Avoiding E-Discovery Heartburn

By Dante Stella

Late in the life of a commercial case, just before the close of discovery, opposing counsel calls to ask whether your client produced documents from a specific source of electronically stored information (ESI). ESI had never come up before, and though you told your client to issue a litigation hold to preserve evidence, you have no idea whether (or how) the client executed the hold or searched the data. Hanging up, you feel uneasy about what could hit if the data is gone: a discovery motion, sanctions for spoliation, or an adverse jury inference. You have, after all, been reading the horror stories.

It is possible to reduce ESI anxiety by effectively managing electronic discovery: being proactive in defining the scope, understanding preservation obligations and protections, and taking reasonable steps calculated to protect potentially relevant information (PRI). A good first step is reading the article on electronic discovery under the Federal Rules of Civil Procedure by Derek S. Witte and D. Andrew Portinga in the March 2007 *Michigan Bar Journal*.[1] With that as background, you can work on conquering the uncertainties of electronic discovery.

Proactively Managing Information Issues

ESI discovery is expensive and complicated. Often, the best thing that comes out of it is *nothing*. But simply letting ESI issues ride risks even more trouble and expense. Parties to a case in a Michigan state court can (and should) proactively discuss key ESI questions:

- Will ESI come into play to a significant degree?
- What ESI will be preserved?
- How will ESI be searched and what date, divisional, organization, and geographic limitations will apply?
- How will ESI be produced?
- What, if anything, will be necessary to authenticate ESI for trial?

The time for these inquiries is at the beginning—not months into discovery, on the day a computer fails, or when backup systems

FAST FACTS

It is best to resolve the scope of discovery of electronically stored information at the outset of a case, using mechanisms provided by the Michigan Court Rules.

It is important to understand the difference between the "safe harbor" provision for discovery sanctions and the law of spoliation.

You can take practical steps to limit exposure to discovery or spoliation sanctions.

become hopelessly overloaded. If the parties can agree on the answers, they can put the judicial seal on ESI agreements. One way is to incorporate an ESI agreement into a scheduling order using MCR 2.401(B)(2)(c). Although circuit courts often issue "stock" scheduling orders, MCR 2.401(B)(2)(a) allows more than one order to be entered. A second avenue is a protective order under MCR 2.302(C) (also useful for opponents who will not cooperate). A third is MCR 2.501(A)(1)(d), the catchall rule for pretrial orders.

Understanding Preservation Obligations

Because ESI-related risks cannot always be eliminated up front, it is important to understand obligations for preserving evidence and "safe harbors" in discovery. Duties to preserve relevant evidence (and sanctions for failure to do so) are independent of the Michigan Court Rules. Under Michigan common law, the duty to preserve arises when a party has notice of the information's relevance to litigation or impending litigation.[2] Unfortunately, notice is often examined in hindsight, and Michigan law provides little, if any, bright-line guidance on when a preservation obligation arises. Federal courts analyzing the issue examine things like

(a) knowledge that a suit will be filed,[3]

(b) investigation of a possible claim by a plaintiff's attorney,[4]

(c) prelitigation correspondence or prelitigation discussions between counsel,[5] and

(d) filing of an administrative claim.[6]

Federal courts have also held that amending a pleading to include additional allegations does not create retroactive notice where it would not have existed before.[7] Once a party has notice, that party must preserve PRI. Failure to do so can constitute spoliation, punishable by sanctions within the "inherent powers" of a Michigan trial court,[8] tailored to remedy the loss of "material and relevant evidence."[9] Michigan courts are instructed to "den[y] the party the fruits of the party's misconduct, but…not interfere with the party's right to produce other relevant evidence," and sanctions may include exclusion of certain evidence or adverse jury instructions.[10] In more extreme cases, sanctions that end the lawsuit (like summary disposition or default judgment) may be on the table.[11]

The Michigan Court Rules now provide a limited safe harbor—but only from sanctions based on a violation of discovery orders. Effective January 2009, the Michigan Supreme Court amended MCR 2.302(B)(5) and MCR 2.313(E). MCR 2.302(B)(5) now provides:

> A party has the same obligation to preserve electronically stored information as it does for all other types of information. *Absent extraordinary circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.* [Emphasis added.]

MCR 2.313(E) contains identical language but omits the first sentence. This safe-harbor language is identical to FR Civ P 37(e). The new Michigan safe-harbor provisions should be understood as narrow and applicable when discovery has been compelled and a party ordered to produce ESI comes up empty-handed. Despite superficial similarities between spoliation sanctions and discovery sanctions (similar stated purpose, discretionary application, and remedies), the Michigan Court of Appeals has specifically recognized the difference between discovery sanctions and spoliation sanctions[12] and therefore the inapplicability of the safe harbor to claims of spoliation. Furthermore, the safe-harbor provisions hinge on taking "reasonable" precautions.

First, in *Brenner v Kolk,* the Michigan Court of Appeals explicitly distinguished spoliation sanctions from discovery sanctions under MCR 2.313. The *Brenner* plaintiff disposed of key evidence years before filing suit. The trial court reacted by granting summary disposition to the defendant. The Court of Appeals reasoned that MCR 2.313 did not apply because it required a violation of a court order[13] but upheld the result on grounds that spoliation sanctions derive from the trial court's "inherent powers."[14] In 2009, the Michigan Court of Appeals, albeit in an unpublished decision, reiterated this point as it relates to newly amended MCR 2.313(E).[15] The *Brenner* Court also made it clear that sanctions issued under "inherent powers" are discretionary.[16] Because interlocutory appeals on sanctions are rarely if ever granted—and because abuse of discretion is a highly deferential standard of review—sanctions can be effectively immune from appeal unless and until the final judgment itself is appealed.

In the federal rules, the limited nature of the safe harbor in FR Civ P 37(e) is clarified by the advisory committee notes stating that "[t]he protection provided by Rule 37[e] applies only to sanctions 'under these rules.' It does not affect other sources of authority to impose sanctions or rules of professional responsibility." The extra statement in MCR 2.302(B)(5) that "[a] party has the same obligation to preserve electronically stored information as it does for all other types of information" changes nothing. Preservation obligations arise at common law, and court rules have always addressed ESI, at least with a broad brush, by discussing "data compilations…[in]…reasonably usable form."[17]

Second, the standard of behavior is different. Under the law of spoliation, *some* corrective measure may result from *any* loss of unique, relevant data,[18] while the federal and Michigan safe harbors involve a standard of care: "routine, good-faith operation."[19] The latter clearly rules out the extraordinary, intentional destruction

of evidence—which is never routine or in good faith—but leaves the question of what constitutes "good faith." The staff comment to the amendments of MCR 2.302(B)(5) and 2.313(E) (which is *not* the official position of the Michigan Supreme Court[20]) states that "[g]ood faith may be shown by a party's actions to attempt to preserve information as part of a 'litigation hold' that would otherwise have been lost or destroyed under an electronic information system." The advisory committee notes to the federal rules lay out a standard most similar to that used for negligence:

(a) A party may not exploit the automatic operation of a data system to destroy information it has a duty to preserve;

(b) depending on the circumstances, a party may have the duty to intervene to prevent the automatic destruction of data;

(c) safe harbor applies only to information lost as a result of routine operations, which include "the alteration and overwriting of information, often without the operator's specific direction or awareness….";

(d) factors in determining "good faith" include "the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information"; and

(e) a party's duty to take steps to prevent loss of information from sources designated as "not readily accessible" under FR Civ P 26(b)(2) depends on the circumstances of each case. "One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources."[21]

One federal commentator notes that the good-faith standard is embryonic and will require additional development.[22] The same should be understood to be the case under the state rule.

Identify custodians early and do not be afraid to concentrate more intensive preservation on key players, i.e., those closest to the action.

Taking Precautions to Prevent Discovery and Spoliation Sanctions

The spoliation doctrine is concerned with *results,* but the safe-harbor language in the Michigan Court Rules measures *efforts.* Satisfying either standard can be difficult because companies cannot simply shut down when litigation commences or is threatened.[23] The federal advisory committee stated in its submission notes that the federal safe harbor

> recognizes that all electronic information systems are designed to recycle, overwrite, and change information in routine operation, not because of any relationship between the content of particular information and litigation, but because they are necessary functions of regular business operations. The proposed rule also recognizes that suspending or interrupting these features can be prohibitively expensive and burdensome, again in ways that have no counterpart in managing hard-copy information.[24]

The good-faith component of the safe harbor requires reasonable steps to head off preventable losses of PRI while the parties (sometimes with judicial "assistance") resolve the scope of discovery. Reasonable steps, if actually effective, can also minimize the risk of claims of spoliation. And whatever steps you take, record what has been done and why.

Issuing a Litigation Hold Memo

A prompt litigation hold is often the most valuable tool for preventing user-initiated or automatic loss of PRI. Litigation holds can contain simple or ornate descriptions of the subject matter of the data to be preserved, and their distribution can be focused or company-wide. But in every case, the recipients should include any known custodians, relevant business unit managers (who can inform subordinates), and information technology staff, who may even have prearranged procedures in place for holds.

Identifying People and Systems with Responsive Information

Preserving, processing, and reviewing data from users and systems with no connection to a case is needlessly expensive, but casting the net too narrowly risks discovery or spoliation sanctions. Identify custodians early and do not be afraid to concentrate more intensive preservation on key players, i.e., those closest to the action.

Making Best Efforts to Retain Relevant, Preexisting Backups

There is no general requirement that parties keep every single byte of every single data backup, but parties may be obligated to preserve backups if (1) they can identify where in the backups particular employees' data would be stored, (2) the backups contain the key players' data, and (3) the relevant information is not otherwise available from readily accessible sources.[25] Although parties often designate backups "not readily accessible" under MCR 2.302(b)(6)

and therefore make them presumptively nondiscoverable, backups may come into play when discovery problems arise with current, readily accessible data. One potential (albeit expensive and extreme) solution is to preserve all existing backups. But if data volumes or backup methods make this impossible, a reasonable course of action is to do what is possible in the near term, based on present knowledge of the case, and adjust the scope as internal investigations progress.

Suspending System-Wide Automatic Deletion of E-mail

Systems that automatically delete e-mail after a certain time might circumvent litigation holds. Federal decisions suggest that if such deletion continues after the duty to preserve arises, attendant data loss is outside the safe harbor in the discovery rules.[26] Auto-delete rules, if they pose a threat, should be deactivated for personnel potentially holding PRI until that PRI is captured or evaluated.

Avoiding Changes to Data Retention Practices During Litigation

Litigation holds serve as *exceptions* to record-retention policies, and record-retention policies should not be instituted or modified during litigation when doing so risks destroying PRI.[27] Likewise, your client should not change practices with regard to on-server retention of "deleted messages" or allow custodians to engage in "cleanup" activities during litigation.[28]

Closely Monitoring Leases, Redeployments, and Reloads

Lease turn-ins, redeployment of equipment to other employees, and "reloading" of malfunctioning computers can result in data-loss situations outside the safe harbor. Information technology personnel should be made aware of which personnel are subject to litigation holds, and before any extraordinary activity, the contents of the affected persons' hard drives should be preserved (if possible).

Watching Departing Employees' Data

On an employee's departure, many organizations start a countdown to deleting that user's data (e-mail and files) from local computers and servers. When identifying personnel with PRI, do not ignore departed employees—and as soon as they are identified, capture any surviving data associated with them.

Conclusion

Under the new Michigan Court Rules, as under the old, the best way to manage the risks of sanctions associated with e-discovery is cooperation to define its scope. Absent mutual agreement or a court order, risks associated with the loss of electronic data can be managed by taking steps that are both calculated to achieve—and actually result in—the preservation of PRI. ■

Dante Stella is a member in Dykema's Business and Commercial Litigation group, heads Dykema's national electronic discovery practice, is co-chair of the firm's Discovery Management group, and co-manages Dykema-Lumen Discovery Management Services, a joint venture devoted to discovery cost containment in complex litigation. Stella routinely addresses government investigations (DOJ, FBI) and other cases involving large-scale data issues. He also advises Fortune 500 companies on their day-to-day data practices.

FOOTNOTES

1. Witte & Portinga, *E-discovery and the new Federal Rules of Civil Procedure: They apply to you*, 86 Mich B J 36 (March 2007).
2. See, e.g., *Bloemendaal v Town & Country Sports Ctr, Inc*, 255 Mich App 207, 212; 659 NW2d 684 (2002); *MASB-SEG Prop Cas Pool, Inc v Metalux*, 231 Mich App 393, 400; 586 NW2d 549 (1998); *Brenner v Kolk*, 226 Mich App 149, 162; 573 NW2d 65 (1997).
3. See, e.g., *Dillon v Nissan Motor Co*, 986 F2d 263, 266–269 (CA 8, 1993); *Struthers Patent Corp v Nestlé Co*, 558 F Supp 747, 765 (D NJ, 1981); *Alliance to End Repression v Rochford*, 75 FRD 438, 440 (ND Ill, 1976).
4. *Headley v Chrysler Motors Corp*, 141 FRD 362, 362–363 (D Mass, 1991).
5. *Computer Assoc Int'l v American Fundware, Inc*, 133 FRD 166, 169 (D Colo, 1990); *Wm T Thompson Co v Gen Nutrition Corp*, 593 F Supp 1443, 1446 (CD Cal, 1984).
6. *Byrnie v Town of Cromwell*, 243 F3d 93, 107–108 (CA 2, 2001); *Couveau v American Airlines, Inc*, 218 F3d 1078, 1084 (CA 9, 2000).
7. *Stephenson v United States*, 37 Fed Cl 396, 405–406 (1997).
8. *Bloemendaal*, 255 Mich App at 211; *Persichini v William Beaumont Hosp*, 238 Mich App 626, 638–640; 607 NW2d 100 (1999).
9. *Martinez v Gen Motors Corp*, unpublished opinion per curiam of the Court of Appeals, issued May 15, 2007 (Docket Nos. 26612 and 267218), available at 2007 WL 1429632; see also *Brenner*, 226 Mich App at 160.
10. *Id.* at 161.
11. *Bloemendaal*, 255 Mich App at 215.
12. *Brenner*, 226 Mich App at 158–159.
13. See MCR 2.313(B)(2).
14. *Brenner*, 226 Mich App at 156–160.
15. *Gillett v Mich Farm Bureau*, unpublished opinion per curiam of the Court of Appeals, issued December 22, 2009 (Docket No. 286076), available at 2009 WL 4981193, at *1.
16. *Brenner*, 226 Mich App at 160–161.
17. MCR 2.310(A)(1).
18. *Hamann v Ridge Tool Co*, 213 Mich App 252, 255; 539 NW2d 753 (1995); *Brenner*, 226 Mich App at 162.
19. MCR 2.302(B)(5); MCR 2.313(E); FR Civ P 37(e).
20. MCR 1.101, staff comment; see also *People v Grove*, 455 Mich 439, 456; 566 NW2d 547 (1997).
21. Order adopting amendments of the Federal Rules of Civil Procedure, 234 FRD 219, 243–244 (December 1, 2006) (excerpts from December 2004 federal advisory committee notes).
22. See 8B Wright & Miller, Federal Practice & Procedure (3d ed), §2284.1.
23. *Lorraine v Markel American Ins Co*, 241 FRD 534, 580 (D Md, 2007).
24. Order, 234 FRD at 282 (excerpts from September 2005 federal advisory committee notes).
25. See *Forest Laboratories, Inc v Caraco Pharmaceutical Laboratories, Ltd*, unpublished opinion of the United States District Court for the Eastern District of Michigan, entered April 14, 2009 (No. 06-CV-13143), available at 2009 WL 998402, at *5, citing *Zubulake v UBS Warburg LLC*, 220 FRD 212, 218 (SD NY, 2003).
26. *Disability Rights Council of Greater Washington v Washington Metro Transit Auth*, 242 FRD 139, 145–146 (D DC, 2007); *Pandora Jewelry LLC v Chamilia LLC*, unpublished memorandum opinion of the United States District Court for the District of Maryland, entered September 30, 2008 (No. CCB-06-3041), available at 2008 WL 4533902, at *8–9.
27. *Rambus, Inc v Infineon Techs, AG*, 220 FRD 264, 281 (D Va, 2004).
28. See *Technical Sales Assoc v Ohio Star Forge Co*, unpublished order of the United States District Court for the Eastern District, entered March 19, 2009 (Docket Nos. 07-11745 and 08-13365), available at 2009 WL 728520.