RISE OF THE MACHINES
How Ethical Mistakes in E-Discovery Can Terminate Your Case

BY Jason B. Tompkins

The computer's invasion of businesses and homes, coupled with ever faster technological development has obviously changed the way we practice law. A recent estimate indicates that more than 90% of all corporate information is electronic and less than 1% of all communication will ever appear in paper form. *See* Harvey L. Kaplan, "Electronic Discovery in the 21st Century: Is Help on the Way?", 733 PLI/Lit 65, 67 (2005). E-discovery is now standard practice for litigators in both state and federal courts, yet it has emerged and advanced so quickly that many attorneys are scrambling to catch up. In fact, in late 2006, the Federal Rules of Civil Procedure were amended to provide uniform ground rules for the discovery of Electronically Stored Information ("ESI").[1] Although many of the ethical rules that govern attorneys' behavior have not changed, their application in e-discovery may take some lawyers by surprise. Indeed, an attorney's failure to comply with ethical obligations in the context of e-discovery has the potential to impact the outcome of the litigation as much as the actual merits of the case.

Several rules of professional conduct[2] are particularly important (and easily violated) in the context of e-discovery:

Rules 1.1 and 1.3: Competence and Diligence

Rules of Professional Conduct 1.1 and 1.3, respectively entitled "Competence" and "Diligence," permeate almost everything that we, as lawyers, do. Read together, these rules require that a lawyer (1) provide competent representation – *i.e.*, "the legal knowledge, skill, thoroughness and preparation reasonably necessary" – and (2) "not willfully neglect a legal matter entrusted to him." These few words hold a myriad of pitfalls for e-discovery, any one of which could lead to catastrophic results. For instance, in e-discovery, preservation is frequently more critical than production issues. Unless clients and their employees know about the duty to preserve, data may be lost forever or become very expensive to retrieve. Depending upon the client's backup policies and email retention rules, data loss can occur almost immediately. If data loss occurs, then in the best case, one may be in the unenviable position of proving a negative (that the e-discovery would not have included relevant information) or of explaining the confusing computer architecture.

In the worst scenario, one's case may suffer fatal blows. In *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004), for example, the court gave an adverse inference instruction to the jury and imposed costs on the defendant based upon both the client's failure to preserve relevant emails and *the attorney's* failure to ascertain the client's electronic storage methods and to ensure the client retained relevant data. The jury awarded the plaintiff over $29 million. The court noted that an attorney's obligations go beyond simply issuing a litigation hold: "Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." Accordingly, for competent and diligent representation, it is imperative that a lawyer familiarize himself with a client's system to ensure that relevant documents are preserved when litigation is reasonably foreseeable.

In fact, often a lawyer should meet directly with a client's IT managers to determine how the computer systems handle email retention; whether backups exist; how electronic data can be preserved; and how individuals may deviate from these practices. In turn, an attorney should meet with individual key witnesses to ascertain the extent to which they keep their own "stash" of electronic documents. In *Zubulake*, one of the errors that the court specifically identified was the attor-

ney's failure to learn that one key employee kept a document archive on her individual computer. 229 F.R.D. at 435.

Once an attorney has properly ensured preservation of ESI, e-discovery does not become much less treacherous. One of the most common pitfalls in handling electronic discovery is inadvertently altering client electronic files through improper copying methods. Normally, one should not copy and paste files, and individual files should not be opened. Doing so typically alters the "date created" and "date modified" fields, and may alter the metadata fields and date macros as well. One way to avoid such issues is to create a full forensic bit stream image, using tools such as Encase. Another possibility is a non-bit stream image – called ghosting – using products such as Norton Ghost. In addition, programs such as Microsoft Robocopy – part of the administrative tool bundle of Microsoft Windows NTs 2000 XP Resource Kit – allow the user to copy selected data.

Other potential pitfalls abound in e-discovery: corrupt data tapes, which can sometimes be restored although it is expensive and time consuming; fragile tapes which can deteriorate over time if not properly stored; tapes missing mapping data, especially if the backups roll over from one tape to another, which may require piecing together the data; complex programs such as GroupWise which stores attachments in separate places within a single database and usually requires converting emails to PST files in order to view them.

As these examples demonstrate, e-discovery is dangerous territory, and a lawyer's obligations to represent his client competently and diligently require more than just knowledge of the law.

Rule 1.6: Confidentiality

Confidentiality is the hallmark of the attorney-client relationship; thus, Rule 1.6 prohibits a lawyer from "reveal[ing] information relating to representation of a client" absent certain enumerated exceptions. Confidentiality problems may arise very easily from the inadvertent disclosure of documents in an immense electronic production or from the disclosure of the information attached to electronic documents. Recognizing the increased danger of inadvertent disclosure when dealing with voluminous electronic discovery, lawyers and parties sometimes use "clawback" and "sneak peek" agreements.[3] Such agreements are "designed to protect the parties, who face massive discovery obligations, from having to litigate the issue of inadvertence." *Prescient Partners, L.P. v. Fieldcrest Cannon, Inc.*, 1997 WL 736726, at *4 (S.D.N.Y. Nov. 26, 1997). These are good options for avoiding the potentially staggering cost of a detailed privilege review for voluminous e-discovery, but given differing degrees of acceptance,[4] a wise attorney will seek judicial approval of any non-waiver agreement, including its incorporation into a case management order, protective order, or pretrial order. In fact, Federal Rule of Civil Procedure 16 expressly provides that parties' agreements may be included in a scheduling order.

A recent amendment to the Alabama Rules of Professional Conduct imposes duties on attorneys who *receive* privileged information. Rule 4.4(b), amended on June 23, 2008, provides:

> A lawyer who receives a document that on its face appears to be subject to the attorney-client privilege or otherwise confidential, and who knows or reasonably should know that the document was inadvertently sent, should promptly notify the sender and
> (1) abide by the reasonable instructions of the sender regarding the disposition of the document; or
> (2) submit the issue to an appropriate tribunal for a determination of the disposition of the document.

The Federal Rules similarly provide guidance regarding inadvertent disclosure. Federal Rule of Evidence 502, which President Bush signed into law on September 19, 2008, expressly protects (at least to some extent) inadvertent disclosures made in federal proceedings or to federal officers or agencies. For a detailed discussion of Rule 502, see Greg Cook & Patrick Runge, "Waive Goodbye to Waivers, Say Hello to Rule 502," in this issue of *Birmingham Bar Association Bulletin*.

Perhaps the most dangerous confidentiality problems, however, can arise from "metadata" – information about a particular set of data which "can describe how, when and by whom ESI [electronically stored information] was collected,

created, accessed, modified and how it is formatted." *The Sedona Conference Glossary: E-Discovery and Digital Information Management (Second Edition)* 33 (The Sedona Conference, Dec. 2007 Version), *available at* http://www.thesedonaconference.org/content/miscFiles/TSCGlossary_12_07.pdf. Such information could reveal client confidences and secrets, litigation strategy, editorial comments, legal issues raised by the client, and other confidential information.

Last year, the Alabama State Bar issued an ethics opinion in which it addressed the disclosure and mining of metadata. *See* R0-2007-02, *available at* http://alabar.org/ogc/PDF/2007-02.pdf. The opinion made clear that attorneys have a duty under Rule 1.6 "to use reasonable care when transmitting electronic documents to prevent the disclosure of metadata containing client confidences or secrets." "Reasonable care" will be evaluated by the steps taken to prevent metadata disclosure, the nature and scope of the metadata revealed, the subject matter of the document, and the intended recipient. On the other side of the coin, the opinion also noted the *receiving* attorney's ethical obligation to refrain from mining an electronic document for metadata, which would constitute "an impermissible intrusion on the attorney-client relationship" in violation of Rule 8.4.

Some courts, however, have held that parties must provide metadata along with electronic discovery submissions. *See, e.g., Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005) (holding that a party must produce documents with metadata intact when asked to provide documents in their native format); *In re Payment Card*, 2007 WL 121426 (E.D.N.Y. Jan. 12, 2007) (implying requirement to produce all metadata); *but see Kentucky Speedway, LLC v. NASCAR*, 2006 WL 5097354 at *7 - *8 (E.D. Ky. Dec. 18, 2006) (no requirement to produce metadata absent need; "general presumption against the production of metadata"). Metadata may sometimes be relevant and material. For example, metadata may be vital to determining who authored a document, who made certain accounting decisions, or when a particular person received an email. Thus, when providing documents in native format, an attorney must carefully balance his or her obligation to produce relevant non-privileged metadata with his or her obligation to protect confidential metadata. This only deepens the ethical pitfalls associated with e-discovery. Recognizing this, the Alabama State Bar ethics opinion recommended that "[b]oth parties . . . seek direction from the court in determining whether a document's metadata is to be produced during discovery."

Rule 3.3: Candor Toward the Tribunal

Rule 3.3 provides, in relevant part, that "[a] lawyer shall not knowingly: (1) make a false statement of material fact or law to a tribunal; (2) fail to disclose a material fact to a tribunal when disclosure is necessary to avoid assisting a criminal or fraudulent act by the client; or (3) offer evidence that the lawyer knows to be false." Some of the most costly e-discovery mistakes have occurred in cases where a party provided inaccurate information to the court regarding the e-discovery. For example, in *Coleman (Parent) Holdings v. Morgan Stanley & Co.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), Morgan Stanley made a false certification that discovery was complete even though it knew electronic documents were still outstanding. Based upon the certification and Morgan Stanley's discovery failures, the court gave a multi-page adverse inference instruction to the jury, which ultimately awarded the plaintiff $1.45 billion, $850 million of which was punitive. The jury verdict was subsequently overturned because Coleman failed to prove compensatory damages by not establishing the fraud-free value of the stock on the date of the transaction. *Morgan Stanley Co., Inc. v. Coleman (Parent) Holdings, Inc.*, 955 So. 2d 1124 (Fla. Dist. Ct. App. 2007).

The danger of violating this rule also appears when one argues that ESI is not "readily accessible." On a practical level, the litigator may need to explain why the costs are undue. The Advisory Committee Notes to the Federal Rules of Civil Procedure provide several examples of data that might not be reasonably accessible. Presumably this list is not exhaustive and may change based upon the amount in controversy and the type of computer architecture. The Advisory Committee Notes state that when an objection is made, the court might want to collect additional information by "requir[ing] the responding party to conduct a sampling" or "allow[ing] some form of inspection" of the computer system or allowing the requesting party to "tak[e] a deposition."

The Alabama Supreme Court has recently

discussed the question of what is accessible and who should have to pay if inaccessible data is required. In *Ex parte Cooper Tire*, 987 So. 2d 1090 (Ala. Oct. 26, 2007), the Supreme Court embarked on a detailed discussion of federal caselaw on discovery including many of the leading federal cases. Ultimately the Court applied a multi-factor test from *Wiginton v. CB Richard Ellis, Inc.*, 229 F.R.D. 568, 573 (N.D. Ill. 2004) as stating the appropriate test to be applied in determining whether the defendant should be required to comply with the plaintiff's extensive discovery requests. The Court adopted the *Wiginton* test for both the breadth of appropriate discovery and whether the costs associated with production of the requested information should be shared by the requesting party.

The remaining scattered case law that has developed appears to focus more upon the "good cause" issue than the "reasonably accessible" issue. That is, the courts appear to find that the data is not reasonably accessible based upon the cost to retrieve, but the dispute is whether good cause has been shown. *E.g.*, *PSEG Power New York, Inc. v. Alberici Constructors, Inc.*, 2007 WL 2687670, 2007 U.S. Dist. LEXIS 66767 (N.D.N.Y. Sept. 7, 2007); *Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority*, 242 F.R.D. 139 (D.C. 2007). When the responding party has done something to make e-discovery more difficult or if the court has reason to doubt the truthfulness of the producing party, courts are usually more willing to order production. *See, e.g.*, *Benton v. Dlorah, Inc.*, 2007 WL 3231431 (D. Kan. Oct. 30, 2007) (responding party deleted emails (some before litigation); court ordered production of hard drive for forensic analysis by requesting party's expert; court made no distinction between accessible and inaccessible).

Rule 3.4: Fairness to Opposing Party and Counsel

According to Rule 3.4, "[a] lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act." To comply with Rule 3.4, an attorney must give his opponent unobstructed access to evidence and preserve discoverable documents and data when litigation is pending or reasonably anticipated. Courts emphasize cooperative efforts in e-discovery and will penalize parties that engage in "purposeful sluggishness," such as producing multi-page TIFF images, no bates numbering, producing files that can only be opened with very powerful workstations, or failing to conduct appropriate key word searches. *E.g.*, *In re Seroquel Products Liability Litigation*, 2007 WL 2412946 (M.D. Fla. Aug. 21, 2007).

This rule became more prominent with the recent revisions of the Federal Rules of Civil Procedure. Rule 26 now requires parties to meet and develop a discovery plan that includes discussion about the proper scope of e-discovery. The initial meeting should cover (if applicable) the scope and method of preserving ESI that will not disrupt day-to-day business operations and "any issues relating to preserving discoverable information." Scope could include: (1) how long to preserve; (2) how far back into the past; (3) whether to include electronic documents created in the future; (4) how many departments or employees to include; (5) what type of electronic documents to include; (6) whether to include backup tapes, hard-drives, old computers, flash drives; (7) how to preserve (tape and other types of backups can be corrupted); and (8) whether to agree to an abbreviated privilege log system.

Litigators have debated whether to raise the litigation hold issue during the Rule 26 conference. They reason that no obligation exists to share the content and date of the litigation hold – especially if not requested by the opponent. There is, of course, no one size fits all solution in litigation; however, most authorities strongly encourage such discussion. The attorney client privilege and/or the work product doctrine seem to protect the litigation hold directives issued by counsel. *E.g.*, *Gibson v. Ford Motor Co.*, 510 F. Supp. 2d 1116, 1123 (N.D. Ga. 2007); *Rambus, Inc. v. Infineon Technologies AG*, 220 F.R.D. 264 (E.D. Va. 2004). Nonetheless, the *fact* of a litigation hold, and the fact of its scope is probably not protected.

The initial meeting may also involve the discussion of appropriate search terms for electronic information. Given an attorney's obligation to protect confidential information, when discuss-

ing search terms, one must carefully balance the obligation to inform opposing counsel of potential sources of information with the prohibition on revealing adverse facts. Courts recognize the value of search terms to electronic documents and will take steps to ensure they are used. In *Tessera, Inc. v. Micron Tech., Inc.*, 2006 WL 733498 (N.D. Cal. Mar. 22, 2006), for example, the court's order actually provided search terms to the parties. In *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 (D. Kan. Mar. 24, 2006), the court ordered an uncooperative plaintiff to suggest appropriate search terms.

Moreover, the failure to use appropriate search terms can be disastrous. The case of *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008), provides an example where counsel's failure to ensure that particular search terms were used led the court to find several ethical violations.[5] In that case, Qualcomm sued Broadcom to enforce two patents, both of which involved the H.264 video coding standard developed by an industry group called the Joint Video Team ("JVT"). An important issue at trial was *when* Qualcomm became involved in the JVT. Any involvement before the H.264 standard was released would result in Qualcomm's waiver of the patents. Naturally, Broadcom requested all materials relating to Qualcomm's participation in the JVT. Qualcomm took the position that it did not become involved in the JVT until September 2003, well after the H.264 standard was released. However, while preparing for trial, one of Qualcomm's attorneys discovered 21 emails, dated November 2002, which discussed issues related to the H.264 standard. Qualcomm did not produce them. Qualcomm later identified tens of thousands of documents that "revealed facts that appear[ed] to be inconsistent with arguments" made at trial.

The jury found that Broadcom had not infringed the patents. A magistrate judge subsequently ordered Qualcomm to pay over $9 million in attorneys' fees in addition to a final fee award of $8.5 million. The court was particularly troubled by the ease with which Qualcomm ultimately discovered 46,000 unproduced documents – by using basic search terms such as "JVT," "H.264," and the name of the email distribution list. The attorneys were faulted for filing a motion for summary judgment and making arguments at trial without conducting a reasonable inquiry into the e-discovery production.

Rule 5.3: Responsibilities Regarding Nonlawyer Assistants

The employment of non-legal ancillary services is not new to the practice of law, but the provision of e-discovery services has exploded in recent years. First and foremost, a lawyer must supervise the third-party vendor to ensure that it does not violate the Rules of Professional Conduct. Naturally, the attorney will want to ensure that the client's confidences are protected during the process, and that any property of the client is kept safe, as required by Rule 1.15. One should not only supervise the actual document review services for which the vendor was hired, but also the vendor's communications with the client, if any. A non-lawyer vendor's advice to a client that a document is or is not relevant or privileged arguably borders on unauthorized practice of law, which Rule 5.5 requires all attorneys to police. Many of these issues are discussed in ABA Formal Op. 08-451, issued on August 5, 2008.

An attorney may also run into problems when he regularly recommends a preferred vendor to clients. Not only does Rule 5.3 still come into play, but the lawyer risks violation of Rules 1.7 ("A lawyer shall not represent a client if the representation of that client may be materially limited by the lawyer's responsibilities to another client or to a third person, or by the lawyer's own interests.") and 1.8 ("A lawyer shall not enter into a business transaction with a client or knowingly acquire an ownership, possessory, security or other pecuniary interest adverse to a client unless," among other things, the lawyer fully discloses any interest he or she has.). Though Rule 1.7 is generally applied to more egregious cases,[6] and Rule 1.8 is intended to regulate business enterprises between lawyer and client, both rules are broad enough to be implicated by one's relationship with a third-party vendor. Finally, ABA Formal Opinion 93-379, which Alabama adopted, *see* Opinion No. 2004-02, *available at* http://www.alabar.org/ogc/fopDisplay.cfm?oneId=64, explains the limitations on an attorney's billing for third-party services.

The well-publicized withdrawal of the prominent law firm of Boies, Schiller & Flexner from the recent Adelphia matter illustrates some

of the dangers of using third-party vendors without ensuring all ethical obligations are upheld.[7] Boies Schiller employed a document management company to provide discovery services in the Adelphia matter. No senior member of the firm, including David Boies, had any direct interest in the company. However, several members of the Boies family had indirect interests through a series of investments. Most prominently, David Boies' son was the largest investor in an entity that owned 50% of the majority owner of the discovery management company. In addition, several Boies Schiller lawyers had indirect interests in a document reproduction company employed by the firm. When media reports began to surface about the relationships, Adelphia requested that Boies Schiller withdraw from representation.

E-discovery is a powerful tool for able litigators, yet it presents great risk for lawyers not well versed in technological nuances. In fact, e-discovery creates a much more dangerous ethical terrain, where a single misstep can cause an avalanche of issues that were inconceivable in traditional discovery. Review the rules, stay abreast of technological advances in document retention and production, and secure your footing.

Endnotes

1. There is a clear indication that Alabama is also considering adopting e-discovery rules. *See, e.g.*, George M. Dent, "Discovery of Electronically Stored Information – Potential Alabama Civil Procedure Rules", 69 Ala.Law. 106 (March 2008) (chair of rules committee soliciting comments on the Uniform Rules Relating to the Discovery of Electronically Stored Information ("URRDESI") and noting with approval that Dean Carroll of Cumberland Law School was reporter for URRDESI). Dent explains that the URRDESI parallel almost all of the 2006 Federal Rules amendments, but contemplate that e-discovery will not occur in every action in Alabama courts. Nonetheless, under the rules, the parties would be required to confer on the matter within 21 days after a defendant files its initial response. *See also Ex parte Cooper Tire*, 2007 WL 312813 (Ala. Oct. 26, 2007) (first Alabama Supreme Court opinion to discuss in detail e-discovery issues).

2. All quotations are from the Alabama Rules of Professional Conduct, available at http://alabar.org/ogc/ropc.cfm.

3. Clawback agreements allow parties to agree beforehand that the inadvertent disclosure of a privileged document will not constitute waiver and that the receiving party will return or destroy any inadvertently produced privileged information. Sneak peek agreements, on the other hand, provide that one's opposing counsel may review a document library and request production of specified segments. The producing party then reviews only the specified documents for privilege. The problem, of course, is that one's opposing counsel has then likely already seen some privileged information.

4. Courts generally enforce clawback agreements so long as reasonable pre-production review takes place. *See, e.g., In re Southeast Banking Corp. Secs. & Loan Loss Reserves Litig.*, 212 B.R. 386, 394 (S.D. Fla. 1997). Courts are split on whether a clawback agreement provides protection for different degrees of culpability in producing privileged information (i.e., negligent, grossly negligent, reckless). *See, e.g., VLT Corp. v. Unitrode Corp.*, 194 F.R.D. 8, 12 (D. Mass. 2000) (holding that clawback agreement would protect negligent disclosure but not grossly negligent disclosure); *cf. Prescient Partners*, 1997 WL 736726, at *4 (stating that the clawback agreement protected disclosure "unless the production was 'completely reckless'") (citation omitted).

5. The case is currently on remand for the attorneys to have an opportunity to refute some of Qualcomm's declarations. The opinion nonetheless illustrates the ethical dangers of e-discovery.

6. *See, e.g., Bezold v. Ky. Bar Ass'n*, 134 S.W.3d 556 (Ky. 2004) (counsel slept with client).

7 Many commentators identify Model Rule 7.2 as the one implicated in the Adelphia matter. Model Rule 7.2(b)(4) provides that "a lawyer may refer clients to . . . a nonlawyer professional pursuant to . . . [and the nonlawyer professional may] refer clients or customers to the lawyer, if . . . the client is informed of the nature and existence of the [reciprocal referral] agreement." Although Alabama has not adopted this portion of Model Rule 7.2, the Adelphia matter is nevertheless instructive, as discussed in the text.