to a privilege claim and the defendants would include the information on a privilege log; and, any dispute regarding a claim of privilege would be submitted to the court for resolution; or (b) the experts would submit all data and information found on the hard disks responsive to Antioch’s requests to the defendants, who would have ten days to review the documents and produce all responsive, non-privileged documents to Antioch and provide the court with any privileged documents for *in camera* inspection; and, any documents which were deemed to be non-discoverable would be returned to the experts, who would maintain a privilege log.^{viii}

In considering Antioch's proposals, the court reviewed prior decisions which addressed such hard disk inspection "protocols,"^{xix} including *Welles* and *Simon*, which are discussed in more detail *infra*.^x The court then fashioned its own protocol as an amalgamation of the protocols set forth in *Welles* and *Simon* as follows: (1) Antioch will select an expert of its choice in the field of computer forensics to produce a "mirror image" of the defendants' hard disks; (2) the defendants will then make available to the expert, at their place of business and at a mutually agreeable time, their computer equipment subject to the request for inspection; (3) within ten days of the inspection/imaging, the expert will provide the parties with a report as to what equipment was produced and the actions taken by the expert, including a detailed description of each piece of equipment inspected, copied or imaged as well as documentation of the chain of custody for any copies or images drawn from the equipment; (4) the expert will then produce two copies of the resulting data from the hard disks – one for the defendants and one for the court; (5) thereafter, defendants will sift through the data provided by the expert to locate any relevant information; (6) defendants will then produce to Antioch all properly discoverable information, as well as a sufficiently detailed privilege log to enable Antioch to assess the applicability of any privileged claimed by defendants; and lastly (7) defendants will forward the privilege log to the court for potential *in camera* review of any entries and corresponding documents which Antioch may dispute.^{xi}

In addition, the court directed the expert to use best efforts to avoid unnecessarily disrupting the normal activities or business operations of the defendants.^{xii} The court also ordered that no one other than the expert should inspect or handle the equipment, particularly no employee or counsel of Antioch.^{xiii}

Welles and Simon

The *Antioch* protocol may be viewed as a combination of the protocols implemented by the courts in *Simon* and *Welles*.^{xiv} *Welles* involved Playboy's claims against a former playmate of the month for trademark infringement, dilution of trademark and unfair competition in connection with the defendant's allegedly unauthorized use of Playboy and Playmate trademarks throughout her website.^{xv} Playboy requested access to defendant's personal computer's hard drive to make a "mirror image" of the disk and have defense counsel review recovered e-mails for production of relevant and responsive information.^{xvi} The request was made after Playboy learned that defendant had a "custom and practice" of deleting e-mails shortly after they were sent and received even if these e-mails were requested for production by Playboy.^{xvii}

The court held that the need for the requested information outweighed the burden on the defendant and set forth a detailed protocol to govern the inspection:^{xviii} (1) Playboy was directed to provide the court with sufficient evidence that recovering deleted e-mails was a likely result of the exercise and that defendant's computer would not be damaged by the procedure,^{xix} (2) the court would then appoint a computer expert to create a "mirror image" of defendant's hard disk and such access would not constitute any waiver of privilege asserted by the defendant; (3) the parties would agree to a day and time to access the defendant's computer with deference given to defendant's schedule; (4) the "mirror image" of the hard disk would be given to defendant's counsel for review and production of relevant and responsive information and to log privileged documents.^{xx} The court provided the parties approximately one month to complete the procedure.^{xxi}

In *Simon*, the plaintiff similarly requested that defendant make certain computers available for inspection in order to recover deleted files.^{xxii} The court found that the basic structure adopted by the court in *Welles* offered the best approach, but modified the *Welles* protocol as follows: (1) plaintiff would select and pay an expert to inspect the computers and create a "mirror image" of the hard disks (defendant would have an opportunity to object to plaintiff's selection; the court would deem whatever

expert was ultimately selected an officer of the court); (2) the expert would provide in convenient form to defendant's counsel all available word processing documents, e-mails, powerpoint or similar presentations, spreadsheets and similar files, and would copy only those files reasonably likely to contain potentially relevant material; (3) defendant's counsel would then review for privilege and responsiveness and supplement discovery responses and privilege log accordingly.^{xxiii} The court further directed the expert to sign the protective order and retain the mirror images until the end of the litigation, at which time the records would be destroyed.^{xxiv}

Other "Protocol" Decisions

Other decisions have provided further examples of hard disk inspection protocols. In *Northwest Airlines v. Local 2000*, Northwest requested discovery of employees' home and office computer hard disks in an action brought by the airline against the unions and 20 flight attendants for declaratory, injunctive relief and damages after an alleged organized "sick-out" forcing Northwest to cancel 317 of its flights during the peak holiday season.^{xxv} The Magistrate Judge issued an order requiring all defendants to allow Ernst & Young access to their office and home computers to copy information and communications on the hard disks "discussing, concerning or relating to" the alleged sick out.^{xxvi} The court set forth the following protocol: (1) E&Y would create mirror images of the hard disks and employ electronic search terms to search for relevant information; (2) E&Y would turn over any relevant information to the defendants so they could determine whether any of it should be withheld as privileged; (3) any remaining non-privileged documents would then be produced to Northwest.^{xxvii}

In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, an action involving claims for discrimination and anti-competition, the Magistrate Judge proposed a more lenient protocol.^{xxviii} In fact, the court expressed the protocol as a set of guidelines which could be modified by the parties. The *Rowe* protocol was set up as follows: (1) the plaintiff was allowed to designate one or more experts, however, the defendants would have an opportunity to object to any expert designated; (2) plaintiffs would formulate search procedures for identifying responsive e-mails, to which defendant would have the opportunity to object; (3) the ultimate search method would be implemented by the experts who would first create mirror images of any hard disks or back-up tapes containing e-mails; (4) the experts would be bound by any confidentiality order entered in the case; (5) plaintiffs' counsel would ultimately review the documents elicited by the experts on an "attorneys' eyes only" basis and provide responsive e-mails to defendants' counsel in hard copy form.^{xxix}

Recently, the Eastern District of Texas set forth protective protocols in connection with requests to access a corporate defendant's servers and hard drives.^{xxx} In *In re: Triton*, the plaintiffs requested access to Triton's servers and hard drives along with those of all present and former members of the Board of Directors and to allow non-destructive testing of the systems to determine what documents and e-mails had been deleted.^{xxxi} Plaintiff supported its request with deposition testimony of former directors who testified that they were not asked to retain or produce any documents in connection with the litigation and any emails sent or received regarding the witness' involvement at Triton were automatically deleted after one year.^{xxxii} Nevertheless, the court would not grant unfettered access to Triton's hard drives, finding that such access would "potentially violate Triton, its employees and outside directors' right to privacy and privileges."^{xxxiii} The court appointed a computer forensics expert to retrieve, and a special master to review, the information retrieved from the computers in question.^{xxxiv} The computer expert was permitted to conduct non-destructive testing of the systems to determine what documents and e-mails, if any, had been deleted. The special master was then to review and identify relevant electronic data and submit a report for the court's review and determination of whether Triton complied with its disclosure obligations.^{xxxv}

There are a number of cases in which the courts have denied discovery requests to inspect, access or copy an adversary's computer hard drive.^{xxxvi} The courts have denied these requests on the grounds that the moving party was unable to show noncompliance with discovery requests, thus, the inspection would be tantamount to a "fishing expedition" and/or that the party's requests were overbroad, burdensome, and too drastic a remedy.^{xxxvii} Courts have also denied these requests because there were no protocols set forth in connection with the inspection and thus, no safeguards were implemented to prevent harm to the computer systems or address the confidentiality and privilege concerns of the respondent.^{xxxviii}

Conclusion

Critics of hard disk inspection have argued that it reverses the traditional process of discovery whereby a party first reviews its own information and documents before it is turned over to an adversary. Courts have addressed these criticisms of hard disk inspections by establishing protocols whereby a computer forensics expert extracts all potentially relevant data from a party's hard drive and provides them an opportunity to remove objectionable information that should not be produced. Parties have a legitimate interest in protecting confidential, proprietary and privileged information which may be found in the digital information of their hard disks. The courts have ameliorated most of these concerns by fashioning proper protocols which address both the risks and burdens associated with such discovery requests.

ⁱ Fed. R. Civ. P. 26 (b)(1); see also *Simon Prop. Group L.P v. my Simon, Inc.*, 194 F.R.D. 639, 640-641 (S.D. Ind. 2000); *Playboy Enters. Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053-1054 (S.D. Cal. 1999).

ⁱⁱ Fed. R. Civ. P. 34(a).

ⁱⁱⁱ *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002)

^{iv} *Id.* at 650.

^v Antioch submitted two affidavits of computer forensics experts who attested to this fact. *Id.* at 650-651. In addition, Antioch pointed to the fact that the defendant was proceeding *pro se* (and thus might not have a complete understanding regarding discovery obligations) and potentially going out of business. *Id.* at 650.

^{vi} The issue of who should bear the cost of electronic discovery has been the subject of a separate body of jurisprudence. See *Electronic Discovery: Law and Practice*, Chapter 5 by Adam I. Cohen and David J. Lender (Aspen Law and Business).

^{vii} *Id.* at 652.

^{viii} *Id.* at 651.

^{ix} Some courts have granted discovery requests for access to hard drive information without enunciating detailed protocols. See *Hayes v. Compass Group USA, Inc.*, 202 F.R.D. 363 (D. Conn. 2001); *GTFM, Inc. v. Wal-Mart Stores*, WL 335558 (S.D.N.Y. Mar. 30, 2000).

^x See *Simon*, 194 F.R.D. 639; *Welles*, 60 F. Supp 2d 1050.

^{xi} *Id.* at 653-654.

^{xii} *Id.* at 653.

^{xiii} *Id.*

^{xiv} *Welles*, 60 F. Supp. 2d 1050; *Simon*, 194 F.R.D. 639 (S.D. Ind. 2000).

^{xv} *Welles*, 60 F. Supp. 2d at 1051.

^{xvi} *Id.*

^{xvii} *Id.*

^{xviii} *Id.*

^{xix} The courts have seemed to routinely consider whether any “damage” will result from the inspection and copying requests – perhaps a cautionary tale resulting from *Gates Rubber Co. v. Bando Chemical*, where a technician overwrote 7-8 percent of a computer hard drive when unnecessarily copying a software program for purposes of retrieving deleted information. 167 F.R.D. 90 (D. Col. 1996). The information contained in the 7-8 percent of the hard drive was irretrievably lost to the parties.

^{xx} *Id.* at 1055.

^{xxi} *Id.*

^{xxii} *Simon*, 194 F.R.D. at 640-1.

^{xxiii} *Id.* at 641-642.

^{xxiv} *Id.* at 642.

^{xxv} *Northwest Airlines, Inc. v. Local 2000 et al.*, No. Civ. 00-08 (DWF/AJB) (D. Minn. Feb. 2, 2000); See David Rubenstein, “*Northwest Union Dispute Raises Internet Privacy Issue; Routine Discovery or Anti-Business Precedent?*” Corp. Legal Times, May 2000, 23

^{xxvi} *Id.*

^{xxvii} *Id.*

^{xxviii} 205 F.R.D. 421 (S.D.N.Y. 2002), *aff’d*, 2002 Dist. LEXIS 8308 (S.D.N.Y. May 9, 2002)

^{xxix} *Id.* at 433.

^{xxx} *In re: Triton Energy Limited Securities Litigation*, 2002 WL 32114464 (E.D. Tx. March 7, 2002)

^{xxxi} *Id.* at *2.

^{xxxii} *Id.* at *5.

^{xxxiii} *Id.* at *6.

^{xxxiv} *Id.*

^{xxxv} *Id.* In the event the Court would ultimately find that Triton had not met its obligations, the plaintiff could look to decisions by courts in *Lauren Corp v. Century Geophysical* and *Minnesota Mining & Mfg. Co v. Pribyl*, where negative inference inferences or presumptions at trial were ordered and upheld as appropriate sanctions for the destruction of computer hardware despite the

unavailability of the evidence to demonstrate how it would support the claims at issue. *Lauren Corp v. Century Geophysical*, 953 P. 2d 200 (Colo. Ct. App. 1998); *Minnesota Mining & Mfg. Co v. Pribyl*, 259 F. 3d 587 (7th Cir. 2001).

^{xxxvi} See *Bethea v. Civ. Action Comcast*, 2003 U.S. Dist. LEXIS 21595 (D.D.C. Dec. 3, 2003); *McCurdy Group, LLC v. American Biomedical Group, Inc.*, 2001 WL 536974 (10th Cir. 2001); *Lawyers Title Insurance Corporation v. United States Fidelity & Guaranty Company*, 122 F.R.D. 567 (N.D. Ca. 1988); *Fennell v. First Step Designs, Ltd*, 83 F.3d 526 (1st Cir. 1996); *Van Westrienen v. American Continental Collection*, 189 F.R.D. 440 (D. Oregon 1999).

^{xxxvii} See *Civ. Action Comcast*, 2003 U.S. Dist. LEXIS 21595 at *4; *American Biomedical*, 2001 WL 536974 at *7; *United States Fidelity & Guaranty Company*, 122 F.R.D. 567 at 570.

^{xxxviii} See *First Step Designs, Ltd*, 83 F.3d 526 at 532-534; *American Continental*, 189 F.R.D. 440 at 441.