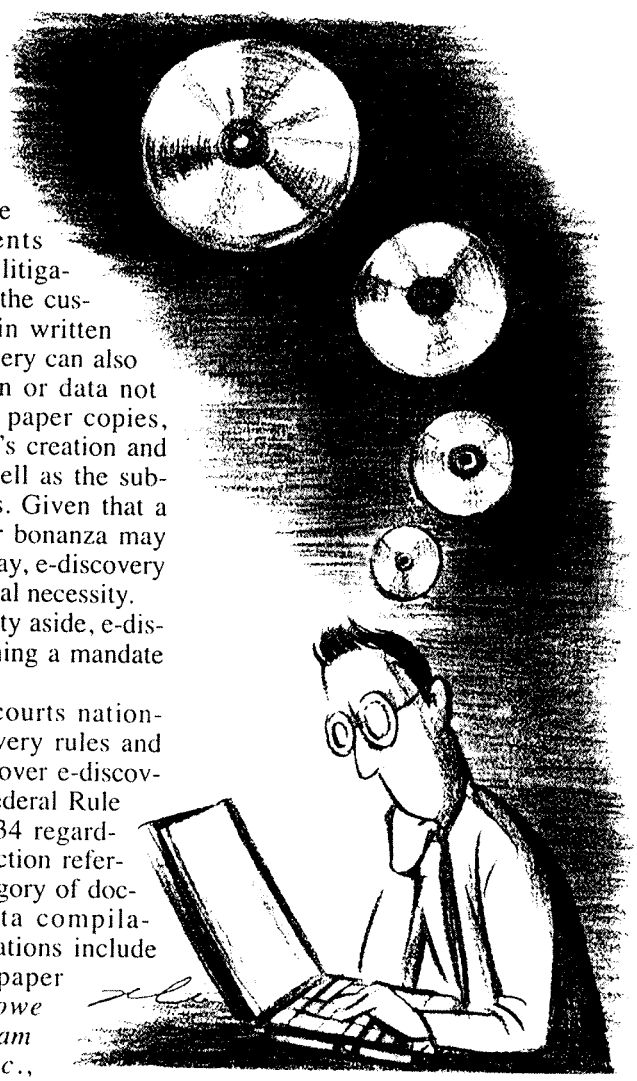
E-Ignorance Is No Excuse

Counsel must not only know the rules of electronic discovery, but understand how clients store and retrieve data

By Douglas S. Brierley and Vaughn R. Klug

With almost all corporate documents created electronically, and with eight or more out of ten corporate documents stored electronically, lawyers in the computer age can hardly be surprised that electronic data has become a routine source of documents and information in litigation. In addition to the customary text found in written documents, e-discovery can also provide information or data not found in "hard" or paper copies, such as a document's creation and revision dates, as well as the substance of prior edits. Given that a litigation liability or bonanza may be just an e-mail away, e-discovery has become a practical necessity.



Practical necessity aside, e-discovery is fast becoming a mandate in the courts.

In the federal courts nationwide, pretrial discovery rules and case law generally cover e-discovery. For example, Federal Rule of Civil Procedure 34 regarding document production references a catchall category of documents: "other data compilations." Such compilations include e-data as much as paper documents. See *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 428 (S.D.N.Y. 2002). Case law has also held that e-data may be discoverable even if hard copies of information have been produced. See *Anti-Monopoly, Inc. v. Hasbro*, No. 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355, at *1 (S.D.N.Y. Nov. 3, 1995). Correspondingly, the current version of FRCP 26 mandates initial disclosures that must include, according to the 1993 Advisory Committee notes, "computerized data and other electronically-recorded information." See *In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. 437, 440-41 (D.N.J. 2002).

In New Jersey, however, the federal district court adopted in October 2003 Local Civil Rule 26.1(d) that expressly requires discovery of digital information.

Under subsection 1 of the rule, and even before the requisite "meet-and-confer" session with the adversary, counsel and client must together review the client's computer-based and other digital information management systems to understand how the information is stored or may be retrieved, what digital evidence may be used to support claims or defenses, and who among the client's personnel knows the most about the client's information management system. As can be readily discerned, Local Civil Rule 26.1(d)(1) effectively presumes, at a minimum, that attorneys are sufficiently versed in high-tech recordkeeping to recognize and inquire about the potential location of e-data sources, such as laptops, individual desktops, hard drives, the increasingly popular personal digital assistants (e.g., Blackberries, Palm Pilots), back-up tapes or media with archival data, and the like.

In the meantime, the local rule also expects counsel to identify the categories of information to be sought, whether e-mail, spreadsheets, or other data. Counsel should notify the opponent accordingly. L. Civ. R. 26.1(d)(2).

Upon assembly by the parties of the above preliminary information, Local Civil Rule 26.1(d)(3)(a) directs the parties to meet and confer not only to exchange what discovery and information that they have gathered, but also to agree on such matters as the preservation and production of digital information, inadvertent production of privileged information, restoration of deleted digital files, and the format in which digital information may be

---

Brierley is a partner at Schenck, Price, Smith & King, and co-chair of the firm's Investigations and Audit Practice Group; Klug is a third-year law student at the Emory University School of Law. An extended version of this article first appeared in The Morris Lawyer, *a publication of the Morris County Bar Association, and is reprinted with permission.*

delivered. Counsel must also address cost issues referable to preservation, production, and restoration, if any, of e-data. L.Civ.R. 26.1(d)(3)(b). For a perceptive discussion of recent developments in the District of New Jersey, see Robert E. Bartkus, *E-Discovery: New Jersey Update*, Jan. 31, 2005 [179 N.J.L.J. 425].

Nationalization of E-Discovery Mandate

To remedy the assorted e-discovery challenges posed in federal court, as well as the conspicuous lack of express guidance provided in the FRCPs themselves in navigating the unique e-discovery process, the federal judiciary's Judicial Conference Advisory Committee on the FRCP proposed on Aug. 15, 2000, certain amendments to the federal rules that relate to electronic discovery. Not to be implemented before December 2006, these proposed rule changes effectively nationalize and either supplant or supplement not only New Jersey's Local Rule 26.1, but also the e-discovery provisions found in similar "cutting-edge" districts that had adopted e-data rules on their own.

More specifically, FRCP 26(f) would be amended to require parties to address in their initial meet-and-confer session disclosure of discovery issues referable to electronically stored information, the format of such a disclosure, preservation/spoliation of information (inclusive of e-data), and agreements to protect against privilege waiver.

Because the volume of e-stored information can be "staggering" and the subject of a variety of storage and maintenance options, the Committee proposes amending Rule 26(b)(2) to permit a responding party to object to a discovery request for e-data by showing the data is "not reasonably accessible" unless good cause requires otherwise. Rule 26(b)(5) would be amended to respond to privilege problems, including inadvertent production of privileged information. The Committee's proposed revision of this rule would further allow post-production assertion of privilege and require the return, sequestration, or destruction of the subject information until overall resolution of the privilege dispute. Notably, the proposed Rule 26(b)(5) extends beyond e-data to all documents and things and does not address whether the privilege has been waived.

The Advisory Committee additionally proposes to amend Rule 33 by defining "business records" to include "electronically stored information" and thereby allowing a party to refer in its interrogatory responses to e-stored information as readily as to other types of business records. The proposed Rule 34 would distinguish "document" from "electronically stored information" and require the requesting party to specify whether the discovery request seeks documents, e-stored information, or both. The final rule amendment on e-discovery offered the Advisory Committee describes in Rule 37 a narrow safe harbor to protect a responding party from discovery sanctions for failing to preserve or produce e-stored information destroyed or altered by routine operation of the party's computer system.

Some experienced practitioners welcome the federal judiciary's proposed rules as a viable means to handle and control the minefield of e-discovery issues confronting the court and bar alike. Other astute observers, while not doubting the effort to address such issues, question the substance of the proposed changes and the introduction of new standards for courts to decide whether certain e-information must be produced or withheld. See, e.g., Gregory P. Joseph, *Electronic Discovery I*, Nat'l L.J., Oct. 4, 2004, at 12; *Electronic Discovery II*, Nat'l L.J., Dec. 6, 2004, at 16, in which the author probes, among other points, the need to adapt the new standard of "reasonably accessible" in deciding whether a party may object to a discovery request

Continued on page S-27

E-Ignorance Is No Excuse

Continued from page S-11

for e-stored information, as well as the advisability of distinguishing between "documents" and "electronically stored information" in the proposed Rule 34. See also Editorial, *E-Discovery*, 178 N.J.L.J. 1126 (Dec. 20, 2004) (examining the "safe harbor" provision proposed in the amendment to FRCP 37).

At an early stage, counsel seeking e-data should also consider in what format the documents should be requested.

Regardless of whether the specific amendments proposed by the Advisory Committee will be adopted, no one can doubt that rule amendments of some sort dealing with e-discovery will be adopted and thereby affect all federal court practitioners. See Pamela A. MacLean, *Electronic Discovery Is In Flux*, Nat'l L.J., Jan. 17, 2005, at 1. And there can be little doubt that the New Jersey Supreme Court and its Civil Practice Committee will consider similar problems and rule amendments for guidance in our state courts. Thoughtful calls for such deliberation on the state level have already begun. Editorial, *E-Discovery*, Dec. 20, 2004 [178 N.J.L.J. 1126].

In light of these inevitable rule changes dealing with e-discovery, what's an attorney to do?

A few practical suggestions may be helpful.

• When confronted with a case in which discovery requests for and responses with e-data can be anticipated, an attorney should consult an expert and develop a viable plan tailored to the particular litigation so that any e-information may be collected, analyzed, categorized, and produced in a systematic, efficient, and economical manner. Consultants have been known to provide such valuable assistance that one court went so far as to order adversaries to consult a litigation support firm specializing in e-discovery. *In re Lorazepam & Clorazepate Antitrust Litig.*, 300 F.Supp.2d 43, 47 (D.D.C. 2004); Jason Krause, *Don't Try This At Home — Doing E-Discovery Is Best Left to Outside Experts*, 91 A.B.A.J. 59 (March 2005); Carole Longendyke, *Data Forensics Investigations — What You Don't Know Can Hurt You*, Feb. 28, 2005 [179 N.J.L.J. 883]

• At an early stage, counsel seeking e-data should also consider in what format the documents should be requested: would a hard copy of the e-data suffice for the client's purposes, or does there exist a preference for electronic review in "native format" so as to gain access to embedded metadata (data on data), which reveals the document's preparation and revision dates, as well as the substance of any prior edits? Compare *Medical Billing Consultants, Inc. v. Intelligent Med. Objects, Inc.*, No. 01 Civ. 9148, 203 U.S. Dist. LEXIS 5606, at *7 (N.D. Ill. Apr. 4, 2003) (refusing on-site inspection of the other side's computer because "[s]uch a physical inspection is likely to unduly burden [the producing party] without leading to the

Continued on next page

E-Ignorance Is No Excuse

Continued from preceding page

discovery of otherwise unobtainable relevant evidence."), with Paul G. Lewis, *Data Forensics: The Smoking Gun May Be a Click Away*, N.J. Lawyer Mag., Aug. 2004, at 41-45.

• Furthermore, counsel seeking e-data should also ponder the scope and location of the requested e-information. Barring special considerations to the contrary, the e-information requested should usually be limited to that of key persons or machines. When possible, requests should be narrowed further to those documents containing certain search terms. Target sources and e-information that you have a sound belief will contribute to resolution of significant issues. The requesting party should strive to confine its demand by asking for data within a particular "file cabinet" rather than "any and all e-information" without limit.

Should you adopt the 'any and all' approach, both you and your client may be exposed to sanctions and possible violations of privacy laws may result.

Should you adopt the "any and all" approach, you and your client may be exposed to sanctions and possible violations of privacy laws may result. See, e.g., *Theofel v. Farey-Jones*, 341 F.3d 978, 986-87 (9th Cir. 2003) (insisting on "all e-mails sent or received by anyone ... with no limitation as to scope" was "massively overbroad," corruptive of the federal rules, violative of the Stored Communications Act, 18 U.S.C. §§ 2701-2712, and the Computer Fraud & Abuse Act, 18 U.S.C. § 1030, and sanctionable in the amount of $9,000 in attorneys' fees).

• Similar factors affect the attorney representing the responding or producing party. In advising the client, always assume that the responding party is likely to find itself before a court explaining its production techniques. Mindful of this assumption, the attorney should make sure the client has or institutes a formal document retention policy that will not only ease the production of any digital information requested, but also shield potentially discoverable information from destruction. See The Sedona Conference Working Group, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production 21* (2004); *Danis v. USN Communs., Inc.*, No. 98 Civ. 7482, 2000 U.S. Dist. LEXIS 16900, at *96-97 (N.D. Ill. Oct. 20, 2000) (reciting "[t]he obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers").

• Thereafter, analyze the document request to determine what kind of information is sought and the date ranges and custodians to cover; determine how and where the information is stored; review the collected data for relevance and privilege; produce the data in an acceptable format; and never allow an opponent free access to the client's digital files, as such access poses a security risk and could raise the specter of spoliation. For a discussion about forensic data collection and the potential for spoliation, see *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216-19 (S.D.N.Y. 2003) (noting possible use of "mirror image" copies in conjunction with other steps to meet preservation obligations), and *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 167 F.R.D. 90, 101-02 (D. Colo. 1986) (failure to make a byte-by-byte mirror image prior to viewing data may result in spoliation accusation).

Evidence of spoliation may give rise to sanctions, including an adverse inference instruction and a monetary award. See *Mosaid Techs. Inc. v. Samsung Elecs. Co.*, 348 F.Supp.2d 332 (D.N.J. 2004) (in finding the duty to preserve potentially relevant evidence as one a party may not shirk, the court determined the data producer's actions warrant a spoliation inference jury instruction and the award of $566,839.97 in monetary sanctions).

• Another important consideration is the cost associated with the production of e-information. The fear of excessive e-discovery costs may be all too real a factor in forcing litigants to settle. See *Proposed Rules on E-Discovery Debated; Cost of Discovery Cited as Prod to Settlement*, 73 U.S.L.W. 2405-406 (Jan. 18, 2005). If a request for e-information seems overly broad, consider offering a sample of a small number of hard drives, servers, and tapes prior to producing the entire universe of information sought: that limited production may well demonstrate both how irrelevant most of the requested e-information is and how much more productive and cost-effective a narrower request would be. See *Theofel*, 341 F.3d at 981, where the producing party provided a sample of 339 e-mail messages mostly unrelated to the litigation, thereby establishing the unreasonableness of a request for "any and all e-mails."

Navigating the seas of electronic discovery can be a daunting task. To be successful under today's current or contemplated court rules, however, gaining a firm grasp of e-discovery is a challenge no wise attorney will avoid any longer. ■