May
2008
Volume 56
Number3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

Kenneth E. Melson
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Program Manager
Nancy Bowman

Law Clerk
William E. Grove

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Program Manager, United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201.

Electronic Discovery

In This Issue

Ethical Issues Associated With Preserving, Accessing, Discovering, and Using Electronically Stored Information

Paul W. Grimm
Chief Magistrate Judge
District of Maryland

I. Introduction

One of the most rapidly developing areas of civil practice concerns issues relating to the discovery of electronically stored data. During the last few years, we have gone from only a few cases addressing this issue to the current state where new rules of civil procedure dealing with electronically stored information (ESI) have been adopted, and new cases are decided nearly every week. Despite the new rules, however, the standards being adopted can differ substantially from court to court. Because nearly all "records" are "drafted" and retained in electronic format, and the unceasing advances in technology make it easier and easier to access, store, transfer, and use electronic records, the resolution of issues associated with discovery of electronic data has become complicated. *See Thompson v. HUD*, 219 F.R.D. 93, 96 (D. Md. 2003) (citing *In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. 437, 440 n.2 (D.N.J. 2002) (estimating that more than 90 percent of all records created are done electronically)).

This article will focus on the ethical issues associated with the "duty" to preserve electronic and other evidence, as well as ethical standards relating to the use of metadata. The aim of this article is modest: to help define these issues and direct the reader to sources that provide comprehensive information that will be helpful in resolving electronic discovery issues. It is essential that attorneys be well-informed about these subjects because the consequences of not knowing what is required can be severe for both counsel and client.

II. Ethical requirements

The Rule of Professional Responsibility most directly affecting the issue of preservation of electronic data is Rule 3.4, entitled "Fairness to Opposing Party and Counsel." American Bar Association (ABA), MODEL RULES OF PROF'L CONDUCT R. 3.4 (2003), *available at* http://www.abanet.org/cpr/mrcp/rule_3_4.html. Lawyers must also be careful to check the version of the rules applicable in each state in which they practice, because many states adopt modified versions of the ABA rules. Rule 3.4(a) states: "[A lawyer shall not] 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." *Id*. The comment to the rule provides further important guidance regarding its purpose and scope:

> The procedure of the adversary system contemplates that the evidence in a case is to be marshaled competitively by the contending parties. Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like.

> Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if the relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purposes of impairing its availability *in a pending proceeding or one whose commencement can be foreseen. . . . Paragraph (a) [of Rule 3.4] applies to evidentiary material generally, including computerized information*.

Id. cmt. 1 and 2 (emphasis added), *available at* http://www.abanet.org/cpr/mrcp/rule_3_4_comm.html.

The annotation to Rule 3.4(a) points out that while a violation of the rule may expose a lawyer to professional discipline,

> [i]t is normally the judge hearing the matter who initially takes the corrective action through litigation sanctions, such as . . . exclusion of evidence, and the payment of fines, costs, and attorneys' fees. A court is likely to consider Rule 3.4, as well as other ethics rules, when imposing these litigation sanctions.

Center for Professional Responsibility, American Bar Association, ANNOTATED MODEL RULES OF PROF'L CONDUCT at 348 (5th ed. 2003) (hereinafter *Annotated Model Rules*); *see, e.g., Attorney Grievance Comm'n v. White*, 731 A.2d 447 (Md. 1999). Thus, the annotation makes an important point: while the ethics rule is the starting point, much of what is important regarding the ethical issues related to the duty to preserve electronic data is found in the case law discussing spoliation of evidence, the duty to preserve evidence, the sanctions available under the discovery rules, and the inherent authority of the court.

III. The duty to preserve evidence

Although it comes as a surprise to many lawyers, the duty to preserve evidence commences prior to the actual initiation of litigation. As one court aptly stated:

> The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation. If a party cannot fulfill this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.

Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) (citations omitted); *accord Fujitsu Ltd. v. Fed. Express Corp*., 247 F.3d 423, 436 (2d Cir. 2001); *Thompson v. HUD*, 219 F.R.D. 93, 100-01 (D. Md. 2003); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

In addition to court rulings discussing the duty to preserve evidence, the American Bar Association's Civil Discovery Standards, Standard No. 10, "Preservation of Documents," relevantly states:

> When a lawyer who has been retained to handle a matter learns that litigation *is probable or has been commenced*, the lawyer should inform the client of its duty to preserve potentially relevant documents in the client's custody or control and of the possible consequences for failing to do so." (Aug. 2004) (emphasis added).

Available at http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf. Similarly, *Principle 1 of The Sedona Principles for Electronic Document Production: Second Edition* states: "Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve

electronically stored information that can reasonably be anticipated to be relevant to litigation." *Available at* http://www.thesedona conference.org/content/miscFiles/TSC_PRINCP_ 2nd_ed_607.pdf. The recent changes to the Federal Rules of Civil Procedure make it quite clear that ESI is discoverable. Accordingly, it can no longer be denied that there is a duty to preserve ESI. The more difficult issue, in practice, is the scope or extent of this duty.

Imagine the following hypothetical: Smith is a mid-level manager who has worked successfully for a large corporation for many years in a series of responsible positions and is now 49 years old. He applies for a new position which, if received, would be a substantial promotion. Because the vacant position is a desirable one, many employees apply. The interview process is conducted by the Human Resources (HR) Director of the company and three vice presidents from the company's three regional offices, each in different states. The process takes several months and involves many telephone conferences to discuss the qualifications of the applicants, which are disseminated by e-mail with attachments to all the committee members. After an initial review, ten applicants are selected and interviews take place. All of the committee members are present for all of the interviews. Each one takes notes, as does the HR director. After the initial interviews are conducted, five candidates, including Smith, are selected for a second round of interviews, again attended by all committee members, who again take notes. After exchanging evaluations in e-mail messages and discussing the candidates during a video conference, two finalists are selected, one of whom is Smith. At that time, two committee members are selected to do further "due diligence" on each of the final candidates. They check references and prior job experience and conduct telephone interviews with former employers and co-workers of the candidates, some of whom now work at other companies. During this process, e-mail communications are exchanged with many of the references. After a final meeting of the committee, the final selection is made, and Smith does not get the job.

When told of the decision, Smith is clearly disappointed. When he learns that the successful candidate is only 35 years old and has been with the company only 18 months, he is angry and sends a memo to the HR director, with a copy to the committee members, stating that he feels his age was the reason he did not get the job. Smith concludes, "I guess that I now have to consider all my options." Two months go by, after which Smith writes a letter to the President of the company stating that he believes he was the victim of age discrimination and asks for unspecified "redress." The President orders the General Counsel and HR Director to conduct an investigation. They interview all the committee members, talk to all the candidates, including Smith, and review all the relevant documents. They conclude that no discrimination occurred and inform Smith of this. He continues at his job for another two months without taking any further action and then files a complaint with the Equal Employment Opportunity Commission (EEOC). After the EEOC declines to take the case and issues a right to sue letter, Smith sues. Given these facts, when did the duty to preserve evidence begin, and what evidence must be saved?

The "right" answer requires answers to many questions and the exercise of sound judgment.

- Does the company have a document retention/destruction policy, and if so, what does it require?
- Who are the "key players" in the selection process that are likely to be witnesses in the litigation?
- Who are peripheral players?
- When did the company have reasonable notice that a claim was likely, triggering the duty to preserve—when Smith did not get the job? When he said he was disappointed? When he wrote the memo? Went to the EEOC? Filed suit?
- Did any of the key players delete any of their notes or e-mails, or destroy any notes? When?

- Whom must the company notify once the duty to preserve is triggered?
- Where are the records located that must be preserved—on desktops? PDA's? Home computers or laptops?
- Are the records contained in back-up tapes or archival information?
- Must the company notify the nonemployees contacted during the selection process to ask them to save records?

Unfortunately, the "black-letter" statements of the law contained in cases do not do as much as could be desired to answer the above questions. However, it is possible to get some guidance. For example, in *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003), an employment discrimination case, the court observed that the duty to preserve evidence is triggered "when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Id.* at 216 (quoting *Fujitsu Ltd.*, 247 F.3d at 436). Using this statement as guidance, reasonable minds could differ about the point at which this occurs. The *Zubulake* court helpfully added:

> [O]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g. those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e. actively used for information retrieval), then such tapes would likely be subject to the litigation hold.

Id. at 218. The court further noted an exception to this rule for key players in the transaction that led to the litigation. For these key players, all back-up tapes would be subject to the litigation hold, regardless of whether the tapes are only traditionally used for disaster recovery. *Id.* Again, reasonable minds may differ in considering who these key players are, but for the purposes of the above hypothetical, at a minimum, key players would include the selection committee, the HR Director, the President, and the General Counsel.

Further guidance may be obtained from the American Law Institute's much respected Restatement of the Law Governing Lawyers. Section 118, "Falsifying or Destroying Evidence," states relevantly: "A lawyer may not destroy or obstruct another party's access to documentary or other evidence when doing so would violate a court order or other legal requirements, or counsel or assist a client to do so." American Law Institute, RESTATEMENT (THIRD) OF THE LAW: THE LAW GOVERNING LAWYERS § 118(2) (2000). The comment to the section clarifies that "evidence is usually defined as documentary or other physical material *(including material stored in electronically retrievable form)* that a reasonable lawyer would understand may be relevant to an official proceeding." *Id.* at cmt. a (emphasis added). The Restatement continues:

> On the other hand, it would be intolerable to require retention of all documents and other evidence against the possibility that an adversary in future litigation would wish to examine them. Accordingly, it is presumptively lawful to act pursuant to an established document retention-destruction program that conforms to existing law and is consistently followed, absent a supervening obligation such as a subpoena or other lawful demand for or order relating to the material.

Id. cmt. c.; *see also In re Kmart Corp.*, 371 B.R. 823, 842 (Bankr. N.D. Ill. 2007) ("While the scope of the preservation duty is broad, the 'duty to preserve potentially discoverable information does not require a party to keep every scrap of paper' in its file.") (citation omitted); *Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003). Determining just where a case lies in the continuum between evidence that "a reasonable lawyer would understand may be relevant" to an

existing or future official proceeding, and retention of all documents and other evidence against the "mere possibility" of future litigation is the stuff of sound judgment and common sense. As next will be seen, however, the adverse consequences of guessing incorrectly are sufficiently dire to warrant prudent counsel to err on the side of caution.

IV. The doctrine of spoliation and its consequences

> Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. The right to impose sanctions for spoliation arises from a court's inherent power to control the judicial process and litigation, but the power is limited to that necessary to redress conduct "which abuses the judicial process."

Silvestri, 271 F.3d at 590 (citations omitted). Thus, if a lawyer violates Rule of Professional Responsibility 3.4(a) by failing to preserve evidence or by counseling or assisting a client to do so, this usually brings into play the doctrine of spoliation of evidence. There are multiple sanctions that may be imposed for such a violation.

A. Rule 26(g): codifying an ethical obligation

An attorney's duty not to obstruct another party's access to evidence and to refrain from unlawfully altering, destroying, or concealing evidence is not only an ethical obligation, but also an obligation that flows from the Federal Rules of Civil Procedure. Rule 26(g) imposes on counsel and unrepresented parties an obligation of good faith and fair dealing in the conduct of discovery by requiring that Rule 26(a) preliminary and pretrial disclosures, as well as discovery requests, responses, and objections, be signed. The signature serves to certify that the discovery disclosure or response is "complete and correct as of the time it is made" to the best of the signer's knowledge, information or belief formed after reasonable inquiry. The Advisory Comments to the 1983 Amendment of Rule 26(g) note that, in signing the disclosure request or response, the attorney is not certifying the truthfulness of the response or request, only "that the lawyer has made a reasonable effort to assure that the client has provided all the information and documents available to him that are responsive to the discovery demand," or that it is "grounded on a theory that is reasonable under the precedents or a good faith belief as to what should be the law." Commentary to the 1983 Amendments to the Federal Rules of Civil Procedure, 97 F.R.D. 165, 218-220 (1983). As one court recently pointed out:

> [t]he Committee's concerns are heightened in this age of electronic discovery when attorneys may not physically touch and read every document within the client's custody and control. For the current "good faith" discovery system to function in the electronic age, attorneys and clients must work together to ensure that both understand how and where electronic documents, records and emails are maintained and to determine how best to locate, review, and produce responsive documents.

Qualcomm, Inc. v. Broadcom Corp., No. 05cv1958-B, 2008 WL 66932, at *9 (S.D. Cal. Jan. 7, 2008) (discussed in greater detail *infra*).

Rule 26(g) also states that if the document is not signed the court "must strike it" unless its lack of signature is promptly corrected after the attorney or party is given notice of the defect. FED. R. CIV. P. 26(g)(2). Additionally, absent a signature on the proponent's document, the responding party is not required to take any action. Finally, if the document is improperly signed or certified, sanctions are mandatory and may be imposed against the offending attorney and/or party in response to a motion or on the court's own initiative unless the court finds substantial justification for such violation. For an in-depth examination of discovery sanctions under Rule 26(g), see Paul W. Grimm, Charles S. Fax,

& Paul Mark Sandler, *Discovery Problems and their Solutions*, at 229-34 (ABA Publishing 2005).

In determining whether sanctions are warranted, the court in *St. Paul Reinsurance Co. v. Commercial Fin. Corp.*, 198 F.R.D. 508 (N.D. Iowa 2000), employed an objective standard to assess whether the signer of a certificate made a reasonable inquiry before submitting a discovery request, response, or objection. *Id.* at 516, n.3. Factors considered were: "(1) the number and complexity of the issues; (2) the location, nature, number and availability of potentially relevant witnesses or documents; (3) the extent of past working relationships between the attorney and the client, particularly in related or similar litigation; and (4) the time available to conduct an investigation." *Id*. (citations omitted). The court held that a finding that the discovery request, response, or objection was submitted for an improper purpose need not be predicated upon a showing of bad faith. *Id*.

Additionally, the court in *St. Paul* recognized that the decision whether to impose sanctions under Rule 26(g) parallels the analysis used in determining whether to impose sanctions under Rule 11. *Id*. at 516, n.4. Accordingly, the court concluded that the available sanctions under Rule 26(g) were not limited to compensatory sanctions, such as an award for costs and reasonable attorney's fees, but also included whatever sanctions are appropriate "in light of the particular circumstances." *Id*. at 515 (citations omitted); *see also Wingnut Films, Ltd., v. Katja Motion Pictures Corp*., No. CV 05-1516-RSWL SHX, 2007 WL 2758571, at *20 (C.D. Cal. Sept. 18, 2007); *Cache La Poudre Feeds, LLC v. Land O' Lakes, Inc.,* 244 F.R.D. 614, 636-37 (D. Colo 2007); *Or. RSA No. 6 v. Castle Rock Cellular of Or. Ltd. P'ship*, 76 F.3d 1003 (9th Cir. 1996); *Project 74 Allentown, Inc. v. Frost*, 143 F.R.D. 77 (E.D. Pa. 1992); *Apex Oil Co. v. Belcher Co. of New York*, 855 F.2d 1009 (2d Cir. 1988); *Poole v. Textron, Inc.* 192 F.R.D. 494 (D. Md. 2000). The *St. Paul* court also required plaintiff's counsel to write an article in an appropriate law journal, explaining why it was improper to make the type of objections he had asserted in that case.

When courts are called upon to determine appropriate sanctions when evidence has been lost or destroyed, among the things that they will evaluate are the discovery disclosures, requests, and responses that were served in the case. If the court finds them lacking because they were not based on a reasonable inquiry, or were incomplete, incorrect, or made for an improper purpose, then the lawyers who signed them can expect to be sanctioned for violating Rule 26(g), unless the failure or violation was substantially justified.

B. Adverse inference instruction

One sanction that may be imposed against a spoliator is for the court to give an adverse inference instruction to the jury. *See Glover v. Costco Wholesale Corp.*, 153 Fed. App'x. 774, 776 (2d Cir. 2005); *Residential Funding Corp. v. DeGeorge Fin. Corp*., 306 F.3d 99 (2d Cir. 2002); *Thompson*, 219 F.R.D. 93; *Zubulake*, 220 F.R.D. 212. The effect of such an instruction has been described as follows:

> In practice, an adverse inference instruction often ends litigation—it is too difficult a hurdle for the spoliator to overcome. The *in terrorem* effect of an adverse inference is obvious. When a jury is instructed that it may "infer that the party who destroyed potentially relevant evidence did so out of a realization that the [evidence was] unfavorable," the party suffering this instruction will be hard-pressed to prevail on the merits. *Zubulake*, 220 F.R.D. at 219-20 (alteration in original) (citations omitted).

Because an adverse inference sanction potentially is so harmful to the spoliator's case, it is not automatically given whenever a court finds spoliation has occurred. Instead, a three-factor test is frequently used to determine if the instruction is warranted. *Thompson v. HUD*, 219 F.R.D. at 101. The factors are (1) whether the party having control over the evidence had an obligation to preserve it when it was destroyed or altered; (2)

whether the destruction or loss was accompanied by a "culpable state of mind"; and (3) whether the evidence that was destroyed or altered was relevant to the claims or defenses being advanced by the party that was deprived of the evidence. *Id.*; *see also EEOC v. LA Weight Loss*, 509 F. Supp. 2d 527 (D. Md. 2007); *Residential Funding Corp.*, 306 F.3d at 107-08; *Zubulake*, 220 F.R.D. at 220.

As for the required state of mind that must accompany the destruction, three distinct varieties have been recognized: (1) bad faith/knowing destruction; (2) gross negligence; and (3) ordinary negligence. *Thompson*, 219 F.R.D. at 101. Moreover, there is a direct relation between the degree of culpability of the state of mind of the spoliator and the amount of proof that must be shown to demonstrate that the destroyed or altered evidence was relevant to the case of the party seeking to discover it—the more culpable the state of mind, the less a showing of relevance is needed. *Id.*; *see also King v. Am. Power Conversion Corp.*, 181 Fed. App'x. 373, 376 (4th Cir. 2006) ("However, bad faith conduct by the plaintiff may not be needed to justify dismissal if the spoliation of evidence effectively renders the defendant unable to defend its case."); *Vodusek v. Bayliner Marine Corp*., 71 F.3d 148 (4th Cir. 1995) (holding that the district court acted within its discretion in allowing the jury to draw an adverse inference from the destruction of evidence that was integral to a theory of the case even when there was no evidence of bad faith).

Although most cases that discuss spoliation and its consequences emphasize the need for some culpability on the part of the party that failed to preserve the evidence, lawyers need to be aware that courts have imposed spoliation sanctions for conduct characterized as merely negligent when the prejudice resulting to the party deprived is great. *See, e.g., Silvestri v. Gen. Motors*, 271 F.3d 583, 593 (4th Cir. 2001) (noting that dismissal of a case because of a plaintiff's failure to preserve evidence could be warranted based on inadvertent and negligent conduct of a party where "the effect of the spoliator's conduct was so prejudicial that it substantially denied the defendant the ability to defend the claim.").

The case law illustrates the type of conduct viewed by the courts as sufficient to warrant a spoliation instruction. *Compare Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 70, 74 (D.D.C. 2003) (holding defendant in contempt for not reasonably informing employees of existence of a clear and unambiguous order enjoining "agents or employees" from "transporting, removing, or in any way tampering" with information requested by plaintiff, leading to erasure of relevant electronic data)*, with Linnen v. A.H. Robins Co.,* No. 97-2307, 1999 WL 462015 (Mass. Super. Ct. June 16, 1999) (defendant's recycling of back-up tapes caused spoliation of relevant evidence and contravened an obligation to preserve such data pursuant to plaintiff's request for documents; the court allowed an adverse inference jury instruction against defendant but rejected plaintiff's additional demands for a default judgment and monetary damages), *and In re Kmart Corp.*, 371 B.R. 823 (Bankr. N.D. Ill. 2007) (bankruptcy court denied request for adverse inference instruction, holding that Kmart acted only with fault and the evidence failed to establish that documents unfavorable to Kmart were deleted as a result of inadequate retention efforts), *and United States v. Koch Indus., Inc.*, 197 F.R.D. 463 (N.D. Okla. 1998) (district court refused to issue an adverse inference instruction, ruling that defendant's lack of a formal document retention policy was indicative of negligence rather than bad faith or purposeful destruction of documents).

C. Discovery sanctions

Another consequence of spoliation of evidence can be the imposition of sanctions under Federal Rule of Civil Procedure 37. This rule provides a comprehensive, though complex, framework for imposing sanctions for various discovery violations. Perhaps stating the obvious, a condition precedent to the imposition of Rule 37 sanctions is that there must be a violation of a discovery-related court order. *In re Kmart Corp*., 371 B.R. at 839; *Wiginton*, 2003 WL 22439865,

at *3 n.5. The most onerous sanctions are found at Rule 37(b)(2) for failures to comply with court-ordered discovery. The rule permits a court to impose, *inter alia*: an order that designated facts shall be taken as established for the litigation; an order that the party who disobeyed the court's order be precluded from asserting certain claims or defenses or offering evidence on designated matters; an order that certain pleadings or parts thereof be stricken or that the litigation be stayed; or an order that the disobedient party or lawyer be punished by contempt. The effect of Rule 37(b)(2) sanctions can end the litigation.

For example, in *Thompson*, 219 F.R.D. 93, the court found that a defendant violated a prior court order to produce certain electronic records, including e-mail. The court imposed Rule 37(b)(2) sanctions against the party that failed to preserve the e-mail records. The court-ordered sanctions included precluding the defendant from introducing any of the existing e-mail records in support of its defenses or in opposition to plaintiff's claims; precluding defendant from using existing e-mail records to prepare witnesses for trial; and leaving open the possibility of contempt proceedings against the defendant. *Id*. at 104-05. Finally, the court found that spoliation had occurred, but declined to give an adverse instruction because the case was being tried before the court without a jury. *Id.*

Many courts have ruled that it is improper for a district court to impose case determinative sanctions under Rule 37(b)(2) without an enhanced showing of willfulness, bad faith, or that the party affected by the discovery violation suffered prejudice thereby. *See, e.g., S. States Rack & Fixture, Inc. v. Sherwin-Williams Co.*, 318 F.3d 592 (4th Cir. 2003); *Wendt v. Host Int'l, Inc*., 125 F.3d 806 (9th Cir. 1997); *Mid-America Tablewares, Inc. v. Mogi Trading Co*., 100 F.3d 1353 (7th Cir. 1996); *Dorsey v. Acad. Moving & Storage, Inc*., 423 F.2d 858 (5th Cir. 1970). In *Columbia Pictures Inc. v. Bunnell*, Order Granting Plaintiff's Motion for Terminating Sanctions, No. 2:06-cv-01093 (C.D. Cal. Dec. 13, 2007) (No. 325), a court imposed case dispositive sanctions and entered a default judgment against defendants in a copyright action against the operators of an Internet search engine Web site alleged to have facilitated unauthorized copying and distribution of movies and television programs. *Id.* The court found that defendants had willfully destroyed evidence, such as group forum postings, user IP addresses, and identifying information of site operators. *Id.* at 2-8. This misconduct permanently affected the plaintiffs' ability to meet the burden of proof, and thus the court imposed sanctions. *Id.* at 10.

Just because a party demonstrates that its adversary has violated a prior court order to preserve evidence does not automatically mean that the court will impose the most draconian sanctions under Rule 37. In *Linnen v. A.H. Robins Co.,* No. 97-2307, 1999 WL 462015 (Mass. Super. Ct. June 16, 1999), the trial court found that the defendant violated a court order to preserve electronic back-up tapes, which was imposed at the commencement of the litigation. As a sanction, the court issued an adverse inference instruction, but declined the plaintiffs' request that the defendants be precluded from introducing at trial evidence of certain communications relating to the electronic records that had not been preserved. The court noted the availability of this sanction under the state rule of procedure that contained provisions similar to FED. R. CIV. P. 37, but stated that evidence exclusion should be narrowly tailored and that the plaintiffs must demonstrate with sufficient precision exactly what evidence should be excluded in order to receive such a sanction. *Id*. at *12. The court denied plaintiffs' request for evidence preclusion because they failed to demonstrate "sufficient precision," but expressed its willingness to reconsider this sanction if the plaintiffs were able to make a less speculative factual demonstration of the relief they sought. *Id.* This case suggests the need for a party seeking evidence preclusion sanctions to be as particular as possible about just what evidence the offending party should be precluded from introducing, or disputing, at trial. *Linnen* also cautions against assuming that just because spoliation has been

demonstrated, the court automatically will impose the harshest sanctions. As one court stated:

> Sanctions for the destruction of evidence serve three distinct remedial purposes: punishment, accuracy, and compensation. Sanctions which serve to punish a spoliator advance the goals of retribution, specific deterrence, and general deterrence. Some sanctions are designed to promote accurate fact finding by the court or jury. Other sanctions attempt to compensate the non-spoliating party by redressing the imbalance caused by the spoliator's destruction of relevant evidence. A court should select the least onerous sanction necessary to serve these remedial purposes. The severity of the sanction selected should be a function of and correspond to the willfulness of the spoliator's destructive act and the prejudice suffered by the non-spoliating party. Thus, courts consider a variety of factors in determining an appropriate sanction, but the following two factors carry the most weight: the degree of culpability of the party who lost or destroyed the evidence, and the degree of actual prejudice to the other party.

United States v. Koch Indus., Inc., 197 F.R.D. 463, 483 (N.D. Okla. 1998) (citing GORELICK, MARZEN AND SOLUM, DESTRUCTION OF EVIDENCE, §§ 1.11-1.13, 1.21 and 3.16 (1989 & 1997 Cum. Supp.)). In *Koch*, the court found that defendants negligently failed to preserve computer tapes, but declined to issue an adverse inference instruction, choosing to issue a less serious sanction of allowing the plaintiff to inform the jury that tapes had been destroyed and that this destruction had an adverse impact on its case. *Id*. at 486.

In addition to giving an adverse jury instruction, the court can impose other sanctions against parties that fail to preserve evidence. In *Krumwiede v. Brighton Associates*, 2006 WL 1308629 (N.D. Ill., May 8, 2006), the court determined that the plaintiff willfully and in bad faith altered, modified, and destroyed evidence that should have been preserved. Consequently, it imposed Rule 37 sanctions against the plaintiff, including the entry of a default judgment to "send a strong message to other litigants, who scheme to abuse the discovery process and lie to the Court that this behavior will not be tolerated and will be severely sanctioned." *Id*. at *11.

Rule 37(b)(2)(D) also permits a court to treat as contempt of court a failure to obey a prior discovery order. While Rule 37(b)(2)(D) identifies contempt as one possible discovery sanction, an independent basis exists for this sanction inasmuch as a court "has the inherent power to protect its integrity and to prevent abuses of the judicial process by holding those who violate its orders in contempt and ordering sanctions for such violations." *Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 70, 75 (D.D.C. 2003) (citing *Cobell v. Babbitt*, 37 F. Supp. 2d 6, 9 (D.D.C. 1999)). Two conditions must exist to warrant such a civil contempt finding: "(1) the existence of a reasonably clear and specific order, . . . and (2) violation of that order by the defendant." *Id*. However, as demonstrated by the court's analysis in the *Landmark* case, a court may not consider the merits of a motion for contempt as a discovery sanction without first determining that the prior order satisfies the specificity requirement of Federal Rule of Civil Procedure 65(d), because "[c]ivil contempt lies only for violation of a clear and unambiguous order." *Id.* at 74. Moreover, a court may not hold a party in civil contempt absent clear and convincing evidence. *Id*. at 75. For these reasons, it can be expected that a court will view a contempt citation as a very serious sanction, available only in instances of extreme misconduct in violating a clear and specific order.

Finally, Rule 37, and court cases interpreting it, make abundantly clear that an additional sanction that may be imposed against an attorney or client found to have spoliated evidence is an award of reasonable attorneys' fees and costs incurred by the party seeking the evidence in connection with motions filed to obtain evidence subsequently determined to have been lost or destroyed. In this regard, Rule 37(a)(4)(A), which deals with motions for an order to compel

discovery, permits the court to deny a request for attorneys' fees and costs by the party that prevails in a motion to compel only if (a) the moving party did not first attempt to obtain the information sought without court involvement before filing its motion, (b) the failure to produce the information sought was substantially justified, or (c) the imposition of monetary sanctions would be unjust. As for Rule 37(b), which addresses sanctions appropriate for a party failing to obey a previous court order to provide discovery, Rule 37(b)(2) states that in addition to, or in lieu of, any of the potentially case determinative sanctions listed at Rule 37(b)(2)(A-E), the court may order the disobedient party to pay reasonable attorneys' fees and costs incurred by the moving party, unless the court determines that (a) the failure to obey the prior court order was substantially justified, or (b) it would be unjust to award monetary sanctions.

It is noteworthy that the recently approved changes to the Federal Rules of Civil Procedure relating to discovery of ESI include a change to Rule 37 and the circumstances in which a judge may impose sanctions under the discovery rules for failure to preserve ESI. In the absence of an order to preserve evidence, the proposed rule would preclude a court from sanctioning a party under the rules of procedure for the loss or destruction of evidence unless there were "exceptional circumstances," provided the loss or destruction was the result of the "routine, good-faith operation of an electronic information system." The rule does not define what constitutes "exceptional circumstances," and the limits on the ability of the court to award sanctions do not apply if a preservation order has been issued. Nor do they prevent the court from imposing sanctions under its inherent or other authority. Additionally, the advisory comment to the newly revised Federal Rule of Civil Procedure 37(e) makes it clear that the "safe harbor" from sanctions provided by revised Rule 37(e) is quite limited, because once a party becomes aware of the existence of a duty to preserve ESI, it may have to intervene "to modify or suspend certain features of that routine operation [of an electronic information system] to prevent the loss of information, if that information is subject to a preservation obligation." *Available at* http://www.law.cornell.edu/rules/frcp.

The recent change to Rule 37 can be expected to heighten, rather than diminish, disputes regarding the preservation of ESI, as parties seeking to discover evidence in the possession of their adversary will seek to obtain a "preservation agreement" from them, and, if unsuccessful, can be expected to immediately seek a court order to preserve evidence. *See*, *e.g., Treppel v. Biovail Corp*., 233 F.R.D. 363 (S.D.N.Y. 2006). Further, if a party seeks to excuse the loss or destruction of relevant evidence by attributing it to the routine, good-faith operation of an electronic information system, it can be expected that opposing counsel will seek discovery of the circumstances of the destruction, the nature of the records maintenance system, and its application. Finally, as observed above, it must be noted that the limitations of the Rule 37(e) rule only apply to imposing sanctions under the rule and would not affect the inherent authority of the court to sanction, *Chambers v. Nasco, Inc.*, 501 U.S. 32 (1991), or to impose sanctions under 28 U.S.C. § 1927 (1980). Therefore, the ethical obligations associated with the duty to preserve evidence will not be diminished by the rule change.

D. Disciplinary proceedings

As noted at the start of this article, because Rule 3.4(a) of the Rules of Professional Responsibility prohibits the unlawful alteration or destruction of material that has potential evidentiary value, a finding by a court that a lawyer has acted to destroy electronically stored evidence, or counseled or assisted a client in doing so, may also result in the initiation of disciplinary proceedings or other sanctions, such as disqualification of counsel. Thus, in *Attorney Grievance Comm'n v. White*, 731 A.2d 447 (Md. 1999), the plaintiff, a lawyer who filed a Title VII employment discrimination claim, was disbarred because she destroyed part of an autobiographical memorandum she authored that discussed events related to the litigation. The federal court suspended her indefinitely, and the Court of

Special Appeals of Maryland disbarred her for violating Rule 3.4(a) and other violations. *See also United States v. Castellano*, 610 F. Supp. 1151 (S.D.N.Y. 1985); *Briggs v. McWeeny*, 796 A.2d 516 (Conn. 2002); *Idaho State Bar v. Gantenbein*, 986 P.2d 339 (Idaho 1999). Although none of the reported cases concerning Rule 3.4(a) violations deal specifically with destruction, alteration, or concealment of electronic records, the analysis in these cases applies with equal force to spoliation of such records. *See Legal Ethics and the Destruction of Evidence*, 88 YALE L. J. 1665 (1979).

E. Discovery obligations case in point: *Qualcomm v. Broadcom*

The duty to preserve ESI and the actions counsel are required to take in retrieving that information were recently examined by the Southern District of California in *Qualcomm Inc. v. Broadcom Corp*., No. 05cv1958-B, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008). During this patent infringement case, the defendant, Broadcom, attempted to support an affirmative defense by requesting documents regarding Plaintiff's waiver of their right to enforce their patent. As part of its discovery in support of its defense, Broadcom served two Rule 34 requests for the production of documents, a set of interrogatories, and a Rule 30(b)(6) deposition notice on Qualcomm. Qualcomm at first appeared responsive and indicated that it would provide materials in its possession "which can be located after a reasonable search" and that it reserved "the right to supplement its response." *Id*. at * 2. It also prepared two 30(b)(6) witnesses for deposition. As discovery continued, Qualcomm became "increasingly aggressive" in its assertions that the materials sought by Broadcom did not exist. *Id.* at *3.

As was later discovered, Qualcomm and its counsel had, in fact, failed to provide "responsive documents, many of which directly contradict[ed]" Qualcomm's repeated position that it had none of the information requested by Broadcom. *Id*. at *8. The court discovered that the attorneys for Qualcomm had, in the course of preparing witnesses for the 30(b)(6) deposition, discovered 21 e-mails that contradicted Qualcomm's representations to opposing counsel and the court, and that counsel affirmatively chose "not to produce these newly discovered e-mails to Broadcom, claiming they were not responsive to Broadcom's discovery requests." *Id*. at *4. However, the e-mails were indeed relevant and soon after their discovery and use at trial, the jury found in favor of Broadcom. *Id*. at *5.

Following the verdict, a subsequent search, by counsel, of the e-mail archives of 21 employees uncovered over 46,000 documents—more than 300,000 pages—that were responsive to Broadcom's discovery requests—but never produced. *Id.* at *6. The court concluded that this gross failure was the result of

> one or more of the retained lawyers [choosing] not to look in the correct locations for the correct documents, to accept the unsubstantiated assurances of an important client that its search was sufficient, to ignore the warning signs that the document search and production were inadequate, not to press Qualcomm employees for the truth, and/or to encourage employees to provide the information (or lack of information) that Qualcomm needed to assert its non-participation argument and to succeed in this lawsuit.

Id. at *13. As a result of this "monumental and intentional discovery violation," *id*. at *17, the court held that sanctions were warranted against Qualcomm and its outside counsel.

The court held that, due to the number and nature of the documents eventually uncovered, outside counsel should have suspected, and likely did, that Qualcomm failed to adequately search for the requested documents. *Id*. at *12-13. Accordingly, the attorney's certification on the discovery response violated Rule 26(g). However, as the court pointed out, a literal reading of Rule 26(g) would permit sanctions only against the signing attorney, and not Qualcomm's litigation team as a whole. The court noted that Rule 37

violations were not available due to the fact that Broadcom, operating under the assumption that Qualcomm was properly responding to its discovery requests, never filed a motion to compel, so there was no subsequent order that, when violated, would warrant sanctions under Rule 37. *Id*. at *13 n. 9. As a result, the court reasoned:

> [T]he federal rules impose a duty of good faith and reasonable inquiry on all attorneys involved in litigation who rely on discovery responses executed by another attorney. *See* Fed. R. Civ. P. 26 Advisory committee's notes (1983 Amendment) (Rule 26(g) imposes an affirmative duty to engage in pretrial discovery in a responsible manner that is consistent with the spirit and purposes of Rules 26 through 37); Fed. R. Civ. P. 11 (by signing, filing, submitting or advocating a pleading, an attorney is certifying that the allegations have factual, evidentiary support). Attorneys may not utilize inadequate or misleading discovery responses to present false and unsupported legal arguments and sanctions are warranted for those who do so. *Id.* The facts of this case also justify the imposition of sanctions against these attorneys pursuant to the Court's inherent power.

Id. at *13, n.9.

Under its inherent authority, the court not only sanctioned Qualcomm, but six of its outside attorneys, for misconduct as the result of, among other things, failing to "conduct a reasonable inquiry into Qualcomm's discovery production before making specific factual and legal arguments to the court." *Id.* at *14. The court imposed monetary sanctions of $8.5 million in attorneys' fees and costs against Qualcomm, referred the attorneys to the California State Bar for an appropriate investigation, and ordered counsel to take part in a comprehensive Case Review and Enforcement of Discovery Obligations (CREDO) program. *Id.* at *18 (describing the CREDO program as a "collaborative process to identify the failures in the case management and discovery protocol utilized by Qualcomm and its in-house and retained attorneys in this case, to craft alternatives that will prevent such failures in the future, to evaluate and test the alternatives, and ultimately, to create a case management protocol which will serve as a model for the future.").

In a footnote, the court explained that monetary sanctions were not imposed against Qualcomm's outside counsel, noting "it is possible that Qualcomm will seek contribution from its retained attorneys after it pays Broadcom's attorneys' fees and costs." *Id*. at n.18. There are many lessons to be learned from Qualcomm, but chief among them is that lawyers can expect that courts will require them to live up to their obligations under Rule 26(g) and that blind reliance on a client's representations that it adequately searched for and produced all responsive ESI will not insulate a lawyer from sanctions or charges of ethical misconduct when the lawyer knows, or should suspect, the client's response is inadequate.

V. Focusing in on the ethical issues associated with accessing and using metadata

Additional ethical concerns arise regarding accessing and using metadata received from an adversary in a suit or from a third party with whom the lawyer is dealing, such as in a commercial transaction. These new concerns arise because, under the recently revised Federal Rules of Civil Procedure, Rule 34 permits a party requesting production of ESI as part of a request for production of documents to specify the form or forms in which the ESI is to be produced. One form of production frequently sought by parties in litigation is production of ESI in its "native format," in which the ESI is produced along with hidden embedded data, commonly referred to as "metadata." Metadata has been defined as follows:

> Metadata, commonly described as "data about data," is defined as "information describing the history, tracking, or management of an electronic document . . . [Metadata includes]

> 'information about a particular data set which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted . . . . Most metadata is generally not visible when a document is printed or when the document is converted to an image file.'"

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005) (citations omitted).

"Hidden" metadata may reflect vitally important information about a document. For example, imagine that a party has filed a personal injury suit against another person. After discovery, plaintiff's counsel decides that the time is right to try to settle the case. She crafts a very detailed settlement demand letter that outlines the issues regarding liability and damages, and concludes by demanding $250,000 to settle the case. She then sends an e-mail to her client, attaching the draft settlement letter, and asks him to carefully review the demand letter and to make any comments about it by "redlining" the document and e-mailing it back to her. Assume further that the client adds the following "redline" comment to the letter: "the letter sounds great, and if you can get $250,000 that would be a home run. As you know, I am really strapped for money right now and I'd grab any offer greater than $50,000." The lawyer receives the e-mail from the client with these comments and dutifully edits them out, leaving the text the way it originally was when she sent it to her client for his review. She then sends an e-mail to the defendant's lawyer, attaching the settlement letter that demands $250,000.

The defendant's lawyer receives the e-mail, opens the attachment, and reads the settlement letter. Because the client's comment was deleted by the plaintiff's lawyer, defense counsel cannot see it by looking at the opened settlement letter as it appears on his desktop computer. However, by applying very standard software applications, the defendant's lawyer can access the metadata embedded in the settlement letter, which includes the plaintiff's comment that he would accept a substantially lower settlement than that demanded. Imagine the tactical advantage that the defendant's lawyer now has in the settlement negotiations.

There is just one little problem with this scenario. Is it ethical for the defense lawyer, acting directly or through others, to access the metadata of the electronic letter he has received—which clearly includes attorney-client communications—even though he does not know whether the plaintiff's lawyer inadvertently sent him the letter with its metadata included? The ABA and a number of state bar associations have recently issued ethics opinions addressing this issue. Unfortunately, the positions taken have not been consistent, and, given the ubiquity of production of ESI, lawyers will need to familiarize themselves with the potential ethical issues affecting the access and use of metadata produced as part of electronic records.

The Maryland State Bar Association's Committee on Ethics recently issued Opinion No. 2007-09, titled "Ethics of Viewing and/or Using Metadata." The opinion addressed three questions: (1) whether it is ethical for an attorney who receives ESI to view or use metadata in documents produced by another party; (2) whether the sending party has an ethical duty to remove metadata from the files before they are sent to another party; and (3) whether the lawyer receiving the ESI has an ethical duty not to view or use the metadata without first determining whether the sender intended to include the metadata with the files produced. Md. State Bar Assoc. Comm. on Ethics, Formal Op. 2007-09 (2006) (hereinafter *MSBA Opinion*).

The committee provided a single answer to the first and third questions, opining that:

> Subject to any legal standards or requirements (case law, statutes, rules of procedure, administrative rules, etc.), this Committee believes that there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining

> whether the sender intended to include such metadata.

Id. at 1.The committee based its rationale on the difference between the Maryland Rules of Professional Conduct [hereinafter MRPC] and the ABA Model Rules of Professional Conduct (Model Rules). In this regard, Model Rule 4.4(b) was amended in 2002 to require that a "lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender," *available at* http://www.abanet.org/cpr/mrpc/mrpc_toc.html. Because the equivalent MRPC has not been amended to include the new language of Model Rule 4.4(b), the committee concluded that under the Maryland ethics rule, a lawyer receiving ESI that contains metadata would not have to notify the sending party in order to ascertain if the inclusion of the metadata was inadvertent. *Id*. The committee further noted that, even under the revised version of ABA Model Rule 4.4(b), a receiving party is only required to notify a producing party of its disclosure, and is not precluded from reading or using the metadata produced, regardless of whether the production was inadvertent or intentional. *Id*. Accordingly, a Maryland lawyer receiving ESI that contains metadata can read and use the metadata and is not required to notify the producing party of its disclosure under the MRPC.

The committee qualified the scope of its opinion, however, to caution that the recent amendments to the Federal Rules of Civil Procedure relating to discovery of ESI could alter the ethical duty of the receiving party. Specifically, under revised Rule 26(b)(5), a party may assert privilege after producing ESI, in which case the receiving party must return, sequester, or destroy the information received that is the subject of the asserted privilege. The receiving party likewise may not use or disseminate the information until the court has delivered a ruling on the issue. Revised Rule 26(b)(5). In addition, the committee pointed out that the parties also could reach an agreement regarding the handling of potentially privileged ESI and that such an agreement would be controlling in that case. MSBA Opinion, note 2 at 2-3. Thus, the ethical duties imposed on a Maryland lawyer that receives ESI containing metadata are governed by the MRPC, the applicable rules of procedure, and any agreements regarding the handling of privileged information reached by counsel.

With respect to the second question, whether a lawyer sending ESI has an ethical duty to delete metadata before producing it to an adverse party, the committee noted that "the sending attorney has an ethical obligation to take reasonable measures to avoid the disclosure of confidential or work product materials imbedded in the electronic discovery," *id*., which might include "scrubbing" the metadata from the ESI before it is produced. Importantly, the opinion did not address MRPC 3.4, which proscribes altering, destroying, or concealing evidence, nor did it address the implication of the substantive duty to preserve evidence relevant to prospective or pending litigation. *See generally Thompson v. HUD*, 219 F.R.D. 93 (D. Md. 2003) (discussing the duty to preserve evidence and the corresponding sanctions that may be imposed for the failure to do so). Accordingly, lawyers who are inclined to scrub metadata from ESI before producing it to another party should be alert to these additional ethical issues and should never scrub metadata without notifying the receiving party that the ESI has been produced without the metadata and preserving a copy of the ESI with the metadata, to insure against an allegation of spoliation of evidence.

As noted above, the ABA Standing Committee on Ethics and Professional Responsibility has also issued a recent opinion regarding the ethical issues associated with viewing and using metadata. ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Opinion 06-442 (2006) [hereinafter *ABA Opinion*]. In this opinion, the ABA concluded:

> The Committee first notes that the Rules do not contain any specific prohibition against a lawyer's reviewing and using embedded

> information in electronic documents. The most closely applicable rule, Rule 4.4(b) relates to a lawyer's receipt of inadvertently sent information. Even if transmission of "metadata" were to be regarded as inadvertent, Rule 4.4(b) is silent as to the ethical propriety of a lawyer's review or use of such information. The Rule provides only that "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

Id. at 3.

The committee noted that its opinion represented a significant departure from earlier ABA opinions, which prohibited a lawyer who received inadvertently produced confidential materials from reading or using them. *Id*. at 3, n.9. Thus, under newly revised ABA Model Rule 4.4(b), a lawyer receiving ESI with metadata, who knows or reasonably suspects that the metadata inadvertently was produced, may read and use it, but must notify the producing party of its disclosure. Although the ABA opinion is silent regarding the impact of the newly revised Federal Rules of Civil Procedure dealing with ESI, practitioners should not ignore them, particularly revised Rule 26(b)(5), which outlines specific actions that must be taken if a party that produced ESI containing privileged information asserts a privilege after the production.

The ABA opinion also discussed the practice of scrubbing metadata before producing ESI to an adverse party, as a means to avoid inadvertent production of confidential information. *ABA Opinion*, note 11 at 4-5. However, like the Maryland ethics opinion, the ABA opinion does not address the question of whether doing so could create an ethical issue of concealing or altering evidence. Accordingly, as already noted, lawyers who scrub metadata from ESI before producing it are wise to notify the receiving party that they have done so and should also preserve a version of the ESI with the metadata intact, to avoid a spoliation argument.

The New York Bar's Committee on Professional Ethics has taken a third and distinctly different, approach to the review and use of inadvertently disclosed metadata. N.Y. State Bar Assoc. Comm. on Prof'l Ethics, Formal Op. 782 at 2 (2004). Focusing on the lawyer's responsibility to refrain from revealing a client's confidences or secrets, the committee concluded that a lawyer sending ESI to another party

> must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information. What constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a "template" used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document.

Id. at 3.

Like the ABA and Maryland ethics committees, the New York committee also addressed the ethical responsibility of the lawyer who receives ESI containing metadata under circumstances where it is uncertain whether the sending party intended to produce it. However, taking a position directly at odds with that taken by Maryland and the ABA, the committee concluded that

> [l]awyer recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets. In N.Y. State 749, we concluded that the use of computer technology to access client confidences and secrets revealed in metadata constitutes "an impermissible intrusion on the attorney-client relationship in violation of the Code [of ethics]."

Id.

Recent opinions issued by ethics committees in Florida, Alabama, and Arizona have followed

New York's lead regarding the duties imposed on attorneys sending and receiving ESI in a form that includes its metadata. *See generally* Fla. State Bar Formal Op. 06-2 (2006); Ala. Ethics Formal Op. RO-2007-02 (2007); Ariz. Ethics Formal Op. 07-03 (2007). As does the New York committee, the committees of these three states find that a lawyer sending ESI containing metadata has a duty to take reasonable steps to prevent the inadvertent disclosure of confidential or privileged information. Similarly, lawyers receiving ESI have a corresponding duty not to "mine" documents for metadata "or otherwise engage in conduct which amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel." Ariz. Ethics Op. 07-03 at 4.

The District of Columbia has taken yet another position, perhaps in an attempt to reach a middle ground between the ABA's stance and that of New York and other states similarly aligned. *See* D.C. Bar Assoc. Formal Ethics Op. 341 (2007). Consistent with the ABA opinion, the D.C. Bar Association issued Ethics Opinion 341, in which it determined:

> A receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent. In such instances, the receiving lawyer should not review the metadata before consulting with the sending lawyer to determine whether the metadata includes work product of the sending lawyer or confidences or secrets of the sending lawyer's client.

Id. at 1. The opinion further noted, however, that "[i]n all other circumstances, a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary." *Id.* at 10.

Finally, rather than stating any specific rule pertaining to the ethical obligations of a lawyer receiving inadvertently transmitted metadata, the Pennsylvania Bar Association's formal opinion encourages receiving attorneys to weigh a multitude of factors in deciding whether to make use of the metadata in question. Pa. Bar Assoc. Formal Op. 2007-500, Mining Metadata (2007). Noting an absence of any Pennsylvania Rules of Professional Conduct determining the obligations of attorneys inadvertently receiving metadata from another lawyer, the Pennsylvania Bar suggests that the decision of how or whether a lawyer may use any such information will depend upon many factors, including:

- the judgment of the lawyer;
- the particular facts applicable to the situation;
- the lawyer's view of his or her obligations to the client under [Pennsylvania Rules];
- the nature of the information received;
- how and from whom the information was received;
- attorney-client privilege and work product rules; and
- common sense, reciprocity and professional courtesy.

Id. at 1. The opinion suggests that attorneys examine the above factors and resolve the issue "through the exercise of sensitive and moral judgment" and concludes by urging that the determination be based upon "common sense, reciprocity and professional courtesy." *Id.* at 1, 7.

For lawyers practicing only in Maryland, or in jurisdictions that have adopted the ABA Model Rules and their interpretations, the New York ethics opinion and others following it have little effect, other than to highlight the divergent views on this issue. To lawyers practicing in multiple jurisdictions, however, the implications are more challenging. If a lawyer is licensed in both Maryland and New York and is involved in litigation in New York, it would be unwise to assume that the Maryland or ABA approach to viewing and using metadata that inadvertently may have been produced in ESI would govern. In the absence of clear guidance on which rule would apply in a given situation, a lawyer should carefully evaluate each potentially applicable

ethics ruling and make sure that his or her conduct does not run afoul of it.

VI. Conclusion

The above discussion is intended to focus on some of the ethical challenges facing attorneys with respect to the preservation, discovery, and use of electronically stored information. From this discussion, practical measures can be identified to help reduce the chance that you or your clients will be found lacking knowledge in this rapidly changing area of the law.

First, it is essential that counsel be well-versed in the requirements of the Rules of Professional Conduct that relate to the preservation, discovery, and use of ESI in whatever version has been adopted by the state(s) in which he or she practices and the state(s) in which the litigation is pending. Further, if there are any comments or published bar opinions interpreting the rules by the relevant bar disciplinary authority, they should be consulted as well.

Second, the best way to avoid problems in this area is to try to prevent them in the first place. If you represent a client that creates, uses, and maintains records in electronic format (and frankly, in today's world that likely is every client), make sure that your client is aware of how courts interpret the duty to preserve evidence, the doctrine of spoliation, and the possible sanctions—including case determinative ones—that can be imposed if the court finds a violation of the duty to preserve. Candidly, this is easier said than done, and it can sometimes seem that you are "damned if you do, and damned if you don't." For example, if your client has no established document retention/destruction policy and the court finds that relevant information has been lost or destroyed improperly, the fact that the client had no procedure in place may be viewed as indicia of bad faith, since most courts regard such policies as commonplace. However, if your client does have a policy, it is almost inevitable that it will not be perfectly complied with, and any failure to comply with an existing policy also may be viewed by the court as evidence of culpable conduct. Be mindful of the fact that just having a record retention/destruction policy does not ensure against an adverse instruction or imposition of other sanctions if relevant information is not preserved. A court can be expected to review any retention plan to ensure that its terms are reasonable and not imposed for an improper purpose. *See, e.g., Lewy v. Remington Arms Co.,* 836 F.2d 1104 (8th Cir. 1988) (the court gives guidance as to the factors a trial court should consider in determining whether to give a spoliation adverse inference instruction against a party that had a records retention policy under which relevant records were destroyed).

Prudent counsel also need to ensure that the obligations relating to preservation of evidence are fully understood by the actual users of the client's Information Technology (IT) system, especially the key players in the events that resulted in the litigation. If outside counsel communicate only with in-house corporate or government counsel and IT managers, there is a real risk that the very people for whom it is most important not to delete or destroy information will not be fully aware of their preservation responsibilities. The *Qualcomm* case illustrates the fallout to counsel and client for failing to address this properly.

Counsel also needs to focus on the potential preservation of evidence issues as soon as they begin to work on the case. If the law in the jurisdiction where the case is pending is clear on the duty to preserve, when the duty is triggered, and the scope of what must be preserved, then counsel know what the applicable standards are. If not, counsel need to get some clarity about what their clients should do. The first step is to attempt to negotiate with opposing counsel to obtain an agreement about what must be preserved, who must preserve information, and the scope of production. If these efforts are unsuccessful, counsel should consider filing a Rule 26(c) motion for a protective order to ask the court to clarify the disputed issues. If this approach is taken, take care to heed the advice of the court in

Thompson v. HUD and make sure that any motion filed contains particularized facts to support your position, as courts are not likely to give much weight to conclusory arguments by counsel in resolving issues that turn on factual considerations. You may need to attach affidavits from individuals with personal knowledge of the IT systems to explain why it would be burdensome or unfair to preserve information to the extent sought by opposing counsel. Pay particular attention to the Rule 26(b)(2) cost-benefit balancing factors discussed at length in *Thompson*. 219 F.R.D. 93 (D. Md. 2003). If highly technical facts are important to resolving the issue, be aware that the court may appoint a court expert to assist in resolving the dispute. Make sure any expert that you rely on is able to support his or her opinions.

In any dealings with the court, whether by way of a motion for protective order or in responding to a motion to compel, try to ensure that the position you are taking is reasonable and that Rule 26(g) has been strictly observed. Too often, counsel adopt an "all or nothing" approach which seldom impresses a court. Regardless of which side of an issue you represent, test the position you are asserting by asking yourself what the likely reaction of the judge will be to what you are advocating. If you have a good idea that the court is going to offer some discovery, do not argue against it. If it is likely that the court is going to simply order the opposing party to produce information and pay your reasonable attorneys' fees and costs, do not demand an adverse inference instruction and that the adverse party and its lawyer be held in contempt.

If you are seeking sanctions relating to the failure to preserve evidence, remember that most judges are cautious about imposing the harshest sanctions, such as evidence preclusion, striking pleadings/claims or defenses, and contempt. Do not ask for these sanctions unless you have a solid factual basis to do so. Remember that just because evidence that should have been preserved was not does not automatically mean the court will grant a request for an adverse instruction or impose other harsh sanctions. You also must demonstrate that the other party engaged in some form of negligence or more serious culpability, the information sought was relevant to your case, and that you were prejudiced by the loss or destruction. Such a showing will greatly enhance the likelihood of serious sanctions.

Finally, counsel must pay particular attention to the ethical issues regarding accessing and using metadata, as well as their obligations not to disclose confidential, privileged, or other sensitive information related to their client's interests. As the discussion has shown, no single position has been adopted by the states addressing these issues. This absence underscores a lawyer's need to know the position of every state's ethics authority in each state in which he or she practices. Hopefully, a solid understanding of the ethical and legal requirements relating to the preservation and production of ESI and adherence to the above common-sense suggestions will assist you in navigating the often turbulent waters of electronic discovery.❖

ABOUT THE AUTHOR

❑**Magistrate Judge Paul W. Grimm**'s legal career began in 1980 when he joined the State's Attorney Office for Baltimore County, Maryland as an Assistant State's Attorney. A year later, he became an Assistant Attorney General for the state of Maryland where he remained until 1984. From 1984 until 1997, Judge Grimm worked in private practice. On February 5, 1997, Judge Grimm was appointed a United States Magistrate Judge for the District Court for the District of Maryland. Judge Grimm has written numerous books and articles on evidence, procedure and trial practice, and is an adjunct faculty member of the University of Maryland and University of Baltimore Schools of Law. He is also a frequent participator in the Civil Trial Advocacy courses held at the National Advocacy Center.✠

I gratefully acknowledge the contributions of Elysha Carouge and Lauren Grossman, student interns, who assisted with this article.

The views expressed in this article are those of the author only and should not be construed as formal guidance. The article has not been adopted as the formal view of the District Court of Maryland, the Department of Justice, or any other federal agency. The article does not create any right or benefit, substantive or procedural, enforceable at law by any person against the United States, its agencies, officers, or any other person.

The Challenges of Electronic Discovery for Federal Government Attorneys under Recent Amendments to the Federal Rules of Civil Procedure

Theodore C. Hirt
Assistant Director
Federal Programs Branch
Civil Division

I. Introduction

Department of Justice (Department) and federal agency attorneys often encounter difficult or voluminous discovery demands in their civil cases, including demands for so-called "electronic discovery." The December 2006 amendments to the Federal Rules of Civil Procedure address electronic discovery issues explicitly. As judges and litigators become more familiar with how the new federal rules should operate, the federal government's counsel in each case need to know how to utilize those rules effectively. While compliance with the new federal rules does present some unique challenges, if counsel can master them, they should be able to represent the government's interests more effectively.

In this article, the new term of art for electronic discovery created by the amended federal rules, electronically stored information (ESI), is used. This article examines the principal highlights of the federal rules changes. It then addresses some of the specific impacts these changes will have on representing federal agencies in both affirmative and defensive litigation, and how the Department and agency

counsel can avoid some of the pitfalls presented by electronic discovery.

By now, every practitioner should have an updated federal rules book that contains these amendments. The Federal Rules of Civil Procedure, however, can also be accessed online from the Web site maintained by the Administrative Office of the United States Courts, *available at* http://www.uscourts.gov/rules/Congress0406.html.

II. Principal highlights of the rules changes

A. Federal Rule of Civil Procedure 26(f)—the role of ESI at the parties' "meet and confer" sessions

One of the first challenges for counsel in dealing with electronic discovery will be assessing and understanding the potential role of that type of discovery in the case as soon as possible.

As described below, ESI discovery has several complex features. ESI issues, however, should not obscure the more fundamental questions presented in all civil litigation. Although this may be self-evident, the "what" and "how" of discovery needs to be assessed with respect to overall case strategy, whether the objective is to bring an affirmative case to a successful conclusion, or is to secure dismissal of a case that has been brought against a federal agency or its officials. Discovery planning is a subset of overall case planning. Ask "What is the objective?" and, then, "What role does discovery have in meeting that objective?"

Department attorneys are already familiar with the provisions of Rule 26(f), under which they must "meet and confer" with opposing counsel concerning case scheduling issues, including discovery matters. Amended Rule 26(f) provides that at the parties' planning meeting, their counsel must discuss "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." FED. R. CIV. P. 26(f)(3)(C). Counsel also must discuss "any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order." *Id.* at 26(f)(3)(D). Finally, they must "discuss any issues about preserving discoverable information," that is, to ensure that ESI is not inadvertently destroyed during the pendency of the case. *Id.* at 26(f)(2). The parties' agreement on these issues, if accepted, will be set out in the court's Rule 16 scheduling order. *See* FED. R. CIV. P. 16(b).

Each of these topics is important to address at the "meet and confer" session. Postponing any of them is *not* advisable. First, and foremost, because counsel for the parties may be expected to discuss their clients' information systems at those sessions, the Advisory Committee's note admonishes that counsel should "become familiar with those systems before the conference." *See* FED. R. CIV. P. 26 Advisory Committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. Second, addressing what types of ESI will need to be preserved as the litigation proceeds will require that each party learn the range of potential ESI available for discovery and what ESI might be subject to automatic deletion or destruction during the pendency of the litigation. As the Advisory Committee's note emphasizes, the "[f]ailure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes." *See* FED. R. CIV. P. 26 Advisory Committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. As noted later in this article, counsel also should discuss the "form or forms" in which various types of ESI will be produced; doing so at this stage of the case will avoid later misunderstandings. Finally, it is important that counsel address the specific arrangements for the exchange of ESI that may include privileged information.

B. Federal Rule of Civil Procedure 26(b)(2)(B)— "Two-Tier" Discovery

The volume of potentially discoverable information in a case can be overwhelming, but how much information ultimately will be produced depends on many factors, including the relevance of the information and the burden or cost that is associated with its review and production. The most innovative change to the new rules, in the author's judgment, is the creation of the "two tier" discovery provisions of Rule 26(b)(2)(B). This rule creates a "reasonable accessibility" standard for the production of ESI, i.e., a party is under a duty to produce ESI from sources that the producing party identifies as "reasonably accessible." FED. R. CIV. P. 26(b)(2)(B). The party, however, may be able to limit the burden that otherwise might be imposed upon it and try to preclude discovery of ESI from sources that it identifies as *not* reasonably accessible because of "undue burden or cost." *Id.*

This rule recognizes that there can be considerable difficulties in locating, retrieving, and providing some varieties of ESI. As the Advisory Committee's note explains, in some situations, the storage of ESI may provide "ready access to information used in regular ongoing activities," and an organization's information system "may be designed so as to provide ready access to information that is not regularly used." *See* FED. R. CIV. P. 26 Advisory Committee's note (2006). But some systems may retain information on sources "that are accessible only by incurring substantial burdens or costs." *Id.* Although the complexities of this rule are discussed in an accompanying article, here are the "basics" on the rule's operation.

As noted earlier, the "meet and confer" session is the opportunity for counsel to discuss their anticipated discovery requests, and the burdens that may be imposed on the other party by those requests. Optimally, the parties will reach agreement on the scope of the discovery. If they do not do so, however, the rule creates a specific procedure for the resolution of their dispute. If a motion to compel or for a protective order is filed, "the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost." FED. R. CIV. P. 26(b)(2)(B). If the party is able to make that showing, the court may deny the discovery altogether. Alternatively, the court may still order discovery from those sources "if the requesting party shows good cause" under the limits and standards prescribed in Rule 26(b)(2)(C). *Id.* That reference incorporates the various factors courts use in evaluating whether the potential benefit of discovery will outweigh its costs.

An important feature of the rule is the district court's ability to set conditions for the "second-tier" discovery. The court may set limits on the "amount, type, or sources of information" to be produced, or it may mandate payment by the requesting party of "part or all of the reasonable costs" of obtaining such information. FED. R. CIV. P. 26 Advisory Committee's note (2006). Conditions for accessing the "second tier" of ESI might involve either a sampling of potentially relevant ESI, or some cost shifting or cost sharing, depending on the volume of ESI. For federal agencies from whom large volumes of ESI may be demanded, this provision could be of some assistance.

The Advisory Committee's note provides some common sense guidance to those who will grapple with the challenge of producing ESI: "The volume of—and the ability to search—much electronically stored information means that in many cases the responding party will be able to produce information from reasonably accessible sources that will fully satisfy the parties' discovery needs"; thus, "[i]n many circumstances the requesting party should obtain and evaluate the information from such sources before insisting that the responding party search and produce information contained on sources that are not reasonably accessible." *See* FED. R. CIV. P. 26 Advisory Committee's note (2006).

Finally, as the Advisory Committee's note cautions, a party's identification of sources of ESI as not reasonably accessible "does not relieve the

party of its common law or statutory duties to preserve evidence." *Id.* Whether the responding party has to preserve such unsearched sources will depend on the circumstances of the case. *Id.*

C. Federal Rule of Civil Procedure 26(b)(5)(B)—the exchange of privileged information during ESI productions

One frequent problem encountered in discovery is how to provide adequate protection to materials alleged to be privileged, and thus exempt from discovery. The sheer volume of ESI information that may be producible by an agency carries with it the burden of identifying, isolating, and reviewing the privileged information. For Department or agency counsel, this can be a significant problem.

Some practitioners—predominantly in the private sector—have addressed this issue through the development of agreed upon protective orders that include either a "claw-back" or "quick peek" procedure. Under the former procedure, each party agrees that inadvertent disclosure will not waive a party's right to claim privilege, if the producing party has released privileged information but requests its return within a reasonable period of time. Under the second procedure, the parties agree that the requesting party can view all of the producing party's information, which means that the producing party does not undertake any prescreening for privileged information. *See* Kindall C. James, *Electronic Discovery: Substantially Increasing the Risk of Inadvertent Disclosure and the Costs of Privilege Review—Do the Proposed Amendments to the Federal Rules of Civil Procedure Help?*, 52 LOY. L. REV. 839, 850-52 (2006).

New Rule 26(b)(5)(B) establishes a procedure to resolve disputes over whether specific information should remain privileged. If information is "produced in discovery [that] is subject to a claim of privilege or of protection as trial-preparation material," the party asserting that claim—which produced the information at issue—"may notify any party that received the information of [that] claim and the basis for it." FED. R. CIV. P. 26(b)(5)(B). The party that received the information, after being notified, "must promptly return, sequester, or destroy the specified information and any copies it has; [and] must not use or disclose the information until the claim is resolved." *Id.* If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it, and must preserve the information until the claim is resolved. The receiving party may promptly present the information to the court, under seal, for a determination of the claim.

This rule is one of procedure. It does not address whether the privilege or protection asserted by the producing party was waived by the production. Counsel need to consider the fact that nonparties are not bound by their agreement, nor even by a court order ratifying the parties' agreement. It is very important that counsel research the law of waiver in their jurisdictions as some circuits are quite strict in that respect. *In re Sealed Case*, 877 F.2d 977, 980 (D.C. Cir. 1989). One recent decision suggests that a protective order may insulate the parties from a later waiver assertion by nonparties but cautions counsel as to the uncertainty of the law in this area, and the need to justify why preproduction review for privileged information was not feasible. *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228, 244-46 (D. Md. 2005).

In September 2007, the Judicial Conference submitted to Congress proposed Federal Rule of Evidence 502. That rule would provide that a party's disclosure of information covered by the attorney-client privilege or work-product protection would not operate as a waiver, in a federal or state proceeding, if the disclosure was inadvertent, the holder of the privilege or protection took "reasonable steps" to prevent disclosure, and the holder "promptly took reasonable steps to rectify the error," including, if applicable, the procedures of Rule 26(b)(5)(B). A federal court "may order" that the privilege or protection is not waived by disclosure connected with the litigation pending before the court, "in

which event the disclosure is also not a waiver in any other Federal or State proceeding." This proposal can be found on the Judicial Branch's Web site, which is available at http://www. http://www.uscourts.gov/rules/newrules6.htm #proposed0806. Because the Federal Rules of Evidence are substantive law, enactment of this rule would resolve the waiver issue. In February 2008, the Senate passed a bill (S. 2450) that would enact the rule. *See* S. REP. NO. 264, 110 Cong. 2d Sess. (2008), *available at* http://www. thomas.gov.

In considering this issue, Department counsel need to bear in mind two other issues. First, agency clients may be particularly sensitive to the type of ESI that may be subject to a potential exchange. For example, can—or should—information protected by either the deliberative process privilege, or the law enforcement privilege, ever be made subject to this new rule? Second, neither the rule nor the Advisory Committee's note prescribes *when* the producing party is to notify the other parties that production of privileged material has occurred. This will be very fact-specific.

D. The Role of ESI in responding to interrogatories under Federal Rule of Civil Procedure 33(d)

Federal agencies often encounter the situation of opposing counsel serving voluminous or highly-detailed interrogatories. Responding to those interrogatories requires considerable time and effort by agency officials and counsel. Rule 33, however, permits a responding party to refer opposing counsel to agency records as the source of the interrogatory answers. The electronic discovery amendments now explicitly incorporate ESI into Rule 33. A responding party can specify ESI as the source for interrogatory answers. FED. R. CIV. P. 33(d).

Department attorneys are familiar with the experience of allowing an agency to permit the opposing counsel to inspect a bank of filing cabinets containing file folders of paper documents. Today, as agencies store more of their information electronically, it is foreseeable that an increased use of amended Rule 33 will occur. But, in some situations, access will be complicated. The Advisory Committee's note explains that if a producing party decides to make ESI available to respond to the interrogatory, it may need to give "technical support," such as compatible software, to the requesting party. *See* FED. R. CIV. P. 33 Advisory Committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_ Notes.pdf. This does not necessarily mean, however, access to the producing party's information systems. *Id.* Agencies will want to consider this problem as they contemplate their Rule 33 responses. Attorneys can anticipate that agencies will oppose unrestricted access by opposing counsel to their online databases, particularly in view of the sensitive information that is often stored there.

E. Federal Rule of Civil Procedure 34—The role of ESI

Although practitioners understand that information from computer databases may be responsive to Rule 34 requests, Rule 34(a) now explicitly makes ESI a new category of information that can be requested. FED. R. CIV. P. 34(a). While this is a helpful clarification, the amendments to Rule 34(b) will have more impact on practice. Rule 34(b) addresses the important and complex issue of the form of ESI production. This Rule seeks to introduce clarity into the Rule 34 process. It is designed so that each party will know the intentions of the other party with respect to the format of ESI production.

While some courts will expect that the "form of production" issue will be resolved by counsel early in the case, *before* the service of Rule 34 requests, Rule 34(b) now clarifies the procedure to be followed if there have been no prior agreements on this issue. This rule recognizes that the parties may not be able to resolve this issue during the earlier "meet and confer" process.

A request for ESI "may specify the form or forms in which electronically stored information is to be produced." FED. R. CIV. P. 34(b)(1)(C).

The responding party, in turn, may object to a requested form for producing ESI. If the responding party objects, it "must state the form or forms it intends to use." *Id.* at 34(b)(1)(D). Rule 34(b) creates a "default" provision in the event the parties have not agreed on the form of the ESI and the court has not entered an order as to form. "[I]f a request does not specify a form for producing [ESI], [the] responding party must produce it" in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." *Id.* at 34(b)(2)(E)(ii). An important feature to this rule is the limitation that "[a] party need not produce the same electronically stored information in more than one form." *Id.* at 34(b)(2)(E)(iii).

Counsel for the responding (producing) party will need to be clear and precise in his or her objections to a request for a specific ESI format, and in explaining the format(s) in which he or she proposes to produce the various types of ESI. As is the case with the Rule 33 response, the producing party may need to "translate" information that it produces into a "reasonably usable" form. This may mean the party will have to provide "some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information." *See* FED. R. CIV. P. 34 advisory committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

Federal agencies need to exercise care in how they undertake their ESI productions. The Advisory Committee's note warns that the option to produce in a reasonably usable form does not mean that the producing party can convert the ESI from the form in which it is ordinarily maintained "to a different form that makes it more difficult or burdensome" for the requesting party to use "efficiently" in the litigation. *See* FED. R. CIV. P. 34 advisory committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. One issue left unresolved by the amended Rule is whether a party must produce ESI in "native format" or through creating an image, such as portable document format (PDF) or tagged image file format (TIFF). There are cases on both sides of this issue, reflecting the fact that the issue is very case-specific. *Compare Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005) (holding that Excel spreadsheet had to be produced in native format), *with Michigan First Credit Union v. Cumis Ins. Soc'y, Inc.*, 2007 WL 4098213 (E.D. Mich. Nov. 16, 2007) (holding that defendant did not need to produce e-mail in native format (with metadata)).

F. The "Safe Harbor" provision of Federal Rule of Civil Procedure 37(e)

Rule 37(e), the so-called "safe harbor" from sanctions, is an innovation in the new rules. Effective December 2007, the former Rule 37(f) became the current Rule 37(e). This occurred in conjunction with the "restyling" of the Civil Rules in an effort to make them simpler to understand. On its face, this rule seems straightforward. "Absent exceptional 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." FED. R. CIV. P. 37(e). The Advisory Committee's note explains that "the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part." FED. R. CIV. P. 37 advisory committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. "Ordinary operation" encompasses the various ways in which information systems are "generally designed, programmed, and implemented to meet the party's technical and business needs" and this can include "alteration and overwriting" of information through automatic functioning. *Id.*

These statements do not exonerate litigants from being held responsible for the accidental deletion of ESI in situations involving pending or reasonably anticipated litigation. The note explains that "good faith," as described in the rule, may require the party's intervention "to modify or suspend certain features of that routine operation

to prevent the loss of information, if that information is subject to a preservation obligation." *Id.* Practitioners are familiar with the term "litigation hold," the instruction to a client that it preserve potentially relevant information for litigation. In order to be able to rely on Rule 37(e)'s "safe harbor" from sanctions, counsel will need to implement a reasonable litigation hold to prevent the routine destruction of ESI. *See*, *e.g.*, *Zubulake v. UBS Warburg*, 220 F.R.D. 212, 216-19 (S.D.N.Y. 2003).

Rule 37(e), itself, does not create new legal duties. A party's duty to preserve information arises out of common law and, in some situations, specific statutory or regulatory responsibilities. Why is this important? Otherwise, the party, or its counsel, could be held to have engaged in "spoliation" of the evidence if information was destroyed. "Spoliation is the destruction or significant [physical] alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999). Sanctions for engaging in spoliation can include the recovery of costs and attorney fees, exclusion of evidence or testimony, or even an adverse evidentiary inference ("that the [destroyed] evidence would have been unfavorable to the party responsible for its destruction"). *Id*; *see Zubulake v. UBS Warburg*, 229 F.R.D. 422, 430 (S.D.N.Y. 2004).

G. Federal Rule of Civil Procedure 45: subpoenas requiring the production of ESI

The rules amendments contain important changes to Rule 45, which governs the discovery of information from nonparties. Amended Rule 45 incorporates the changes made in Rule 34(b) governing the form of production of ESI, the "two tier" provision of Rule 26(b)(2)(B), and the procedures of Rule 26(b)(5)(B) for assertion of privilege. FED. R. CIV. P. 45. These changes should prove to be of considerable assistance to federal agencies, which can encounter significant problems in responding to discovery demands in private litigation. Just as courts have recognized the burdens that Rule 45 can impose on nonparties, Department attorneys will want to rely on these rules in advocating reasonable limits on the scope and volume of ESI subpoenaed from federal agencies. *See Guy Chem. Co. v. Romaco AG*, 243 F.R.D. 310, 313 (N.D. Ind. 2007) (holding that defendant's subpoena of private nonparty's ESI would impose a substantial burden upon it, justifying the defendant paying for the costs of that discovery).

III. How Department attorneys can use these rules effectively

It is widely understood that the new rules will pose, for some practitioners at least, a range of new, or even unanticipated challenges in dealing with ESI-related issues during discovery. If this news is of any comfort to federal agencies, it means, at the very least, that courts and litigants will be learning the operation of these rules for the next several years. During this transition period, however, the objective should be to become as proficient as possible in handling ESI discovery.

For Department and federal agency attorneys, the challenges in dealing with ESI will be similar to those faced by private sector practitioners. While cases will differ in the complexity of ESI issues, there are some practical steps that counsel should take. Being proactive in this area is an advantage.

Given the courts' expected emphasis on the "meet and confer" sessions, it is imperative that federal agency attorneys learn about their clients' information systems *before* litigation is filed.

Each agency needs to create a formal inventory of its ESI sources. This will mean:

- determining whether those sources are centrally or locally distributed;
- in what media they reside; and
- how long information is kept on those ESI systems without being overwritten, deleted, or otherwise destroyed.

Agencies need to learn and document the nature of their information technology systems

and operations, identify who is in charge of agency servers, and identify who will be involved in the discovery process. Agency personnel (including counsel) should invest that time now. They should include "orientation" sessions with the agency's information technology staff and agency records management staff. These orientation sessions will be important because, as the Advisory Committee's note suggests, one result of a "meet and confer" session may be the deposition of an information technology expert. *See* FED. R. CIV. P. 26 advisory committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

Advance work will enable agency counsel to be better prepared to comply with discovery requests. Over time, attorneys can count on federal district judges and magistrate judges expecting counsel for the parties to be extremely well prepared to address ESI issues comprehensively at the "meet and confer" sessions and in conferences with the court. When counsel fails in that respect, the court, at the very least, will express criticism or impatience. *See In re Seroquel Prod. Liab. Litig.*, 244 F.R.D. 650, 653, 656 (M.D. Fla. 2007) (imposing sanctions and criticizing defendant's counsel for failure to investigate client's information systems). In developing the agency's position on these issues, it is also important to know the agency's objective as to the expected duration of the litigation and the corollary duration and scope of its preservation obligations.

In addition, counsel need to be aware that individual district courts, or even judges in those courts, may develop more specific rules, as "supplementary" to the national rules, for the resolution of electronic discovery issues. By one count, at least 30 district courts (or individual judges within those districts) already have developed rules or protocols. Some of these additional requirements are quite complicated. Expect that such courts will utilize these rules to impose additional demands on counsel. (For an overview of local rules, see a private law firm's Web site devoted to e-discovery issues, *available at* http://www.ediscoverylaw.com/2007/10/articles/resources/updated-list-local-rules-of-united-states-district-courts-addressing-ediscovery-issues.)

Here are some practical suggestions for addressing other frequently-encountered ESI issues.

- First, in both Rules 33 and 34 demands and responses, be specific as to the location of ESI and the format for its production. Try to secure an agreement as to each specific issue so that there are no misunderstandings later.
- Second, be careful to document whatever agreements are made with opposing counsel, not only as a result of any "meet and confer" sessions, but also other ESI discovery issues.
- Third, if either counsel demands "second-tier" discovery from the opposing party, be sure that the reasons why that information is important to the case are effectively advocated.
- For the producing party, be prepared to document which sources of ESI were accessed and at what cost. Be prepared to submit detailed declaration(s) from the agency's information technology staff describing why it would be an undue burden to produce the demanded information. Finally, confer with the agency on whether cost sharing or cost shifting is feasible in the case.

IV. Conclusion

Attorneys can expect that the electronic discovery rules will direct and focus the Department's efforts to manage the large volumes of ESI maintained by our client agencies for some time to come. Discovery demands of the opposing party also will be evaluated for proper scope and relevance, and subject to the "proportionality" principles of Rule 26(b). The amended discovery rules, however, are not a panacea for the hard work involved in managing ESI issues, and no one should minimize the challenge or the effort to manage the various tasks of retrieving, searching, and producing ESI. The challenge for Department

attorneys and their colleagues in the federal agencies will be how to undertake those efforts to ensure that discovery demands, and the overall case, can proceed effectively.❖

ABOUT THE AUTHOR

❑**Theodore C. Hirt** is an assistant director in the Federal Programs Branch, Civil Division, of the Department of Justice. Mr. Hirt has been extensively involved in the federal rule-making process in his capacity as an advisor to the Assistant Attorney General for the Civil Division. He serves as an ex officio on the Civil Rules Advisory Committee, and as the Coordinator of the Department's E-Discovery Working Group and has given numerous presentations on Rules issues.

Investigations and Prosecutions Involving Electronically Stored Information

Andrew D. Goldsmith
First Assistant Chief
Environmental Crimes Section
Environment & Natural Resources Division

Lori A. Hendrickson
Assistant Chief
Western Criminal Enforcement Section
Tax Division

I. Introduction

The topic of "e-discovery" has been on the leading edge of civil litigation over the past several years. *See, e.g.,* "The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery," Sedona Conference Working Group Series (Jan. 2004), *available at* http://www.thesedona conference.org/dltForm?did=SedonaPrinciples200 303.pdf. Although there has not been a similar focus on criminal investigations and prosecutions that involve electronically stored information (ESI), this subject is becoming increasingly important in practice. The 2006 amendments to the Federal Rules of Civil Procedure, including a mandatory "meet and confer" session regarding electronic documents, have caught the attention of criminal litigants as the possibility of similar practices in their field has grown. *See* FED. R. CIV. P. 16, 26, 33, 34, 37. Nonetheless, the criminal bar is generally far behind their civil brethren in terms of their approach to e-discovery. This is somewhat surprising given that civil litigants and criminal prosecutors appear before the same judges and magistrates, and interact with similar information technology (IT) personnel at law firms. For these reasons, prosecutors should be aware that federal judges may hold them to certain standards common to civil litigation. *See United States v. O'Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008).

Clearly, the future is now for criminal prosecutors as far as ESI principles and practices in their investigations and prosecutions. This article explains some methods that law enforcement officials can use to obtain ESI, the use of ESI during discovery and at trial, and prosecution for offenses involving ESI's improper manipulation. It concludes with a discussion of ethical obligations in the context of metadata. Importantly, as prosecutors consider their e-discovery strategy, they should recognize that ESI is not necessarily a one-way street. While this topic is beyond the scope of this article, practitioners with questions in this area should feel free to contact Mr. Goldsmith (andrew.goldsmith@usdoj.gov) or Ms. Hendrickson (lori.a.hendrickson@usdoj.gov).

II. Obtaining ESI

At the outset, the prosecutor has to make certain decisions regarding the approach to the investigation. Notably, the usual considerations as to whether to seek a grand jury subpoena or search warrant apply where ESI evidence is sought.

- Who has, or should have, custody and control over the pertinent information?
- Is there a reasonable basis to believe evidence may be destroyed, altered, or removed if a subpoena is issued?
- Is there probable cause for a warrant?
- Can the scope of the information requested be narrowly defined?
- How likely is it that a party may seek, and the court may grant, a protective order setting parameters for production in response to the grand jury subpoena (e.g., assertion of attorney-client privilege)?
- Is it likely that third-party subpoenas will present a battle (e.g., grand jury subpoena to internet service provider under 18 U.S.C. § 2703 (2006))?

Definitions can be critical. For example, the apparently simple definition of "document" can have far-reaching implications. A broad definition of document might read: "electronically stored data from which information can be obtained . . . such as computer drives, diskettes, computer tape, CDs, and DVDs." (Example of typical subpoena language). More specific subpoena language, typical in the antitrust context, could read as follows:

> [t]he term "documents" means all written, recorded, and graphic materials and all electronic data of every kind in the possession, custody or control of the company. The term "documents" includes electronic mail or correspondence, drafts of documents, metadata, embedded, hidden and other bibliographic or historical data describing or relating to documents created, revised, or distributed on computer systems . . . . Thus, the company should produce documents that exist in electronic form, including data stored in personal computers, portable computers, workstations, minicomputers, personal data assistants, archival voice storage systems, group and collaborative tools, electronic messaging devices, portable or removable storage media, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of online or offline storage, whether on or off company premises. . . .

(Example of typical subpoena language).

If the prosecutor chooses to proceed via grand jury subpoena, she must consider how compliance will take place. Several questions abound. How broad should the subpoena be (including the time period)? Can the government agree to narrow the subpoena's scope? Will production be ongoing or rolling? Does the government need originals, or will copies suffice? When the subpoena calls for electronic data (e-data), the recipient must first take steps to identify, preserve, and harvest—or cull—the data before it can be provided to the grand jury. As explained in more detail in Section III, *infra*, there may be a duty to preserve ESI *prior* to receipt of a subpoena.

In light of these considerations, the prosecutor should consider possible approaches to developing information about ESI in the grand jury. For example, the prosecutor might obtain a broad subpoena with a reasonable target window for compliance (2 months out). The prosecutor could then subpoena an IT person from the subject or target company for appearance in the grand jury to obtain testimony describing the data that exists, where that data is located, and what the company's retention policies and practices are for paper and electronic information. In so doing, the grand jury investigation would be appropriately focused to ensure that ESI has been properly preserved, searched, and transmitted.

III. Duty to identify and preserve ESI

In seeking electronic information, prosecutors should recognize that e-data is persistent, voluminous, and in varied locations. There are many places where data could reside, such as in desktops, laptops, PDAs, digital cameras, off-site storage, e-mail servers, back-up tapes, Blackberries, thumb drives, and other electronic consoles.

Efforts to fulfill the duty to preserve the electronic information can be time intensive. General preservation steps include issuing a litigation hold to suspend routine document retention/destruction policies. Automatic deletion policies must be reviewed and sometimes halted, and notice must be given to affected employees, vendors, and contractors. In appropriate cases, such as where there may be concerns about the recipient's ESI practices, the prosecutor may consider specifying in the grand jury subpoena that the recipient should suspend auto-deletion practices (if not already suspended), including recycling back-up tapes and desktop computers.

An important part of the preservation process for the party receiving the subpoena is to comb through the network-shared files and home directories, engage in forensic imaging of desktops and laptops if appropriate, and evaluate the effect of routine computer and system upgrades on stored data. It is crucial to understand that deliberately ignoring preservation requirements could result in prosecution for obstruction of justice. This is particularly true following Congress's passage of the Sarbanes-Oxley Act (SOX) in response to the Supreme Court's decision in *United States v. Arthur Andersen*, 544 U.S. 696 (2005) (overturning conviction under 18 U.S.C. § 1512(b) (2008)) because of defective jury instructions). In *Andersen*, an accounting partner in charge of the Enron account directed staff to revive a little-used document destruction policy after learning of the investigation. These SOX statutes, set forth in 18 U.S.C. §§ 1512(c) and 1519 (2002), are discussed in Section V *infra*.

Prosecutors should demand documentation concerning the methods used by subpoena recipients to preserve, collect, process, and produce data. This documentation should include any forensic tools and protocols employed, culling methods, search terms, review instructions and tools, and chain of custody. For crimes that span several years, the prosecutor should also ask how long the current policies and procedures have been in place and how they have changed over time. Where the investigation may also involve ongoing business practices, the prosecutor should consider requiring documentation on how data is archived.

In addition to specifying the procedures connected to the preservation step, prosecutors should request that parties responding to grand jury subpoenas utilize properly-trained personnel to identify, harvest, and produce ESI. Moreover, the government should utilize law enforcement officials with sufficient expertise to ascertain whether data was improperly deleted, wiped, or hidden. These individuals can often determine whether data was tampered with by reviewing electronic information hidden from the untrained eye. Finally, the government may consider using privately-retained experts to determine whether data was transferred, printed, copied, created, modified, or deleted.

IV. Form of production of ESI

The initial default for prosecutors should be to demand that parties produce information in the form in which it was originally generated. Thus, if documents (such as bills of lading, receipts, or letters bearing original signatures in ink) were originally generated in hard-copy form, prosecutors should demand original hard copies. Even if the prosecutor agrees to receive electronic copies of documents that have been scanned onto electronic media, the producing party should be required to retain the original documents and to produce them, if requested. This is particularly critical if the case goes to trial, where the prosecutor will likely want to show the jury the true original versions of documents, complete with "wet (ink) signatures," coffee stains, and staple holes, all indicia that the documents are, in fact, genuine.

If information was originally generated in electronic format—such as word processing, spreadsheets, or e-mails—prosecutors should consider whether to demand production of this information in its "native format." Evidentiary concerns may weigh in favor of receiving data in native format. Also, the ability to view and search ESI in native files, including spreadsheets, databases, e-mails, and metadata, is far preferable. Some parties may balk at producing ESI in native form, citing document control and number issues, claimed fear of evidence tampering, and production of "metadata" (explained *infra* at Section VI).

Increasingly, paper documents are provided in criminal cases in tagged image file format (TIFF) and portable document format (PDF). PDF is a file format developed by Adobe System that enables documents, once converted to this format, to be readable outside of the application that created them. TIFF is a format developed by Aldus and Microsoft commonly used for exchanging bitmapped graphics images between application programs. When the prosecutor chooses to accept documents in one or both of these formats, he or she should ensure that there is preservation of the native forms of the documents.

When the prosecutor provides voluminous records in discovery, such as bank account transactions and evidence seized in search warrants, these are often in TIFF or PDF format, as a result of being scanned by the investigating agency. After indictment, the prosecutor may provide this information on compact discs or digital versatile discs, supplemented by a written index to assist the defense in their review. Where the government provides discovery in convenient electronic format with searchable text, it will be more difficult for defense counsel to refuse to reciprocate.

Over the past decade, many new courtrooms have been outfitted with equipment to facilitate electronic presentation of evidence. Many judges and jurors now expect the government to present a polished, cohesive presentation with technical expertise. Creating the presentation is much less time-consuming when the government already is handling discovery in electronic fashion, as the information can usually be imported directly to Sanction, Trial Director, or similar programs for presentation at trial.

Some downsides to the TIFF and PDF formats—whether for paper or electronic documents—is that outside litigation support vendors often must create them, they usually do not retain metadata, and they do not work well for databases or other nonpaginated evidence. In some situations, the government will want to obtain and utilize all or part of another entity's preexisting electronic database. This can include databases created by civil private plaintiffs, regulatory agencies (e.g., Occupational Safety and Health Administration), or civil governmental litigants, which, because they are already easily viewable, can save all parties involved time and money.

In recent years, banks have been willing to respond to financial subpoenas in electronic format, as it saves hours of research time spent locating and printing individual deposit items or checks. When dealing with a large nationwide bank in a complex case, it also may be possible for the investigating agency to use forfeiture

funds to purchase the bank's proprietary software, if needed. This allows immediate manipulation of the subpoenaed records without the need to convert the data into a format compatible with government software.

Finally, prosecutors should be prepared to address issues relating to privilege logs. Production of these logs requires document date, author, recipient, others given copies, a description of the subject matter and the privilege asserted and why, and references to the subpoena paragraph(s) to which it is responsive. Failure to provide a complete log substantiating the privilege(s) asserted may constitute a waiver. *See In re Grand Jury Subpoena*, 274 F.3d 563, 576 (1st Cir. 2001).

V. E-data crimes

Prosecutors should bear in mind that criminal conduct involving the destruction and alteration of ESI has a dual evidentiary effect.

- First, the conduct may constitute a crime in and of itself (e.g., SOX obstruction offenses).
- Second, it can demonstrate consciousness of guilt concerning the substance of the e-data sought to be destroyed or altered (e.g., deleting e-mails pertaining to air sampling may serve to prove guilty knowledge of underlying Clean Air Act charge).

See, e.g., Edmonds v. United States, 273 F.2d 108, 114-15 (D.C. Cir. 1959) (jury could consider whether murder defendant's actions to remove potentially incriminating evidence indicated a consciousness of guilt); *see also* BUREAU OF NATIONAL AFFAIRS, DIGITAL DISCOVERY & E-EVIDENCE REPORT (Aug. 1, 2007) and BUREAU OF NATIONAL AFFAIRS, WHITE COLLAR CRIME REPORT (Aug. 3, 2007), *available at* http://www.ddee.bna.com. A shorthand formula to keep in mind when thinking about ESI-related crimes is as follows: ESI destruction/alteration = crime itself + consciousness of guilt for underlying offense.

Generally, ESI-related crimes can arise where a company responds to regulatory or administrative inquiries and investigations (including from federal and state agencies), as a result of investigations conducted by the company's own attorneys, or is in relation to, or in contemplation of, a criminal investigation. This broad swath of circumstances reflect the far legal reach of SOX's document destruction offenses. Under 18 U.S.C. § 1512(c) (2008)), "whoever corruptly alters, destroys, mutilates, or conceals a record, document, or other object . . . with the intent to impair the object's integrity or availability for use in an official proceeding" faces a 20-year term of imprisonment. 18 U.S.C. § 1512(c)(1). Under 18 U.S.C. § 1519 (2002),

> whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction . . . of the United States . . . or in relation to or contemplation of any such matter . . .

similarly faces a 20-year prison term.

Under these SOX statutes, altering or modifying paper or electronic documents or data may be a crime even though documents and data are not actually destroyed. Additional crimes may occur when e-documents or e-mails are deleted, wiped, or altered. They may also exist even when no official "investigation" is pending or imminent, and no grand jury, civil, or administrative subpoena has been issued. It is sufficient that the act is done "in relation to or contemplation of" any matter of investigation. 18 U.S.C. § 1519 (2002).

Early prosecutions under § 1519 demonstrate the far reach of these laws. In *Atlantic States*, following an 8-month trial, the longest environmental crimes-related trial in United States history, the company was convicted on 32 of 33 counts and four managers were also convicted of numerous crimes. *United States* v. *Atl. States Cast Iron Pipe Co.*, 2007 WL 2282514 (D.N.J. Aug. 2, 2007). The § 1519 conviction, one of the earliest guilty verdicts by a jury under

this statute, was based on the defendants altering the condition of a cement mixer and hiding the fact that safety switches had been bypassed before OSHA arrived to investigate an accidental amputation. *Id*.

Several courts have applied § 1519 in the ESI context. For example, in one case, the target of a grand jury investigation took steps to destroy e-mails after he received a grand jury subpoena. The government relied on § 1519 to support its pursuit of the crime fraud exception as the attorney had potentially assisted the target in this scheme to delete e-mails on the computers of an organization. *In Re: Grand Jury Investigation*, 445 F.3d 266, 275-76 (3d Cir. 2006). In another case, after the defendant Chief Executive Officer learned of a federal grand jury investigation, he attempted to suddenly implement an e-mail "retention" policy in which employees' e-mails would be deleted after 6 months and deleted other relevant files from his laptop computer, his desktop computer, and an employee's computer. *United States v. Ganier*, 468 F.3d 920 (6th Cir. 2006). The defendant was charged with, *inter alia*, three counts of violating § 1519. (The issue before the Sixth Circuit concerned the United States' expert disclosure obligations under Rule 16 when it planned to call a forensic computer specialist to describe what files had been deleted after receipt of a grand jury subpoena.)

In another prosecution, an audit partner of an accounting firm received a request from the Office of Comptroller and Currency for part of the company's working file. In response, the partner added and deleted information in relevant documents and reset the date in a computer on which alterations were made to make it appear that they had occurred during the audit. *United States v. Trauger*, No. 03-CR-00308-JSW (N.D. Cal., Oct. 14, 2003). In January 2005, after pleading guilty to violating § 1519, the partner was sentenced to 12 months in prison. *See* FBI-Department of Justice Press Release, *available at* http://sanfrancisco.fbi.gov/dojpressrel/2005/trauger013105.htm.

In addition to the SOX crimes related to the mishandling of ESI, there are several other potential crimes. For example, where several people agree to delete e-mails after they learn of a potential government investigation—whether criminal, civil, or regulatory in nature—they each potentially could also be prosecuted for a *Klein* conspiracy under 18 U.S.C. § 371 (1994). *United States v. Klein*, 247 F.2d 908 (2d Cir. 1957). This conduct would also violate § 1519. Another potential statute is 18 U.S.C. § 1503 (1996), a different obstruction of justice offense. In *Lundwall*, the district court held that the defendants could be prosecuted under § 1503 when they allegedly withheld and destroyed documents sought during discovery between private litigants in a civil case. *United States v. Lundwall*, 1 F. Supp. 2d. 249 (S.D.N.Y. 1998). The crime of misprison of a felony is another possibility, committed when a person has knowledge of a felony, does not advise the judge about it, and takes some deceptive step (this can even include misleading the company's attorneys). 18 U.S.C. § 4 (1994).

VI. Ethical duties with regard to handling another party's metadata

Lawyers, including prosecutors, can have special duties as receivers of metadata that was inadvertently included in discovery productions or otherwise. This can arise, for example, when a prosecutor receives metadata as part of ESI obtained pursuant to a grand jury subpoena, through a search warrant, or even when a draft letter is received by e-mail from a defense attorney. Metadata is hidden data within ESI. Metadata, "which most computer users never see, provides information about an electronic file, such as the date it was created, its author, when and by whom it was edited, [and] what edits were made." 3 BARBARA J. ROTHSTEIN, RONALD J. HEDGES, & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES (2007), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf. This part discusses

lawyers' ethical duties when receiving metadata that was sent inadvertently. In order to highlight the lack of uniformity in this area, this section will focus on opinions from the American Bar Association (ABA) and the District of Columbia, Maryland, Virginia, and New York Bar Associations on this subject.

Although "[t]he Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's review and use of [metadata]," ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) (discussing the Review and Use of Metadata), the ABA concluded that the rules "generally permit" a recipient lawyer to review and use such inadvertently sent information contained in e-mail and other electronic documents received from opposing counsel, so long as the recipient lawyer promptly notifies the sending lawyer that potentially privileged metadata was received. *Id.* Such review by the recipient lawyer would not, according to the ABA, violate Rules 8.4(c) and (d) that prohibit conduct "involving dishonesty, fraud, deceit, or misrepresentation" or "that is prejudicial to the administration of justice." *See id.* at n.10, *available at* http://www.pdfforlawyers.com/files/06_442.pdf; *see* ABA Model Rules 8.4(c) and (d), *available at* http://www.law.cornell.edu/ethics/aba/current/ABA_CODE.HTM#Rule_8.4. Even if the lawyer does not wish to review the metadata, however, she must nonetheless notify the sending lawyer.

To support its conclusions, the ABA draws from the "most closely applicable rule," Rule 4.4(b), which states "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows, or reasonably should know, that the document was inadvertently sent, shall promptly notify the sender." ABA Model Rule 4.4(b), *available at* http://www.law.cornell.edu/ethics/aba/current/ABA_CODE.HTM#Rule_4.4. Comment 3 to Rule 4.4(b) indicates that a lawyer who receives an inadvertently sent document ordinarily may, "but *is not required* to," return it without reading it, as a matter of that lawyer's professional judgment. ABA Formal Op. 06-442 (emphasis added). Thus, it seems that for the ABA, the recipient lawyer's duty to diligently represent her client under Rule 1.3 outweighs the protection of the sending lawyer's client confidences under Rule 1.6. *See* ABA Model Rules 1.3, 1.6, *available at* http://www.law.cornell.edu/ethics/aba/.

In the District of Columbia, however, when the receiving lawyer has actual prior knowledge that the sending lawyer inadvertently sent metadata in a document, the receiving lawyer cannot review and use it. In fact, the receiving lawyer has an affirmative obligation to consult the sending lawyer to determine whether to return or destroy the document. D.C. Legal Ethics Comm., Op. 341 (no date given) (discussing Review and Use of Metadata in Electronic Documents), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions.cfm; District of Columbia Rules of Professional Conduct 4.4(b), Cmt. 2 & 3 (discussing respect for rights of third persons), *available at* http://www.dcbar.org/new_rules/rules.cfm; District of Columbia Rules of Professional Conduct 8.4 (discussing misconduct), *available at* http://www.dcbar.org/new_rules/rules.cfm. The District of Columbia Bar departs from the ABA in that the ABA requires the "receiving lawyer only to notify the sender in order to permit the sender to take protective measures," ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006), *available at* http://www.pdfforlawyers.com/files/06_442.pdf, whereas the D.C. Bar precludes use of the data and requires the receiving lawyer to wait for the sending lawyer to notify her whether to return or destroy the document. District of Columbia Rule 4.4(b) Cmt. 2 (respect for rights of third persons), *available at* http://www.dcbar.org/new_rules/rules.cfm.

Where the "privileged nature of the document is not apparent on its face, however, there is no obligation to refrain from reviewing it, and the duty of diligent representation under D.C. Rule 1.3 may trump confidentiality concerns." D.C. Legal Ethics Comm. Op. 341 (no date given) (discussing Review and Use of Metadata in

Electronic Documents), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions.cfm; District of Columbia Rules of Professional Conduct 1.3 (discussing diligence and zeal), *available at* http://www.dcbar.org/new_rules/.cfm. Examples of cases in which the receiving lawyer has actual prior knowledge include those in which the receiving lawyer is told by the sending lawyer of the inadvertence before the receiving lawyer reviews the document or where the receiving lawyer immediately concludes, upon review of the metadata, that the protected information was not intentionally included. D.C. Legal Ethics Comm. Op. 341 (no date given) (discussing Review and Use of Metadata in Electronic Documents), *available at* http:www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions.cfm.

Unlike the D.C. Bar and ABA, the Maryland Bar places no ethical obligation on the receiving lawyer to refrain from review or use of the metadata prior to determining whether the sending lawyer intended to include that metadata. Maryland State Bar Ass'n, Inc. Comm. on Ethics, No. 2007-09. The Maryland Bar merely suggests that the receiving lawyer "can, and probably should, communicate with his or her client concerning the pros and cons of whether to notify the sending attorney and/or to take such other action which they believe is appropriate." *Id., available at* https://www.lexisnexis.com/applieddiscovery/LawLibrary/CourtRulesArticles/MarylandEOonMetadata.pdf.

For receiving lawyers, the New York Bar prohibits the use of technology to surreptitiously examine and trace e-mail and other electronic documents. New York State Bar Ass'n Ethics Op. 749 (Dec. 14, 2001). Further, "absent an explicit direction to the contrary, [sending counsel] plainly does not intend the [receiving counsel] to receive the 'hidden' material or information about the authors of revisions to the documents." New York State Bar Ass'n Ethics Op. 782 (Dec. 8, 2004) (discussing relevance of inadvertent and nauthorized disclosure cases). This portion of the opinion indicates that unless the sending lawyer expressly authorizes the receiving lawyer to review or use the metadata, the receiving lawyer cannot examine such material.

Although the Virginia Bar gives no opinion specifically addressing metadata, it prohibits a lawyer from "keep[ing] and us[ing] documents inadvertently transmitted to him by opposing counsel." Virginia State Bar Legal Ethics Op. 1702 (discussing confidentiality of initial consultation). Further, if the receiving lawyer recognizes that the information was confidential and misdirected, the receiving lawyer must not read the communication and must immediately notify the sending lawyer and abide by whatever instructions the sending lawyer may give with regard to the disposition of the communication. *Id.*, *available at* http://www.vsb.org/profguides/FAQ_leos/LEO1794.html.

From a technological standpoint, the issue of metadata is highly relevant, as professionals increasingly rely on electronic mail as a method of both general correspondence and the transfer of electronic documents. Prosecutors are increasingly facing this subject as well, since many documents sought by the government will include metadata. In the area of professional responsibility and legal ethics, the topic is just as relevant. Like all lawyers, prosecutors and other government lawyers who receive documents inadvertently containing metadata may have certain obligations, depending on the jurisdiction where the matter arises and their own state bar rules. Prosecutors should be aware of what they can and should do, recognizing that courts customarily hold government lawyers to the highest standards of ethics. These situations can arise even when undertaking a task as seemingly mundane as corresponding with opposing counsel via e-mail.

VII. Conclusion

The collection, preservation, and potential manipulation of ESI will be increasingly encountered in federal criminal investigations and prosecutions. It is incumbent upon the prosecutor to know the promise and potential peril of

demanding ESI production, including issues relating to metadata.❖

ABOUT THE AUTHORS

❑**Andrew D. Goldsmith** is the First Assistant Chief of the United States Department of Justice, Environment and Natural Resources Division, Environmental Crimes Section. Prior to joining the Environmental Crimes Section in 1997, he served as Chief of the Environmental Crimes Unit of the New York Attorney General's Office, as an Assistant United States Attorney in the District of New Jersey, and as an Assistant District Attorney in the Manhattan District Attorney's Office. Mr. Goldsmith regularly serves as an instructor for the Office of Legal Education at the National Advocacy Center.

❑**Lori A. Hendrickson** is the Assistant Chief of the United States Department of Justice, Tax Division, Western Criminal Enforcement Section. Prior to joining the Tax Division in 1998, she was a Special Agent with the Internal Revenue Service, Criminal Investigation Division, in Cleveland, Ohio for 11 years.✠

The authors wish to thank Mark G. Eskenazi (J.D. expected May 2008, Georgetown University Law Center), a law intern during the Spring 2008 with the Environmental Crimes Section of the Justice Department, for his assistance in the preparation of this article.

The views expressed in this article are those of the authors only and should not be construed as formal guidance. The article has not been adopted as the formal view of the Environment and Natural Resources Division, the Tax Division, the Department of Justice, or any other federal agency. The article does not create any right or benefit, substantive or procedural, enforceable at law by any person against the United States, its agencies, officers, or any other person. Department attorneys who are considering their own responsibilities in handling metadata should contact their component or division's Professional Responsibility Officer or the Department's Professional Responsibility Advisory Office.

Working with Expert Witnesses in the Age of Electronic Discovery

Adam Bain
Senior Trial Counsel
Environmental Torts Section
Torts Branch
Civil Division

I. Introduction

Expert witnesses are an important part of almost every civil case. Often an expert's testimony will make the difference between winning or losing a case. Additionally, expert reports and deposition testimony are often crucial in pretrial motions practice and in obtaining a favorable settlement for the client. Because they are so important, attorneys naturally want to work closely with experts in assessing the strengths and weaknesses of a case, in preparing expert reports, in deposing fact and expert witnesses, and, ultimately, in presenting a case at trial.

Attorneys should be aware that, under the current Federal Rules of Civil Procedure, their

communications with experts are likely subject to discovery as information that the expert "considered." Usually attorneys will not be able to assert an attorney work-product protection, or any other privilege, to guard their communications with experts from discovery. Opposing parties may seek information revealing interactions between attorneys and their experts in order to show undue attorney influence and bias. Moreover, with the 2006 amendments to the Federal Rules of Civil Procedure regarding electronically stored information (ESI), the information that parties may seek will likely include e-mails between experts and attorneys, as well as electronic "draft" versions of expert reports. Unless and until the Federal Rules are changed to protect this information from discovery, attorneys should be aware that their opponents may be able to discover what the lawyer may otherwise view as "work product," if it is disclosed to an expert in an electronic communication or if it is reflected in changes to an expert report. Conversely, attorneys should know that they can seek this information from their opposing experts to cross-examine the expert, or even to challenge the admissibility of the expert's opinions.

This article focuses on the obligation that most courts recognize to disclose attorney-expert communications and draft expert reports, and describes how this obligation applies specifically to ESI, such as e-mails and word-processing files. With the duty to disclose, there is a concomitant duty to preserve. This is particularly significant with electronic files, which can be readily modified and deleted. This article will discuss the obligation to preserve an expert's potentially discoverable electronic information and how this impacts an attorney's instructions to the witness, as well as the attorney's preservation of his or her own electronic files. The article suggests some best practices for dealing with expert witnesses, given the potential for discovery of attorney-expert communications and draft reports. Finally, some potential changes to the Federal Rules of Civil Procedure, which would protect from discovery certain attorney communications with experts and draft expert reports, are discussed.

II. The legal obligation to disclose and preserve all information that an expert considered

Initially, under Rule 26(a)(2) of the Federal Rules of Civil Procedure, a witness who is "retained or specially employed to provide expert testimony," FED. R. CIV. P. 26(a)(2)(B), must disclose "the data or other information considered by the witness in forming" the expert's opinions. *Id.* 26(a)(2)(B)(ii). This is one of several disclosure requirements for retained experts under the 1993 amendments to Rule 26.

Since the 1993 amendments, courts have broadly interpreted the phrase "data or other information considered" to include practically anything the expert took into account as part of the case. *See*, *e.g.*, *Schwab v. Phillip Morris USA, Inc.*, No. 04-CV-1945, 2006 WL 721368, at *2 (E.D.N.Y. Mar. 20, 2006); *Karn v. Ingersoll-Rand Co.*, 168 F.R.D. 633, 635 (N.D. Ind. 1996). The drafters of Rule 26(a)(2) of the Federal Rules of Civil Procedure rejected a narrower requirement which would have obliged the expert to disclose only the data or other information that the expert *relied upon* in forming the expert's opinions. *See Preliminary Draft of Proposed Amendments to the Federal Rules of Civil Procedure and the Federal Rules of Evidence*, 137 F.R.D. 53, 89 (1991). The reliance requirement, which developed in case law, provided opportunities for experts to bury potentially relevant, but adverse, information by deciding that they had not relied upon it. *See* Gregory P. Joseph, *Emerging Expert Issues Under the 1993 Disclosure Amendments to the Federal Rules of Civil Procedure*, 164 F.R.D. 97, 103-04 (1996).

In broadly interpreting the phrase "data or other information considered," courts recognized the importance of information that the expert had considered, but had not relied upon, in "understanding and testing the validity of an expert's opinion." *See Trigon Ins. Co. v.*

United States, 204 F.R.D. 277, 282 (E.D. Va. 2001). Indeed, one of the primary purposes of the disclosure requirements in Rule 26 was to provide an opposing party with information sufficiently in advance of trial to allow the party "a reasonable opportunity to prepare for effective cross examination and perhaps arrange for expert testimony from other witnesses." FED. R. CIV. P. 26(a)(2) advisory committee's note (1993), *available at* http://www.law.cornell.edu/rules/frcp/ACRule26.htm. Consequently, one court has stated that "information considered" means any information that the expert "generates, reviews, reflects upon, reads, and/or uses in connection with the formulation of his opinions, even if such information is ultimately rejected." *Synthes Spine Co., L.P. v. Walden*, 232 F.R.D. 460, 463 (E.D. Pa. 2005).

In addition to this broad interpretation of the phrase "data and other information considered," an "overwhelming majority" of the courts that have analyzed the issue have determined that a party must disclose information that an expert considered, notwithstanding that the information may be protected by the attorney work-product doctrine or some other privilege. *See Reg'l Airport Auth. of Louisville v. LFG, LLC*, 460 F.3d 697, 714, 717 (6th Cir. 2006) (collecting cases). This interpretation is supported by the Advisory Committee's note to the 1993 amendment, which states that "litigants should no longer be able to argue that materials furnished to their experts to be used in forming their opinions—whether or not ultimately relied upon by the expert—are privileged or otherwise protected from disclosure when such persons are testifying or being deposed." FED. R. CIV. P. 26(a)(2) advisory committee's note (1993).

Courts have also found that the text, itself, of Rule 26 shows the drafters' intent to require disclosure of information that might otherwise be protected from discovery, for example, finding that the general work-product doctrine in Rule 26(b)(3) must yield to the more specific expert disclosure requirement of Rule 26(a)(2). *See Reg'l Airport Auth.*, 460 F.3d at 716; *see also Karn*, 168 F.R.D. at 635-39 (tracing the history of the amendment and finding that Rule 26(a)(2) creates a "bright-line" requirement of disclosure).

Finally, courts have found that requiring full disclosure of information that an expert considered is necessary for effective cross-examination of experts, which is sufficient reason to override the attorney work-product doctrine. *See*, *e.g.*, *TV-3, Inc. v. Royal Ins. Co. of Am.*, 194 F.R.D. 585, 588 (S.D. Miss. 2000); *see also Karn*, 168 F.R.D. at 639-41 (finding that disclosure enhances cross-examination and is at little, if any, cost to the policies underlying the work-product doctrine); *Mfg. Admin. & Mgmt. Sys., Inc. v. ICT Group, Inc.*, 212 F.R.D. 110, 115-18 (E.D.N.Y. 2002) (same).

The Federal Rules of Civil Procedure provide sanctions for a failure to make a complete disclosure under Rule 26(a). Under the sanctions provisions of Rule 37(a)(3) and Rule 37(c)(1), a court may exclude an expert's trial testimony, or impose another sanction, if a party fails to comply with the expert disclosure requirements of Rule 26(a)(2)(B), unless the court finds that there was substantial justification for the failure to disclose or that the failure was harmless. FED. R. CIV. P. 37. The rule treats an "incomplete disclosure" as a failure to disclose. *Id.* 37(a)(3).

With respect to information that is discoverable—as containing potentially relevant evidence to the litigation—there is a corresponding duty to preserve the information. This is governed by the substantive law of spoliation in the controlling jurisdiction. Under spoliation law, if potentially relevant evidence is not preserved, but is destroyed, the court may impose a variety of sanctions, including dismissal or default judgment if the transgression is sufficiently serious. *See* Marjorie A. Shields, Annotation, *Electronic Spoliation of Evidence*, 3 A.L.R. 6th 13 (2005) (collecting cases). In addition, an attorney has an ethical obligation to ensure that potentially relevant evidence in the attorney's possession or control is not destroyed. Rule 3.4 of the Model Rules of Professional Conduct provides that a lawyer shall not

"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." Model Rules of Prof'l Conduct R. 3.4(a), *available at* http://www.abanet.org/cpr/mrpc/rule_3_4.html.

As a practical matter then, unless an attorney is litigating in one of the few jurisdictions that continues to provide protection for attorney work-product provided to an expert (*see*, *e.g.*, *Krisa v. Equitable Life Assurance Soc'y*, 196 F.R.D. 254, 259-60 (M.D. Pa. 2000); *Haworth, Inc. v. Herman Miller, Inc.*, 162 F.R.D. 289, 292-96 (W.D. Mich. 1995)), the attorney must assume that all information that an expert considered is discoverable. For that reason, as discussed in more detail below, the attorney must take reasonable steps to ensure that the retained testifying expert, who is under the attorney's control, preserves the information that he or she considered. Moreover, to the extent that the attorney personally has possession of this information, he or she should also take steps to retain the information.

III. Applying the legal obligation to disclose and preserve information to electronic files reflecting attorney-expert communications and draft expert reports

The December 2006 amendments to the Federal Rules of Civil Procedure concerning ESI acknowledged that much of the relevant evidence in modern litigation consists of electronic files managed by electronic systems. The amendments provided procedures for discovery of electronic information, and, perhaps more significantly, raised attorneys' awareness of the potential for discovery of electronic files. Because the 1993 amendments broadly provided that information considered by an expert was discoverable, attorneys should be cognizant of the sources of ESI that their experts may have reviewed. As most courts have found that there is no attorney work-product protection for information that an expert has considered, an opposing party can discover an attorney's mental impressions that are reflected in attorney-expert communications and draft expert reports.

Many expert-attorney communications and draft expert reports are captured in the form of electronic files. Attorneys and their experts communicate frequently by e-mail and voice mail. These communications create electronic files that are stored for various times in several places. Additionally, as an expert drafts and modifies his or her report, there is a potential for the creation of electronic files. The expert typically sends draft reports, either electronically or in hard copy, to the attorney (and perhaps to others) for review and comment. The expert will often modify the report several times before completing the final copy for submission to the opposing party. Depending upon who has seen and commented upon the draft, and whether the expert has saved prior iterations of the draft on his or her computer, there may be several electronic files of the draft report in various locations.

Courts have typically found that attorney-expert e-mails and draft expert reports are discoverable, notwithstanding the fact that they may contain attorney-client material or reflect attorney work-product. *See*, *e.g., Bro-Tech Corp. v. Thermax, Inc.*, Civ. No. 05-2330, 2008 WL 356928, at *1-2 (E.D. Pa. Feb. 7, 2008); *Varga v. Stanwood-Camano Sch. Dist.*, No. C06-0178P, 2007 WL 1847201, at *1 (W.D. Wash. June 26, 2007) (finding e-mail communications between an attorney and expert discoverable and not protected by attorney work-product doctrine; *Univ. of Pittsburgh v. Townsend*, No. 3:04-cv-291, 2007 WL 1002317, at *2-5 (E.D. Tenn. Mar. 30, 2007) (finding e-mails and draft reports discoverable but holding no duty to preserve until issuance of subpoena; refusing to impose sanction for destruction); *Bitler Inv. Venture II, LLC v. Marathon Ashland Petroleum LLC*, No. 1:04-CV-477, 2007 WL 465444, at *1-7 (N.D. Ind. Feb. 7, 2007) (finding e-mails discoverable and not protected by the

attorney-client privilege or the attorney work-product protection; *Colindres v. Quietflex Mfg.*, 228 F.R.D. 567, 570-72 (S.D. Tex. 2005) (requiring production of expert's e-mail to counsel which discussed questions that the court had asked at a hearing); *W.R. Grace & Co.-Conn. v. Zotos Int'l Inc.*, No. 98-CV-838S(F), 2000 WL 1843258, at *2-5 (W.D.N.Y. Nov. 2, 2000) (finding draft expert reports discoverable notwithstanding attorney work-product protection).

One case which preceded the 2006 Rules amendments, *Trigon Ins. Co. v. United States*, 204 F.R.D. 277 (E.D. Va. 2001), should be a wake-up call for attorneys to the potential electronic discovery dangers in working with expert witnesses. In *Trigon*, the United States defended a complex tax recovery action and hired testifying experts and an economic consulting firm. *Id.* at 279-80. When the United States' testifying experts produced their reports, two of the experts revealed that they had reviewed a declaration from the consulting firm as well as each other's expert reports. *Id.* at 281. The plaintiffs requested communications and draft reports, noting that Rule 26(a)(2) required production of all documents considered by the testifying experts. *Id.* Upon receiving the request, the United States directed the testifying experts and the consulting firm to preserve all draft reports and communications with each other. *Id.* It was too late by the time the direction was received. The testifying experts and the consulting firm had already deleted many e-mails and draft reports pursuant to their routine document retention policies and practices. *Id.*

The court determined that under the language of Rule 26(a)(2) "[a]ny information reviewed by an expert" was subject to discovery, including e-mail communications and "drafts of reports sent from and to the testifying experts." *Id.* at 281-83. The court also found that the disclosure obligation in Rule 26(a)(2) was sufficient, on its own terms, to put the United States on notice that it must take steps to preserve these materials so that the United States could disclose them at the appropriate time. *Id.* at 288. The court ordered the United States to hire an independent forensics expert to determine whether it could retrieve the apparently deleted documents from the computers of the testifying experts and the consulting firm. *Id.* at 282. While the forensics firm was able to recover "[h]undreds of communications and many draft reports," it was unable to recover all of the ESI. *Id.* at 282, 290. The court found that fragments of e-mails that were recovered revealed that the United States' consultant had been extensively involved in drafting the report of at least one of the testifying experts. *Id.* at 290. The court stated that this raised "serious doubts" regarding whether the opinions of the testifying expert were actually his own. *Id.* Consequently, the court found that the United States' failure to produce all of the drafts for the expert prejudiced the plaintiff's ability to cross-examine him. *Id.* Morever, the court found that the United States' other experts were also potentially tainted because, due to the missing electronic data, the United States could not disprove that the consultant had been intimately involved in writing their expert reports as well. *Id.* at 290 n.9.

While seriously considering striking the testimony of the United States' experts, the court declined to do so because the plaintiff and the United States opposed that remedy. *Id.* at 291. However, the court found that, based upon the evidence at trial, it may be appropriate "to draw adverse inferences respecting the substantive testimony and credibility of the experts." *Id.* The court also foreclosed the consultant from any further participation in the government's "development and presentation" of expert testimony. *Id.* Finally, the court found that the plaintiff was entitled to recover attorney fees and costs as a result of the spoliation of evidence, and noted that "[t]here has been significant expense in the briefing, deposing of experts, argument and hiring of computer forensics experts to adjudicate the issues [related to spoliation]." *Id.* at 291 & n.11. Fortunately for the United States, the court ultimately decided not to draw adverse inferences regarding the government's experts and ruled for the government on the merits. *See Trigon Ins. Co.*

v. United States, 215 F. Supp. 2d 687, 741-42 (E.D. Va. 2002). Nevertheless, the court awarded the plaintiff $179,725.70 in fees and expenses for the spoliation. *See Trigon Ins. Co. v. United States*, 234 F. Supp. 2d 592, 595 (E.D. Va. 2002).

Trigon illustrates the potentially severe sanctions that a court can impose against a party for failing to preserve all information that an expert "considered," including e-mails and draft reports that may exist only as ESI. Significantly, the court found that the document-retention policies and practices of the testifying experts and consulting firm did not excuse the United States from its preservation duties. 204 F.R.D. at 289. Since the *Trigon* decision, the recent rules amendments regarding ESI provide that "absent exceptional circumstances" a court may not impose sanctions for "failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." FED. R. CIV. P. 37(e). The Advisory Committee and commentators have noted, however, that "good-faith" likely requires a party's intervention to suspend routine operations of the information system to prevent the loss of information if it is subject to a preservation obligation. *See*, *e.g.*, FED. R. CIV. P. 37(f) advisory committee's note (2006); Thomas Y. Allman, *Defining Culpability: The Search for a Limited Safe Harbor in Electronic Discovery*, 2 FED. COURTS L. REV. 65, 77-80 (2007). Thus, an expert's failure to suspend routine system deletion of electronically stored e-mails regarding a case and draft reports is still likely sanctionable under the Rules. While there is little discussion in the case law regarding voice mail, it would theoretically be subject to the same requirements as other ESI.

Trigon is also instructive regarding the respective roles of consultants and testifying experts in litigation. Generally, an opposing party may not obtain discovery of materials considered or worked produced by a consultant. Rule 26(b)(3) protects trial preparation materials from discovery absent a showing of substantial need and undue hardship in obtaining equivalent materials by other means. Even when a court orders discovery of these materials, Rule 26(b)(3)(B) requires the court to protect attorney work-product from disclosure. Additionally, unless the consultant has done an independent medical examination under Rule 35, an opposing party may discover facts and opinions of the consultant only upon a showing of exceptional circumstances. *See* FED. R. CIV. P. 26(b)(4)(B). Consequently, given these protections for consultants, contrasted with the breadth of discovery that the Federal Rules of Civil Procedure allow for testifying experts, attorneys will often hire consultants with whom they can more freely communicate regarding scientific and legal theories. *Trigon* shows that, unless attorneys strictly prohibit communications and exchanges of information between consultants and experts, the consultant's work may become open to discovery as information that the testifying expert considered.

The 2006 amendments concerning ESI will undoubtedly result in attorneys more frequently seeking this information from opposing parties and their experts. With courts holding that parties can discover expert e-mails and draft reports, and imposing sanctions on parties who fail to preserve electronic information, attorneys must be diligent and vigilant in working with their expert witnesses.

IV. Best practices for working with expert witnesses in the age of electronic discovery

Attorneys should be cognizant of the potential breadth of discovery from retained testifying experts and be proactive from the outset of litigation in assisting them to preserve potentially discoverable information. Perhaps the most important step is to educate the expert about his or her preservation and disclosure obligations. This should be done at the time of retention. The attorney should inform the expert that, because everything that he or she "considered" related to the litigation is potentially discoverable, any

information that was within his or her possession and considered must be preserved. The attorney should stress that this preservation obligation includes any e-mails related to the case, any electronic data files that were stored on the computer, and any draft reports created.

The expert must be told that if his or electronic information system routinely deletes files, such as e-mails, the system must be altered so that it no longer eliminates potentially discoverable information. It should be suggested that the expert create a folder to store all case-related e-mail. As the case progresses, periodic reminders about the disclosure requirement and the duty to preserve should be given. The attorney should consider documenting these instructions, albeit with the knowledge that such documentation is, itself, likely discoverable. This documentation may become important if an issue arises regarding preservation of information that the expert considered.

Attorneys representing the United States should be beyond reproach in dealing with expert witnesses. Attorneys should not try to use their experts as "willing musical instruments upon which manipulative counsel can play whatever tune desired." *Karn*, 168 F.R.D. at 639, citing John H. Langbein, *The German Advantage in Civil Procedure*, 52 U. CHI. L. REV. 823, 835 (1985). The role of the expert is to assist the trier of fact to understand the evidence through testimony concerning scientific, technical, or other specialized knowledge. FED. R. EVID. 702. Courts require expert testimony to be reliable, *id.*, and expect some degree of objectivity from expert witnesses. This does not mean that attorneys must refrain from assisting their experts. In fact, the Advisory Committee's note to the 1993 amendments to Rule 26 specifically states that the Rule "does not preclude counsel from providing assistance to experts in preparing the reports." FED. R. CIV. P. 26(a)(2) advisory committee's note (1993). Government counsel should strive to avoid any appearance that they have attempted to influence their experts improperly.

That being said, as part of an attorney's zealous representation of the client, he or she should take steps to limit the creation of stored information containing attorney work-product for the expert to consider, whether such information consists of hard-copy documents or electronically stored files. The attorney should assume that the opposing party will gain access to case-related e-mails to and from the expert witness. The attorney should also assume that the opposing party will be able to discover an expert's draft reports and be able to gauge attorney influence on the report-drafting process. The opposing party will be able to analyze the changes in successive iterations of the report and perhaps even question the expert at deposition about those changes.

Thus, given the opposing party's potential access to this information and the expert's duty to preserve it, the procedures for working on a case must be discussed in detail at the time of retention. The attorney should counsel the expert to avoid substantive discussions of the case in e-mail and voice mail communications. To the extent possible, an expert should confine substantive discussions regarding the case to in-person meetings and telephone conversations. The substance of these conversations is also theoretically discoverable but they do not create stored information that an opposing party can use to confront and impeach an expert. Good practice and zealous representation do not mandate foregoing use of e-mail and voice mail entirely. These are very convenient methods of communication, particularly with expert witnesses who are often very busy. A good "rule of thumb" for the expert (and for the attorney and others who may communicate with the expert) is never to put any information in an e-mail or voice mail that one would not send or say directly to the opposing lawyer. Matters of scheduling and procedure are perfectly acceptable in e-mails; however, substantive discussions about theories of the case may not be. The attorney should inform the expert that note taking is also potentially discoverable.

Similarly, an attorney should discuss the expert's report-drafting procedure early in the

case. The lawyer should ask the expert to discuss, in detail, opinions and the reasoning with the attorney before drafting a report because of the opposing party's potential access to draft reports. It should be explained that this is necessary because the opposing party may be able to discover modifications to the report through reviewing drafts and examining the witness at deposition. Thus, the expert should be extremely careful regarding the initial draft of the report. The drafting process is not the time to test different opinions or theories. Instead, the expert's theories and opinions should be discussed well in advance of drafting an initial report. These discussions should take place through phone calls and in-person meetings

It is important for the attorney to know the procedures that the expert intends to use in drafting the report before the initial draft is prepared.

- Will the expert continually work with one electronic word processing file, or will separate electronic files be created as part of the process?
- Will others review and comment on the report before the draft is sent to the attorney for review?
- As comments are received, does the expert intend to overwrite electronic files, or will prior iterations of the report be saved?

The attorney and the expert should agree on a defensible procedure for producing and saving drafts, depending upon the nature of the case and the identity of the expert. At a minimum, the attorney should ask the expert to save any draft sent out of his or her office. Depending upon the size and type of the expert's office, the attorney may also request drafts sent to others within the office be saved. It is doubtful, though not inconceivable, that a court would require an expert to save prior drafts which reflect only his or her internal thought process in reaching expert opinions. *See Trigon*, 204 F.R.D. at 283 n.8 (stating that there are cogent reasons not to require production of drafts "prepared solely by that expert while formulating the proper language in which to articulate that exper[t's]; own, ultimate opinion arrived at by the expert's own work or those working at the expert's personal direction.")

After an expert produces an initial draft and conveys it to others for review, he or she and the attorney must realize that changes to the draft may be accessible material for cross-examination. This is not to say that attorneys should not suggest, and experts should not make, changes to the report. Counsel should consider, however, every proposed change in light of the potential impact on the persuasive value of the expert's opinion if the opposing party cross-examines him or her regarding the change at deposition or trial. Certainly, stylistic, grammatical, and minor substantive changes should have little effect on the credibility of the expert's opinions. On the other hand, an expert can be vulnerable to strong impeachment if the drafting process shows major substantive changes or substantial attorney involvement in writing the report.

Attorneys should be wary of any devices that experts or others suggest to protect the expert report-drafting process from discovery. An expert may propose that an attorney review a report on a Web-based application and suggest changes, without ever "possessing" the report for purposes of discovery. Courts are beginning to recognize, however, that even more ephemeral forms of electronic information, stored only temporarily in the random access memory of a computer, can be subject to discovery. *See Columbia Pictures Indus. v. Bunnell*, 245 F.R.D. 443, 446-48 (C.D. Cal. 2007) (finding that information stored only in random access memory is ESI that may be subject to discovery). A court would not likely be receptive to an argument that a draft expert report is not discoverable because the attorney only reviewed it on the Internet and never possessed a hard copy or an electronic file containing the report.

If the attorney feels the need to discuss legal, scientific, and technical theories with an expert, he or she may consider hiring a consultant. As the *Trigon* case illustrated, however, the attorney

must be extremely careful to keep a wall of separation between the consultant and the testifying experts. Consultants, however, may only be necessary in rare, complex cases. The testifying expert can usually provide the consulting services that the attorney needs with little risk of damaging disclosures, as long as both are careful to confine their consultations to phone calls and in-person meetings.

Additionally, a good practice for the attorney is to preserve copies of attorney-expert e-mails and draft reports in the attorney's possession. This may be especially helpful in case the expert fails to follow the preservation instructions. The retained copies of the materials in the attorney's possession setting forth the attorney's preservation instructions to the expert, along with his or her own preservation of materials, should be sufficient to meet the professional obligations of Model Rule 3.4(a), *available at* http://www.abanet.org/cpr/mrpc/rule_3_4.html.

Finally, attorneys may consider entering into an agreement with the opposing party to protect draft-expert reports and attorney-expert communications from discovery. This is a strategic decision that must be made on a case-by-case basis. However, by giving up the right to obtain this discovery from an opposing party, the attorney may be missing evidence that could seriously compromise the effectiveness of the opponent's experts. The attorney must consider whether entering such an agreement allows zealous representation of the client's interests.

V. Proposals for limiting discovery of attorney-expert communications and draft reports

While the current federal civil rules provide for broad discovery from experts, they may change in the next few years to provide protection for certain material that contains attorney work product or other privileged information considered by an expert. In August 2006, the American Bar Association (ABA) House of Delegates adopted a resolution recommending that federal and state civil procedure rules be "amended or adopted to protect from discovery draft expert reports and communications between an attorney and a testifying expert relating to an expert's report." *See* American Bar Association, Resolution 120A, Discoverability of Expert Reports, Adopted by the House of Delegates, August 7-8, 2006, *available at* http://www.abanet.org/litigation/standards/docs/120a_policy.pdf.

Under the specific provisions of the ABA resolution, a party should not be required to produce a draft expert report to an opposing party, or attorney-expert communications—including notes reflecting the communications—except on a showing of exceptional circumstances. *Id.* The resolution contains a caveat that the opposing party should not be precluded from obtaining any "facts or data that the expert is relying upon" or inquiring fully into the facts or data that the expert considered. *Id.* The emphasis on "facts or data" is narrower than the "information that the expert considered" as most courts have interpreted that phrase under the current rule, and it is designed to preclude discovery into attorney mental impressions that form the core of work product.

The drafters of the Federal Rules of Civil Procedure are currently studying whether to amend the Rules to protect draft reports and attorney-expert communications from discovery. In December 2007, the Advisory Committee on the Rules reported to the Standing Committee on Practice and Procedure that a Discovery Subcommittee had concluded that draft reports should be protected from discovery. *See* Memorandum from Hon. Mark R. Kravitz, Advisory Committee, to Hon. Lee H. Rosenthal, Standing Committee, Report of Civil Rules Advisory Committee, Civil Rules Committee Report 9 (Dec. 17, 2007), *available at* http://www.uscourts.gov/rules/Reports/CV12-2007.pdf.

The Discovery Subcommittee also concluded that some attorney-expert communications should receive work product protection. *Id.* This continues to be a work in progress. In 2008, the

Discovery Subcommittee will likely make a formal recommendation of changes to Rule 26 to protect these expert materials. *Id.* at 10. If the Advisory Committee votes to recommend proposed rules changes to the Standing Committee, it must then obtain approval from the Standing Committee to publish the proposed rules for public comment. *See* James C. Duff, *The Rulemaking Process: A Summary for the Bench and Bar*, Federal Rulemaking, Apr. 2006, *available at* http://www.uscourts.gov/rules/proceduresum.htm. There is usually a 6-month public comment period and several additional steps before the United States Supreme Court submits the proposed rules changes to Congress. *Id.* Once that occurs, the changes go into effect on December 1 of the calendar year if Congress has had at least 7 months to consider the rules and has failed to take any action to reject, modify, or defer the rules. *Id.* Given this procedure, it will likely be quite some time after the publication date of this article before there are any federal civil rules changes to protect draft-expert reports and attorney-expert communications from discovery. Interested attorneys can track the progress of proposed rules changes on the United States Courts' Web site. *See* http://www.uscourts.gov/rules. Notwithstanding any rules changes, counsel would be prudent in dealing with experts to limit access to attorney work product in e-mails and comments on draft reports. Once this information is out of the attorney's possession, there is always a danger of inadvertent disclosure and waiver.

VI. Conclusion

Working with experts in the age of electronic discovery can be a minefield. An attorney must be careful to limit the creation of ESI that experts consider because it is unlikely that the lawyer will be able to assert successfully that any of the information is privileged or otherwise protected from disclosure. At the same time, he or she must be proactive to ensure that the expert does not inadvertently delete material related to the litigation. By following the best practices outlined in this article, an attorney should be able to limit the possibility that an expert witness will be compromised through the creation of evidence that an opponent can use to impeach the witness or through the destruction of discoverable evidence in his or her possession.❖

ABOUT THE AUTHOR

❑**Adam Bain** is a Senior Trial Counsel in the Environmental Torts Section of the Civil Division. He has worked extensively with expert witnesses during his 20-year career in defending the United States in complex toxic tort litigation. He has also lectured frequently in Washington, D.C. and at the National Advocacy Center on using expert witnesses and on the rules amendments relating to electronic discovery. ✠

The author would like to thank Jane Mahoney and Theodore Hirt for their helpful comments on this article.

The "Two-Tier" Discovery Provision of New Rule 26(b)(2)(B)—How Can Federal Agencies Benefit by Using this Rule?

Theodore C. Hirt
Assistant Director
Federal Programs Branch
Civil Division

I. Introduction

One persistent challenge for litigants, including federal agencies, is how to balance legitimate and reasonable discovery demands against the inevitable burdens and costs associated with that discovery. The latest example of an attempt to achieve that balance is one of the "electronic discovery" amendments to the Federal Rules of Civil Procedure that became effective in December 2006. The author is referring to the so-called "two tier" system for the discovery of electronically stored information (ESI), under new Rule 26(b)(2)(B). *See* FED. R. CIV. P. 26(b)(2)(B). In brief, that Rule states that "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." *Id.* Sources that are "reasonably accessible are the "first tier." Sources that are not reasonably accessible are the "second tier."

This article first describes the Rule and how the Civil Rules Advisory Committee, which formulated the December 2006 amendments, expected it to operate. Next the Rule's practical implications and its relationship to other discovery rules is discussed. Finally, some recommendations on how Department of Justice (Department) attorneys can use the new Rule effectively are provided.

II. The Rule—its background and function

In creating the electronic discovery amendments, the Civil Rules Advisory Committee recognized the "difficulties in locating, retrieving, and providing discovery of some electronically stored information." *See* FED. R. CIV. P. 26 advisory committee's note (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. It also recognized that electronic storage systems "often make it easier to locate and retrieve information" and that "[t]hese advantages are properly taken into account in determining the reasonable scope of discovery in a particular case." *Id.* The Advisory Committee added that "some sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible." *Id.*

The Advisory Committee also recognized that businesses might possess a broad range of information sources with varying levels of accessibility. The storage of information in electronic format, in some situations, could "provide ready access to information used in regular ongoing activities," and information systems also "may be designed so as to provide ready access to information that is not regularly used." *Id.* But, at the same time, the Advisory Committee concluded that such information systems "may retain information on sources that are accessible only by incurring substantial burdens or costs." *Id.* The Rule reflects the reality that private and public organizations—including

the federal government—collect and retain ESI in a variety of sources and media, with different levels of ease or difficulty in accessing, retrieving, or producing such information.

The Advisory Committee simultaneously recognized that "[t]he volume of—and the ability to search— much electronically stored information means that in many cases the responding party will be able to produce information from reasonably accessible sources that will fully satisfy the parties' discovery needs." *See* FED. R. CIV. P. 26 advisory committee's note (2006). The note then explains that "[i]n many circumstances the requesting party should obtain and evaluate the information from such sources before insisting that the responding party search and produce information contained on sources that are not reasonably accessible." *Id.* This explanation could prove to be quite helpful to cite when a discovery dispute arises.

As mentioned previously, new Rule 26(b)(2)(B) states that "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." FED. R. CIV. P. 26(b)(2)(B). The Rule does not try to define or describe what sources of information are "reasonably accessible," and which are not. The committee note concludes that such a definition would be impractical. "It is not possible to define in a rule the different types of technological features that may affect the burdens and costs of accessing electronically stored information." *See* FED. R. CIV. P. 26 advisory committee's note (2006). This reflects the Advisory Committee's conclusion that the difficulties in accessing electronic information "may arise from a number of different reasons primarily related to the technology of information storage, reasons that are likely to change over time." *See* Memorandum from Honorable Lee H. Rosenthal, Chair, Advisory Committee on the Federal Rules of Civil Procedure to Honorable David F. Levi, Chair, Standing Committee on Rules of Practice and Procedure 34 (May 27, 2005) (on file with author), *available at* http://www.uscourts.gov/rules/supct1105/Excerpt_CV_Report.pdf.

Because the Rule does not specify the kinds of sources of ESI that might not be "reasonably accessible" in litigation, the responding party needs to decide, in the first instance, the anticipated scope of its ESI production. It then needs to describe to the opposing party what sources of information it does *not* intend to search or produce. The committee note explains that the responding party "must . . . identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing." *Id.* This identification "should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources." *Id.*

In some cases, the producing party's identification of its first and second-tier sources may be satisfactory to the requesting party. In those situations, presumably, the discovery will be limited to the first-tier sources. In other cases, however, the requesting party still may demand production of ESI from the second-tier sources. If the parties reach an impasse, they can present the dispute to the court for resolution, through either a motion to compel production of the ESI under Rule 37, or a motion for protective order under Rule 26(c) against that production. As is the case with other discovery disputes under the Rules, the parties must confer before filing either motion. *See* FED. R. CIV. P. 26(c), 37(a)(2)(B).

The Rule provides a "roadmap" for how such disputes can be addressed. Assume that, after the responding party has provided the required identification of "second-tier" information sources, an impasse occurs. The Rule provides that, in resolving such motions, "the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost." FED. R. CIV. P. 26(b)(2)(B). As the text makes clear, the burden of proof is on the nonproducing party to

demonstrate that the requested information is not "reasonably accessible."

If the nonproducing party establishes that point, then the burden shifts to the requesting party to establish good cause for the discovery. If it fails to do so, the dispute ends. If, however, the requesting party establishes good cause, the court then may order discovery from the second-tier sources. At that stage, the Rule incorporates the pre-existing limitations on discovery of Rule 26(b)(2)(C). For example, a court may limit discovery if it determines that

> (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the discovery in resolving the issues.

FED. R. CIV. P. 26(b)(2)(C).

Courts are expected to engage in a balancing analysis before permitting the second-tier discovery—assessing the costs against the potential benefits of the discovery in each specific case. The note identifies some "appropriate considerations," which may include:

> (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is not longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

See FED. R. CIV. P. 26 advisory committee's note (2006). As litigants become more familiar with the Rule, we can expect that they will urge courts to apply these factors. *See Petcou v. C.H. Robinson Worldwide, Inc.*, 2008 WL 542684, *1 (N.D. Ga. Feb. 25, 2008) (noting these factors in holding that the burden on defendant of restoring deleted e-mails outweighed plaintiff 's purported need for them).

Resolving disputes concerning access to second-tier discovery may involve proceedings in addition to the motions practice described. The requesting party might challenge the responding party's contention that the ESI "fits" within the second tier. The committee note states that the requesting party may need discovery to "test" that contention, which might involve requiring the responding party to conduct a sampling of information contained on those second-tier sources, permitting the inspection of such sources, or depositions of witnesses "knowledgeable about the responding party's information systems."

See FED. R. CIV. P. 26 advisory committee's note (2006).

Another important feature of this Rule is its explicit recognition that second-tier discovery may be subject to limits or conditions. If the requesting party has shown "good cause" for the production of the second-tier information, the court may specify conditions for that discovery. Although the Rule does not identify those conditions, the committee note explains:

> The conditions may take the form of limits on the amount, type, or sources of information required to be accessed and produced. The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. A requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause. But the producing party's burdens

> in reviewing the information for relevance and privilege may weigh against permitting the requested discovery.

See FED. R. CIV. P. 26 advisory committee's note (2006).

One other feature to this Rule deserves special emphasis. The Rule does *not* address a party's duty to preserve potentially relevant ESI from sources of information that the responding party has determined are not reasonably accessible. The Advisory Committee's note cautions, however:

> A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.

See FED. R. CIV. P. 26 advisory committee's note (2006).

III. Rule 26(b)(2)(B) and other discovery rules

Rule 26(b)(2)(B) cannot be considered in isolation from the other discovery rules. It "fits" closely with the parties' duty to "meet and confer" under Rule 26(f). It also takes on critical importance in the context of Rule 34 requests.

A. The parties' duty to "meet and confer"

Under amended Rule 26(f), counsel for the parties have to confer in order to devise a proposed discovery plan and to provide their views and proposals, *inter alia*, as to "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." FED. R. CIV. P. 26(f)(3)(c). The court's scheduling order may incorporate the parties' agreements. *See* FED. R. CIV. P. 16(b). When the case involves the discovery of ESI, the parties must address such issues, "depend[ing] on the nature and extent of the contemplated discovery and of the parties' information systems." FED. R. CIV. P. 26 advisory committee's note (2006). The committee note explains that "[i]t may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems." *Id.*

Rule 26(f) also contemplates that the parties will do more than simply exchange information about their information systems at the "meet and confer" session. The note explains that the parties may identify "the various sources of such information within a party's control that should be searched for electronically stored information." *See* FED. R. CIV. P. 26 advisory committee's note (2006). With specific reference to Rule 26(b)(2)(B), the note adds that the parties should discuss "whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information." *Id.*

One challenge for counsel will be their ability to confer with opposing counsel concerning the production of ESI, with sufficient knowledge and understanding of the complexities of the ESI they ultimately will produce as the case proceeds. There is an implicit premise in both Rule 26(f) and 26(b)(2)(B) that counsel will be able to speak knowledgeably about their respective client's information systems. Counsel should determine what sources of ESI *may be* reasonably accessible, and, as importantly, which may *not* be reasonably accessible. At the very beginning of the litigation, however, counsel may lack comprehensive knowledge of the clients' information systems. The committee note implicitly recognizes that it may be unrealistic to expect that the "meet and confer" process will resolve these issues, for it states that the parties "*may* identify" the various sources of information in a party's control that should be searched, and that the parties "*may*

discuss whether the information is readily accessible to the party that has it. . . . " *See* FED. R. CIV. P. 26 advisory committee's note (2006) (emphasis added). Counsel will be understandably reluctant to commit themselves to a position—at the very first conference—on what ESI sources should be searched, or, perhaps more important to this problem, what ESI sources will be considered "off limits."

B. Disclosure under Rule 26(a)(1); discovery under Rule 34

The parties also will have to address how the two-tier discovery provisions of Rule 26(b)(2)(B) will be incorporated into the broader discovery "landscape." This will apply first to the duty to provide the "initial disclosures" under Rule 26(a)(1)(B). Each party must identify the ESI that it may use in support of its claims or defenses early on, as counsel needs to address the sources of information that will be "reasonably accessible," in order to make that disclosure. Consequently, knowing about a client's information systems as soon as possible takes on increasing importance. Counsel cannot argue simultaneously that specific ESI sources are not reasonably accessible, and thereby refuse to disclose them, but then determine to rely upon them in support of the government's claim or defense.

Distinguishing between first-tier and second-tier ESI will be particularly critical when Rule 34 requests are served. It is foreseeable that counsel will not resolve this issue at the "meet and confer" sessions. For that reason, amended Rule 34 creates a formal structure for the resolution of this issue. Once a request is served, the party demanding access to second-tier ESI may face the objection from the responding party that it will not search or produce such sources because they are not "reasonably accessible." This is the point at which intervention of the court may be required.

As noted above, the parties' disagreements on accessibility may even lead to discovery, including a deposition under Rule 30(b)(6) directing the responding party to identify deponent(s) knowledgeable about the relevant information systems, in order to probe the basis for the objection that the sources of information are not reasonably accessible. In the alternative, counsel for the requesting party may issue a more "targeted" Rule 34 request, directed at requiring a sample of information from those sources. The Rule creates several opportunities for this issue to be resolved. Counsel should consider whether to use those options before they reach an impasse and the judge then needs to become actively involved.

IV. How Department attorneys can use the rule effectively

Federal agencies hold a vast amount of information, some in traditional paper format and, increasingly, in electronic format. Department attorneys, particularly those who defend federal agencies when those agencies or their officials are sued in district court, already recognize the importance of trying to establish limits to what otherwise can be very burdensome discovery. In contrast, when Department attorneys bring affirmative litigation on behalf of federal agencies, they want to be thorough and comprehensive in securing access to the opposing party's information. Some practical suggestions follow.

A. Learn about the agency's ESI systems

The first challenge for those dealing with ESI issues is learning about the client's various information systems and what kinds of ESI are maintained on them. Being conversant with those systems will make it easier for counsel to determine whether ESI should be categorized as first-tier or second tier discovery. The Department attorney should work with agency counsel, and agency program, information technology, and records management staff to secure an understanding of the agency's information systems. This will facilitate the effectiveness of the inevitable negotiations that he or she will have with opposing counsel at the Rule 26(f) conferences. Agencies need to have detailed ESI

inventories developed before they face actual litigation. That inventory will be critical to discovery planning and implementation.

B. Be able to explain ESI sources—and their limits—to opposing counsel

It is critical that Department counsel is able to explain the agency's ESI sources, and their limitations, to opposing counsel. Attorneys must be realistic, however, and *not* assume that they can attain comprehensive knowledge about an agency's ESI sources, at least in a complex case, as early in a case as some courts might expect. This is a learning process, although some courts expect that counsel will be in a position to exchange *some* of this knowledge early in the Rule 26(f) "meet and confer" sessions.

There will be substantial pressure to resolve, as early as feasible, what sources of ESI will be produced and on what timetable. There also will be pressure for counsel to know, or at least have a solid estimate, as to what sources will be not reasonably accessible and, therefore, presumptively not discoverable. For that reason, counsel for a producing party will need to have conducted an "inventory" of the client's information systems to know what sources of information fit in the first and second tier. Making a mistake in either direction may have significant ramifications. For example, if counsel represents to the opposing party that specific sources are accessible, but later learns that the cited sources are not accessible, this will be quite embarrassing. *Cf. Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 WL 1409413, *6 (S.D.N.Y. May 23, 2006) (failure of counsel to investigate existence of servers; the court awarded monetary sanctions). Similarly, if counsel misstates that certain sources are not "reasonably accessible," but later learns that, in fact, those sources are reasonably accessible, the misrepresentations will compromise counsel's credibility and lead to mistrust in the discovery process. Given the potential for misinformation and misunderstanding, Department attorneys representing agencies who resist the production of second-tier discovery need to be as thorough as possible in the investigation of the agency's information systems prior to making representations.

Department counsel should prepare a checklist of ESI discovery sources so that he or she can argue persuasively and effectively for, or against, access to second-tier sources of information. Counsel will need to inventory what information sources were actually searched from the first tier. This is important because the court may want to know specific details on "the quantity of information available from other and more easily accessed sources." *See* FED. R. CIV. P. 26 advisory committee's note (2006). It is critical to document what information has been provided from those sources. The more comprehensive that showing, the more reasonable will be the agency's position that second-tier sources should not be searched. Counsel also need to know what information sources previously existed, but no longer exist, what kind of information was stored on them, and whether that information has migrated to other systems. That is important because the court will evaluate "the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources." *See* FED. R. CIV. P. 26 advisory committee's note (2006).

C. Be able to advocate the contours of "reasonable" accessibility

When the Department is representing an agency that refuses to produce second-tier discovery, counsel will need to set the groundwork for a successful defense of that position. First, it is important to document that the agency has offered the opposing party ESI from the sources that it has identified as "reasonably accessible," and what agreements may exist as to that production. If the dispute reaches the court, the Department attorney will be in a position to show that the agency attempted to resolve the problem in a reasonable manner by providing the requesting party a full opportunity to access the first-tier sources to find relevant information.

In contrast, when the Department is seeking second-tier discovery on behalf of an agency (or to enforce a statute), counsel will need to show that the requested second-tier information will *not* be derived from the "reasonably accessible" sources of information. The Department attorney will need to be able to show that the information, even if it can be derived *only* from sources that are not reasonably accessible, nevertheless should be produced because of its relevance and its role in establishing the government's case. The challenge will be how to demonstrate that the benefit of securing that information outweighs the burden or cost of production, applying the "proportionality" factors in Rule 26(b). *See McPeek v. Ashcroft*, 212 F.R.D. 33, 35-36 (D.D.C. 2003), 202 F.R.D. 31, 34-35 (D.D.C. 2001) (court applies "marginal utility" analysis to authorize a limited search of agency back-up tapes to locate relevant e-mails).

D. Involve the agency closely in the process

The agency's information technology (IT) staff plays a key role in the discovery dispute process. First, this staff is indispensable in the creation, and ongoing maintenance, of an ESI inventory. They also are key to the successful development and monitoring of the "litigation hold" necessary to ensure that the inadvertent, or purposeful, destruction of potentially relevant ESI that otherwise might be deleted during the course of the litigation is avoided. IT personnel need to be involved in consulting on the feasibility of accessing second-tier ESI, including the potential for sampling. *See Zurich Am. Ins. Co. v. Ace Am. Reinsurs. Co.*, 2006 WL 3771090, *2 (S.D.N.Y. Dec. 22, 2006) (permitting sampling of claims files on computer system, and deposition of individual knowledgeable about that system); *Semsroth v. City of Wichita*, 239 F.R.D. 630, 640 (D. Kan. 2006) (permitting search of employer's back-up tapes but limiting scope of search to specific search words and the identification of a specific number of identified mail boxes); *J.C. Assoc. v. Fid. & Guar. Ins. Co.*, 2006 WL 1445173, *1-2 (D.D.C. May 25, 2006) (permitting sampling of claim and litigation files).

Counsel should also involve the IT staff because they may need to provide declarations describing ESI systems and, specifically, the difficulties of accessing or producing second-tier information. The initial burden of proof is on the nonproducing party to justify why it does not intend to produce information from second-tier sources. That party will have to corroborate its contentions with affidavits or declarations. Department counsel will need the collaborative assistance of IT or records management specialists. Such specialists can describe, in detail, the various information systems at issue, including the limitations and the specific costs of accessing second-tier information (including monetary and personnel-related costs). These explanations must be presented in language that judges and opposing counsel can understand. The IT staff will become the principal proponents of the agency's position on this critical issue. A counsel's mere assertion that sources of information are not "reasonably accessible" is insufficient. *Peskoff v. Faber*, 2006 WL 1933483, *2 (D.D.C. July 11, 2006); *Thompson v. U.S. Dep't of Hous. and Urban Dev.*, 219 F.R.D. 93, 98 (D. Md. 2003) ("Conclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail.") Thorough preparation of IT staff, and, if appropriate, records management personnel, is indispensable if they become witnesses either at a deposition or at a discovery hearing.

Department attorneys also will need to evaluate what limits on second-tier discovery might be acceptable to the agency. The offer of opposing party to share or defray the costs of that discovery does not mean that the discovery is justified, or that it necessarily should proceed. *See* FED. R. CIV. P. 26 advisory committee's note (2006); Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 7 SEDONA CONF. J. 1, 21 (Fall 2006).

> The fundamental principle is that if electronically stored information resides on a

> source that is not reasonably accessible, such that the relevance of the information to either the claims or defenses or the general subject matter of the litigation cannot be determined without incurring 'undue' costs and burdens, then that electronically stored information is presumptively outside the scope of discovery. (Footnote omitted.)

See Cognex Corp. v. Electro Scientific Indus., 2002 WL 32309413,*5 (D. Mass. July 2, 2002) (willingness of requesting party to share or bear discovery costs did not outweigh the reasons against permitting the discovery).

Finally, when a Department attorney seeks second-tier discovery from the opposing party, it also will be important to provide a solid justification for that demand. The challenge will be how to show why the government's demands are not "unreasonably duplicative or cumulative" within the meaning of the Rule, and why the discovery is not obtainable from another source that is "more convenient, less burdensome, or less expensive." Department counsel will need to demonstrate that the burden of this discovery on the opposing party is outweighed by its "likely benefit" to the government's case.

V. Conclusion

No one should underestimate the many challenges of dealing with electronic discovery issues. The problems can be daunting and, unfortunately, there is not yet much useful guidance from decisions applying the recent Rules amendments. Rule 26(b)(2)(B) has considerable potential to assist our federal agency clients in resolving ESI disputes. The attorneys' goal should be to focus efforts on the first-tier discovery and work with opposing counsel to resolve discovery demands in that fashion. If that fails, then counsel needs to be able to convince the court to limit and insulate the agency from the burden and expense of ESI discovery.❖

ABOUT THE AUTHOR

❑**Theodore C. Hirt** is an assistant director in the Federal Programs Branch, Civil Division, of the Department of Justice. Mr. Hirt has been extensively involved in the federal rule-making process in his capacity as an advisor to the Assistant Attorneys General for the Civil Division. He serves as an ex officio on the Civil Rules Advisory Committee and as the Coordinator of the Department's E-Discovery Working Group and has given numerous presentations on Rules issues.✠

Managing Electronic Discovery in the Rule 26(f) Conference

Daniel S. Smith
Trial Attorney
Environmental Enforcement Section
Environment and Natural Resources Division

I. Introduction

The amendments to the Federal Rules of Civil Procedure that went into effect on December 1, 2006 drew a great deal of attention to the growing needs associated with electronic discovery, but they enacted little substantive change. Federal courts have recognized for more than 30 years that

electronically stored information (ESI) is subject to discovery. FED. R. CIV. P. 34 advisory committee's notes (1970), *available at* http://www.law.cornell.edu/rules/frcp/ACRule34.htm. Rather than drastically change the scope of discovery, the 2006 amendments implemented procedural changes that recognized that the world is simply not the same place that it was 30 years ago. Electronic communications have proliferated rapidly and have replaced not only paper correspondence, but also casual talk around the office water cooler. *Thompson v. HUD*, 219 F.R.D. 93 (D. Md. 2003) (citing *Byers v. Ill. State Police*, 2002 WL 1264004 at *10 (N.D. Ill. June 3, 2002)). Government agencies may have to obtain electronic information and evidence in order to execute their congressionally-mandated functions. Consequently, these agencies have particular interest in both obtaining and properly managing electronic discovery.

The volume of ESI that a large organization might possess is staggering; like astronomical distances, it is difficult to comprehend. *See* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?* 13 RICH. J.L. & TECH. 10 (2007) (comparing the expansion of ESI to cosmic inflation). The cost of managing this volume of data can become unmanageable in civil litigation. The Sedona Conference recently estimated that it can cost as much as $32,000 to have a single gigabyte of data reviewed for privilege, using typical page-by-page methods of review. *The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189, 198 n. 13 (Jason R. Baron et al. eds., 2007) [hereinafter *Sedona Conference® Commentary on Search Methods*], *available at* http://www.thesedonaconference.org/content/miscFiles/publications_html (select hyperlink below pub. no. 7). With some organizations now measuring their network data storage in petabytes (1,000,000 gigabytes), *see* Kevin Maney, *Size of NSA's database of phone-call records isn't all that impressive*, USA TODAY, May 17, 2006, at 3B, *available at* http://www.usatoday.com/money/industries/technology/maney/2006-05-16-nsa-privacy_x.htm, the potential litigation costs are astronomical.

The 2006 amendments to the Federal Rules sought to create a framework on which trial lawyers can build solutions to the problems associated with electronic discovery. Chronologically, the first of the major 2006 amendments that an attorney will encounter, after filing or being served with a complaint, is the amendment to Rule 26(f) regarding the discovery planning conference. This article will discuss how the 2006 amendments changed the rules governing the Rule 26(f) conference. Next, this article will discuss the things that a well-prepared attorney can do at a Rule 26(f) conference if significant discovery of ESI is expected. Finally, this article will discuss how an attorney might change his or her approach to the Rule 26(f) conference and what advice to give to clients who are frequently involved in litigation dealing with ESI.

II. The 2006 Amendments to Rule 26(f)

The 2006 amendments to Rule 26(f) changed little of the text of the rule, but those small changes carry the possibility for significant change to the process of civil litigation. As edited by the nonsubstantive 2007 amendments, Rule 26(f) now states that parties must, *inter alia*, "discuss any issues about preserving discoverable information," FED. R. CIV. P. 26(f)(2), and submit a proposed discovery plan that includes the parties' views on "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." *Id.* 26(f)(3)(C).

Nearly all of the other 2006 amendments to the Federal Rules are linked to the amendment to Rule 26(f). Amended Rule 16(b), which now includes provision "for disclosure or discovery of electronic information" among the topics to be addressed in the scheduling order, FED. R. CIV. P. 16(b)(3)(b)(iii), relies upon the outcome of discussions at the Rule 26(f) conference. The format of ESI that may be produced in discovery under Rules 33, 34, and 45 must be discussed at

the Rule 26(f) conference. FED. R. CIV. P. 26(f)(3)(C). Even the amendment to Rule 26(b)(2)(B), which excludes from discovery ESI that is "not reasonably accessible," comes into play in the Rule 26(f) conference pursuant to the directive that parties discuss "any issues about disclosure or discovery of electronically stored information." FED. R. CIV. P. 26(f)(3)(C).

Litigation holds, which have drawn ever-increasing amounts of attention and concern among trial lawyers, are listed among the topics for discussion. FED. R. CIV. P. 26(f)(2) (stating that the parties must "discuss any issues about preserving discoverable information"). This, in turn, raises the issue of the parties' and the court's interpretations of the 2006 amendment to Rule 37, which created a limited safe harbor for ESI "lost as a result of the routine, good-faith operation of an electronic information system." FED. R. CIV. P. 37(e); *see also* FED. R. CIV. P. 37, advisory committee notes (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. ("Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to preservation obligation.")

III. Goals for the Rule 26(f) conference

The mandatory topics for discussion at the Rule 26(f) conference raise a number of opportunities for the well-prepared attorney.

- First and foremost, the litigator is afforded an early opportunity to seek to prevent the scope of discovery from becoming so unmanageable that the client loses the ability to function.
- Second, the Rule 26(f) conference provides an opportunity to negotiate the scope of a litigation hold.
- Third, the Rule 26(f) conference affords an opportunity to bring wasteful discovery to a stop before it starts.
- Finally, the Rule 26(f) conference provides the parties with an opportunity to improve efficiency by ensuring that ESI produced in discovery can be readily accessed and used.

A. Preserving the client's ability to function

The first opportunity mentioned above, the opportunity to ensure that discovery does not unreasonably obstruct the business of the client, is perhaps the most important one afforded. FED. R. CIV. P. 26(f), advisory committee's note (2006), *available at* http://www.uscourts.gov/rules/Reports/CV5-2005.pdf, ("The parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities.") One early case provides an example of what can happen to unwary counsel. In *Palgut v. Colorado Springs*, 2006 WL 3483442 (D. Colo. Nov. 29, 2006), a magistrate judge issued an order entitled "Electronic Discovery Plan and Order to Preserve Evidence." Among other things, the order stated that "[n]either party may alter, interlineate, destroy, or permit the destruction of any document, as defined herein, in its possession, custody or control, without further order of court." The term "document" was defined in the order to mean, among other things, "[a]ll digital or analog electronic files, including 'deleted' files and file fragments." The problem lies in this highly inclusive definition of "document." Whenever a typical computer is performing any sort of operation, it is likely to be writing and rewriting to various portions of the hard drive to store information. Some of the portions of the hard drive used in this process will inevitably contain files that have been deleted but are still recoverable until the time that portion of the hard drive is used again. Thus, by performing even the most basic functions with a computer, including starting it up or shutting it down, the parties in *Palgut* could arguably be seen as destroying or

deleting files or file fragments in violation of the court's order.

In order to help avoid such problematic orders, an attorney can explain how a proposed preservation order or agreement will likely affect the client prior to the Rule 26 conference. This explanation will usually vary for each client, depending on the client's resources, the number, variety, and age of electronic information systems, and the manner in which electronic data systems are operated and maintained. An attorney can also prepare to offer reasonable preservation terms tailored to the facts and issues in dispute in the case. In formulating reasonable preservation terms, an attorney can seek to exclude from discovery—or make special preservation arrangements for—categories of ESI that are "not reasonably accessible" within the meaning of Rule 26(b)(2), or are otherwise not germane to the case.

In many civil cases, an attorney may identify categories of ESI that, depending on the facts and circumstances of the case, are "not reasonably accessible" or need special preservation arrangements. In some situations, the discovery and preservation of such ESI can become so burdensome as to interfere with the client's business. Some categories to consider include:

- disaster recovery back-up tapes;
- continuity of operations plan (COOP) equipment;
- system "mirrors" or "shadows";
- voice mail messages in a system not integrated with e-mail;
- instant messages;
- data on a personal digital assistant (PDA) that is regularly synchronized with more accessible hardware;
- logs of calls made from a wireless phone;
- "deleted" computer files;
- temporary or cache files, including Internet browsing history;
- server, network, or system logs;
- data temporarily stored on computer peripherals, such as laboratory equipment; and
- large or complex databases.

Deciding how to handle such materials will depend on the facts and circumstances of the case.

Some of the categories of ESI listed above include a high degree of duplication and indiscriminately including them in the scope of discovery can create a process so burdensome that the litigation becomes unmanageable. The contents of disaster recovery back-up tapes, COOP servers, system mirrors, shadow drives, and regularly synchronized PDAs will often consist almost entirely of duplicates of data more readily obtainable, in a more organized form, from active servers and computers. A party that expects to find significant differences between the active version of a document and a copy on a disaster recovery back-up tape may have to justify the high cost of copying, storing, and reviewing massive volumes of duplicative ESI. For organizations that generate several hundred gigabytes of disaster-recovery back-ups per day, the concern with preserving every back-up tape includes not just the cost of the tapes, but also the likelihood that a tape preserved for one case will contain data relevant to many other cases and the burden of searching, reviewing, and producing all preserved back-up tapes in the original case at a cost of up to $32,000 per gigabyte. In some cases, the parties may be able to achieve a satisfactory degree of preservation and discovery, at relatively low cost, by identifying specific files of interest that might exist on back-up tape and restoring only those files, rather than preserving entire tapes or libraries of tapes.

Attorneys should be careful to distinguish between disaster recovery back-up tapes and archival tapes created to provide long-term storage of data that is not stored on an active system. *See Zubulake v. UBS Warburg*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

> As a general rule, [a] litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

Id. But cf. Kemper Mortgage v. Russell, 2006 WL 2319858, *2 (S.D. Ohio Apr.18, 2006) ("[A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary.") with FED. R. CIV. P. 37, advisory committee notes (2006), *available at* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. ("Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation.") The distinction between disaster recovery back-up tapes and archival back-up tapes can be difficult in cases where a tape originally created as a back-up tape is set aside for a number of years.

Although many of the 12 categories of ESI listed above are included because of the level of potential redundancy, some categories of ESI are included because of the practical difficulties in accessing them. These categories can include voice mail, logs of calls made from cellular phones, deleted computer files, and temporary or cache files. Voice mail, in particular, can become an important item for discussion at the Rule 26(f) conference.

Whether recorded to analog audio tape, stored on hard drives in a specialized system (which may have its own digital back-up tape system) or delivered to an e-mail inbox as compressed digital audio files, voice mail messages are ESI. *Cf. Thompson*, 219 F.R.D. at 96. Many large-scale voice-mail systems available commercially use hard drives to store voice mail messages but, nonetheless, lack a convenient means of transferring the electronic files to other media, such as another hard drive or a CD-ROM. Users attempting to save voice mail in such a system as part of a litigation hold may have only a few readily available means of doing so.

- They can save the voice mail message in the voice mail system, which can quickly fill up.
- They can hold a microphone next to the speaker of their phone and record the messages onto another media, which might have to be preserved and indexed in some way.
- They can transcribe the voice mail message, an activity likely to be time-consuming for individuals not trained to take dictation.

Although some companies may be preparing to fill this void by offering internet-based transcription services, *see* Kevin C. Tofel, *Souping Up a Cellphone for Maximum Multitasking*, N.Y. TIMES, Apr. 3, 2008, at C6, *available at* http://www.nytimes.com/2008/04/03/technology/personaltech/03basics.html, such services may prove unreliable and unduly expensive. At the Rule 26(f) conference, litigators can consider asking about the limitations of other parties' voice-mail systems, disclosing limitations in one's own voice-mail system, and possibly proposing to exclude voice mail from discovery or significantly restricting the discovery of voice mail.

As discussed above in connection with the *Palgut* order, deleted files can also pose a significant challenge. A broad order not to overwrite any deleted files can essentially equate to an order not to use a computer or a server, at least until a forensic image can be made. Forensic copying is expensive and can be disruptive or crippling to the client, particularly if servers are involved. Forensic copying can also generate massive quantities of ESI that the parties must review for privilege, produce, and consider for its evidentiary value. Forensic copying generates this volume of material not just by introducing many new documents, but possibly by introducing many copies of documents. Take for example, a Word document that took 4 hours to write. The author

will probably have his or her computer configured to automatically save a copy of the document every 10 minutes so that a power outage or computer crash does not cause the loss of several hours of work. In some computing environments, each auto-save can be recovered as a separate deleted file, such that the document that was undergoing changes for 240 minutes may have 24 "deleted" drafts available. Multiply the volume of discoverable documents in a civil case by 20 times or more, and the volume can become unmanageable for even the largest and most sophisticated parties.

Finally, databases, the last of the 12 categories of ESI identified above, present special challenges. First, an attorney may find that some client databases are highly relevant but too large, too sensitive, or too valuable to business competitors to produce in their entirety without reasonable limitations. In this situation, litigators may consider developing a plan to extract relevant data and produce it in a form that retains as much of the functionality of the original database as necessary. Conversely, an attorney may need to ensure that any data accepted from an opposing party's database include, to the extent possible, other elements of the source database that make it useful.

As discussed above, litigators may need to consider special provisions for preservation agreements because "freezing" a database may disrupt the client's ability to function. Sometimes, the entire value of a database to an individual or an organization lies in the fact that the database provides the most up-to-date representation of events as they change in real time, often entered from a number of different sources simultaneously. Telling a client to no longer update a database can be the same as saying not to keep track of information that is mission critical. When commentators warn that an overzealous litigation hold can threaten the ability of an organization to function, the possibility of freezing important databases is probably a major part of what they have in mind.

The potential for disruption to important databases is not the only concern at the Rule 26(f) conference. Litigators may wish to ensure that opposing parties have a reasonable plan for preserving important data that might otherwise disappear in the ordinary operation of a database. This might entail, for example, an obligation on the database's owner to run certain reports on a defined schedule, or in the case of some Web-enabled, nonprivileged government databases, it could be as simple as providing the opposing party with the knowledge that the database exists and instructions on how to make use of it.

B. Negotiate the scope of the litigation hold

The second opportunity afforded at a Rule 26(f) conference is the opportunity to negotiate the scope of a litigation hold. The duty to preserve evidence, which includes the duty to implement a litigation hold on documents and ESI, attaches when a party reasonably foresees litigation. *See Zubulake*, 220 F.R.D. at 218. When the duty arises before litigation actually begins, and when for strategic or practical reasons the party cannot negotiate document preservation with the opposition, the litigant must simply make its best informed judgment about what it must preserve and how. If it preserves too much, it may waste scarce resources. If it preserves too little, it may risk sanctions. *See, e.g., Mosaid Techs. Inc. v. Samsung Elecs. Co.,* 348 F. Supp. 2d 332, 335 (D.N.J. 2004). Faced with this dilemma, a litigating party may be anxious to try to reach an agreement on the scope and method of preservation once litigation begins. The Federal Rules of Civil Procedure give parties two opportunities to reach an agreement: the Rule 26(f) conference and the Rule 16 conference. *See* FED. R. CIV. P. 16(c)(2)(F) & 26(f)(3)(F).

There are good reasons to take advantage of the opportunity to reach an agreement or seek an order regarding preservation. One reason is that it allows the parties and the court to consider the costs, burdens, and benefits of specific preservation methods on more equal footing. In the absence of a preservation agreement or order, a party later alleging spoliation will have the benefit of hindsight and theoretical arguments.

That party may be able to identify a specific preservation method that was not used and argue that the failure to take that step resulted in the destruction of certain identifiable pieces of evidence. In the context of drafting a preservation agreement at the Rule 26(f) conference, however, the parties and the court can consider the proposed preservation methods, and their cumulative burdens and benefits, more evenhandedly.

A negotiated preservation agreement or order also entails risks. An attorney may fail to identify problematic categories of ESI or agree to broad preservation requirements that the client cannot meet. Conversely, an attorney might inadvertently excuse an opposing party from preserving important information because he or she fails to appreciate the relevance of the ESI at the time of the agreement. One strategy to address these risks is to draft the preservation agreement narrowly so that it merely exempts fixed categories of ESI that have no relevance, while leaving all other ESI subject to generally applicable preservation requirements, without specifying them.

C. Curtail wasteful discovery before it starts

In addition to ensuring the ability of the client to function and negotiate the scope of the litigation hold, the Rule 26(f) conference provides a number of opportunities to try to put a stop to wasteful discovery. A thorough discussion of techniques is beyond the scope of this article. However, if the parties have agreed to exclude some categories of ESI (see part III. A. above), they will find themselves on the right track. Two additional techniques warrant mention here.

One way that litigators may be able to significantly reduce wasteful discovery is to use agreed-upon search terms to identify which documents will be produced in discovery. Various search techniques are discussed in detail in a recent paper by the Sedona Conference®. *Sedona Conference® Commentary on Search Methods*, *supra*. The resulting savings from using a tailored list of search terms can extend throughout the discovery process if the volume of materials identified by the electronic search is smaller and more accurate than what traditional techniques would have identified.

In many cases, the Rule 26(f) conference will come too early in the litigation for the parties to discuss specific search terms. However, the Rule 26(f) conference affords, at a minimum, a good opportunity to educate opposing counsel, if necessary, about the benefits of electronic searches and the variety of techniques available, and to secure a commitment from him or her to meet and confer on the issue of electronic search technology at a later date. If counsel for both parties are already familiar with the benefits of electronic search technology and agree that such techniques are appropriate for the case, counsel may be able to discuss which electronic information systems maintained by each side are electronically searchable, which search techniques are available, and whether new search tools might be desirable or practicable.

A second technique applies in those cases where opposing counsel has little interest in cooperating or reducing the pain and expense of discovery. In those cases, such as where one side expresses an interest in what some call "scorched earth discovery," the Rule 26(f) conference nonetheless remains an important step in putting a stop to wasteful discovery. The strategy of the litigator can shift to documenting the rejection of sound proposals so that those proposals can be renewed at the Rule 16 conference. If litigators are to protect their clients from undue burden and expense in civil discovery, they must be willing to ask the court to impose reasonable limitations in the absence of agreement among the parties.

D. Ensure that information obtained in discovery is usable

As mentioned above, the Rule 26(f) conference affords litigators an opportunity to improve the efficiency of litigation by ensuring that information is exchanged in a form that maximizes its usability. At its most basic level, this can mean specifying the format of the ESI that the parties exchange so that the receiving party can use it, or demanding a showing of

relevance where an opposing party demands a burdensome format. *See* FED. R. CIV. P. 34(b)(1)(C). However, it can mean much more.

First, in cases where native format ESI is important, a party can try to address any concern that opposing parties will "downgrade" ESI in the process of preserving or producing it. Downgrading ESI means reducing its usability. The most common example is printing e-mails to paper. *See, e.g., In re Instinet Group, Inc. S'holders' Litig.*, 2005 WL 3501708 (Del. Ch. Dec. 14, 2005). When e-mails are in an electronic form, users can search them and quickly sort them by sender, recipient, domain name, subject matter, and/or date. If e-mails are in their electronic form with metadata available, users may also be able to eliminate duplicate copies by relying on a unique identifier string contained in the "MessageID" field.

Spreadsheets are another type of file that can be downgraded by printing to paper. In many cases, the results of each cell in the spreadsheet will print to paper, but the formulas contained in each cell will not. Yet formulas are an important part of spreadsheets. Moreover, exchanging paper copies of spreadsheets can create unnecessary data-entry work. If the receiving party wants to run calculations, the data will have to be typed into a new spreadsheet (with or without the help of optical character recognition) in a process that takes time and money and has the potential to introduce errors.

Well-prepared parties may have the opportunity to go even further in ensuring the efficiency of discovery. In a case involving extensive expert testimony and computer models, the parties may be able to reach agreement as to which software the expert witnesses will use. In the case of expert witnesses using sophisticated computer-modeling applications, the ability of each expert to read the opposing party's model without converting it into a useable format can significantly reduce the time and expense of expert discovery.

IV. Preparing for a Rule 26(f) conference

If any of the potential benefits of the Rule 26(f) conference discussed above are to come to fruition, the litigator must take a different approach to the conference and to discovery in general. It is more important now than ever to "front-load" the work, spending more time on discovery planning, hopefully with the result of spending less time on the actual preservation, gathering, review, production, and use of ESI.

To accomplish any of these objectives, the litigator needs information.

- What electronic information does the client possess or have control over?
- Where is the electronic information physically located?
- What form is it in and to what forms can it be converted?
- What ESI is routinely deleted or overwritten?
- What ESI is likely to be duplicated?
- What ESI, such as legacy data and systems, is going to be difficult to access?
- Have problems been encountered in discovery in earlier cases?
- What can the client agree to that would facilitate discovery?
- How will incoming ESI from the opponent be managed?

Gathering the answers to these questions can take time. It can take days or even weeks just to identify the individuals able to answer these questions. Even after the individuals are identified, it may take some time to ensure that the attorney and client understand the questions and the answers and to address any miscommunication and false assumptions.

Clients, particularly large organizations, may balk at such demands and object to any drastic change to the usual way of doing business with respect to discovery. To help manage the

transition to cases with increased electronic discovery (e-discovery), litigators may recommend that clients begin collecting the information needed for the Rule 26(f) conference, even in the absence of any specific litigation, in the form of an inventory of ESI. Large organizations that are regularly involved in litigation may find such an inventory to be efficient in that it can help ensure consistency and thoroughness and avoid having information technology (IT) staff answer the same questions for every litigation. Taking an inventory of ESI can also help establish the baseline "routine operations" of the client's electronic information systems, which may prove useful should the client need to argue that a loss of ESI occurred within the safe harbor of Rule 37(e).

An increasingly common step in preparing for a Rule 26(f) conference is to arrange for an IT specialist to attend. This can be helpful, but may not be sufficient. IT specialists have their own subspecialties and scope of responsibilities. A specialist who designed and operates the client's e-mail system, for example, may know little about voice mail or important databases.

V. Conclusion

ESI has become so important to business, government, and individuals that forgoing it in discovery can mean, in some cases, forgoing the bulk of the information available. Yet poorly managed electronic discovery has the potential to derail litigation and impose exorbitant costs on the parties. The trial lawyer has the opportunity to strike a balance between the burden and benefits of electronic discovery. Striking such a balance usually requires early preparation and a coordinated approach. The Rule 26(f) conference presents the first formal opportunity to proactively manage the scope of e-discovery, and its importance cannot be overstated. Litigators who handle these conferences the same way they did 30 years ago do so at their client's peril. The Rule 26(f) conference is an opportunity to lay a framework that affects every phase of e-discovery. Taking advantage of this opportunity requires much advance preparation. Attorneys with clients who are frequently involved in litigation can consider advising their clients to start preparing an inventory of ESI to manage discovery burdens.❖

ABOUT THE AUTHOR

❑**Daniel S. Smith** is a Trial Attorney in the Environmental Enforcement Section. He has held that position for five years, since being accepted into the Attorney General's Honors Program.✠

The views expressed in this article are those of the author and should not be construed as formal guidance. This article has not been adopted as the formal view of the Environment and Natural Resources Division, the Department of Justice, or any other federal agency. This article does not create any right or benefit, substantive or procedural, enforceable at law by any person against the United States, its agencies, officers, or any other person.

Electronic Discovery Resources

Adam Bain
Senior Trial Counsel
Environmental Torts Section
Torts Branch, Civil Division

Jennifer L. McMahan
Supervisory Librarian
Justice Management Division
U.S. Department of Justice

I. Introduction

The 2006 amendments to the Federal Rules of Civil Procedure regarding electronically stored information (ESI) present many new challenges for Assistant United States Attorneys (AUSAs). The amendments encourage AUSAs to become familiar with the workings and management of information technology systems to meet discovery obligations. The rules also address issues unique to ESI that many AUSAs have had little, if any, experience addressing. For example, AUSAs will need to determine where electronic information resides and how they can manage and preserve the ESI. They will need to develop strategies for searching ESI for relevant material. In turn, large amounts of ESI will require that AUSAs determine the best way to protect privileged matters within the ESI. AUSAs will also need to decide which forms of ESI are appropriate for production in a case. These and other issues will test the abilities of AUSAs to adapt to information technologies and to deal with the increasing amounts of data.

Fortunately, there are many resources available to help deal with ESI issues in litigation. In addition to the traditional sources, such as case law, articles, and treatises, an entire industry of electronic discovery consultants offer a variety of information and services. Not surprisingly, almost all of these resources are available electronically and many provide information free of cost. This article discusses the various electronic discovery resources that are available.

This description of the electronic discovery resources is not exhaustive, nor could it be. New sources of information regarding electronic discovery appear almost daily. The purpose of this article is to inform the reader of some useful resources that will help AUSAs keep abreast of current developments in the field. Initially, the article discusses primary sources of information, including information about the Federal Rules of Civil Procedure and the case law addressing electronic discovery issues. Some useful secondary sources, including law reviews, treatises, and Web sites that focus on electronic discovery, are also covered. Finally, the article reviews some internal resources that offices have developed specifically for AUSAs.

II. Primary sources of information regarding electronic discovery

In dealing with electronic discovery issues, the most important place to begin is with the procedural rules governing ESI. The federal rules are available at http://www.uscourts.gov/rules. In interpreting the amendments to the Federal Rules of Civil Procedure regarding ESI, many courts will consider the Advisory Committee's notes for the amendments, which are available at http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. For more in-depth discussion of the rules changes, Advisory Committee Reports can be found at http://www.uscourts.gov/rules/supct1105/Excerpt_CV_Report.pdf (Excerpt of the Report of the Advisory Committee on Civil Rules (July 2005)). Primary materials regarding the rules are also available on LexisNexis, which maintains a site on the e-discovery rules changes, *available at* http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp. Significantly, this site provides easy access to other electronic discovery rules, including federal court local rules, state court rules, and evidentiary rules. There is also a link to bar association and ethics opinions on electronic discovery.

Perhaps the most important primary source for AUSAs is the case law. There are several resources that provide ready access to the case law on electronic discovery, though none of these can serve as a substitute for traditional case law research. LexisNexis provides short summaries of electronic discovery cases, organized alphabetically, by topic, jurisdiction, and federal rule. *See* http://www.lexisnexis.com/applied discovery/lawlibrary/casesummaries.asp. Full-text access to the opinions is available with a Lexis account. The law firm of Kirkpatrick & Lockhart Preston Gates Ellis LLP also provides a Web site with an electronic discovery case search engine. *See* https://extranet1.klgates.com/ediscovery. The cases on this site are searchable by federal rule number, procedural context, issue, or keywords. The cases often include a detailed case summary and sometimes include a link to the full text of the opinion. Finally, Westlaw has a database (EDSCVRY-CS) devoted to cases addressing electronic discovery issues.

ESI documents produced by the Sedona Conference, a nonprofit legal policy organization that sponsors working groups of judges, attorneys, and others to address cutting-edge legal issues, including electronic discovery, may also fit within the general category of primary resources because many judges and practitioners consider these as foundational documents for the Civil Rules amendments on ESI. Both before and after the 2006 amendments to the Federal Rules of Civil Procedure, courts have referenced documents from the Sedona Conference to help resolve e-discovery issues. *See*, *e.g.*, *In re Seroquel Prod. Liab. Litig.*, 244 F.R.D. 640, 656 (M.D. Fla. 2007); *Zubulake v. UBS Warburg*, 229 F.R.D. 422, 440 (S.D.N.Y. 2004). Specifically, the Sedona Conference Working Group on Electronic Document Retention and Production has produced "The Sedona Principles Addressing Electronic Document Production, Second Edition (June, 2007)," and "The Sedona Conference Commentary on Email Management (Aug., 2007)." All of the documents of this Working Group are available at the Sedona Conference Web site at http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110.

III. Secondary sources of information regarding electronic discovery

There are also a wide variety of secondary sources of information on electronic discovery issues. Some of the secondary sources are devoted exclusively or primarily to electronic discovery. Others, including several law journals, frequently include topics on electronic discovery. Many law journals that focus on technological issues include a link to the full text of the articles on the journal's Web site. For example, the *Richmond Journal of Law and Technology* has an "e-discovery archives" on its Web site and has recently published articles on preservation, accessibility, and privilege-waiver, among other electronic discovery topics. *See* http://law.richmond.edu/jolt/ediscovery/index.asp. Another law review that has frequently published on electronic discovery issues is the *Federal Courts Law Review*. *See* http://fclr.org/content/articlelist.htm. The editorial board of this journal consists primarily of United States Magistrate Judges and law school professors. Consequently, its articles frequently focus on issues of importance to federal litigators. The Sedona Conference also publishes a journal which often includes articles on electronic discovery. *See* http://www.thesedonaconference.com/thejournal_html. The full text of articles from the *Sedona Conference Journal* are not available at the Sedona Conference Web site, but are accessible through Westlaw or Lexis.

The Bureau of National Affairs (BNA) and other publishers produce periodic litigation reports that cover electronic discovery and related topics. The newsletters typically include summaries of recent cases and practice articles. *See* BUREAU OF NATIONAL AFFAIRS, DIGITAL DISCOVERY & E-EVIDENCE REPORT (Aug. 1, 2007), *available at* http://www. ddee.bna.com. Access to the monthly newsletter and the full text of individual cases and articles, as well as the text of pleadings, motions, and briefs addressing electronic discovery issues, are available at the site. The Web-based journal LLRX.com contains an extensive archive of

articles on electronic discovery. The site also publishes a periodic article on electronic discovery entitled the "E-Discovery Update" which is available at http://www.llrx.com/category/1056. Finally, Findlaw.com has a page devoted to electronic discovery in its legal technology center which is available at http://www.technology.findlaw.com/electronic-discovery. In addition to articles, this page includes a number of useful resources, including an "e-discovery wizard" which provides an index of articles and a checklist for each Federal Rule of Civil Procedure dealing with electronic discovery.

Westlaw maintains a database (EDSCVRY-TP) devoted to secondary sources addressing electronic discovery issues. This database contains documents from law reviews and journals, annotated law reports, continuing legal education material, and other periodical material related to electronic discovery. Lexis maintains a Litigation Practice and Procedure directory. Within this directory, Electronic Discovery and Evidence is a subset of Emerging Issues and includes the following:

- *Mealey's Litigation Report: Discovery*, a monthly litigation report on discovery issues generally, which frequently addresses electronic discovery;
- Chapter 37A, "Discovery of Electronically Stored Information," of James Wm. Moore, et al., MOORE'S FEDERAL PRACTICE; and
- Chapter 900 of Jack B. Weinstein, WEINSTEIN'S FEDERAL EVIDENCE, titled, "Discovering and Admitting Computer-Based Evidence."

In addition to court rules and case law, LexisNexis contains:

- a newsletter on electronic discovery;
- sample motions, orders, and preservation letters related to electronic discovery; and
- white papers covering various electronic discovery topics.

See http://www.lexisnexis.com/applieddiscovery.

A number of private companies that offer electronic discovery consulting services also maintain Web sites which provide access to information regarding electronic discovery and evidence. Kroll Ontrack maintains a site which includes a monthly newsletter, case law summaries, and articles. *See* http://www.krollontrack.com/legalresources. Some companies require the user to register and provide identifying information before allowing access to their sites—Fios is one such organization. It publishes periodic newsletters and white papers on electronic discovery services. *See* http://www.fiosinc.com/resources.

These are just two of the companies that offer electronic discovery services. There are other resources from private companies available online; however, they are of variable quantity and quality. Additionally, remember that these companies are ultimately in the business of making money through consulting, and the information offered online is a marketing tool. The information provided may be a good source of background material, but AUSAs should not substitute this information for traditional legal research or the use of primary sources to resolve electronic discovery issues.

Some companies provide electronic discovery training, including in-person seminars and online "Webinars." This training can be useful for staying current on developments in the law of electronic discovery. Sometimes the training is certified for continuing legal education credit. AUSAs must make sure that they are not receiving any impermissible benefits under applicable government ethics rules if they take advantage of the "free" services that are offered. If there is any doubt at all, consult with the appropriate ethics officer.

Finally, if an AUSA determines that it is necessary to hire an electronic discovery consultant, he or she should check with litigation support employees and others in the organization for references. The same due diligence is required in hiring an electronic discovery consultant as in hiring any other type of consultant or expert. There

may be security requirements that the electronic discovery consultant must satisfy in order to work with government information systems. Therefore, the AUSA should make sure that the organization's information technology and litigation support personnel are involved in hiring and working with the consultant. Socha Consulting provides a yearly survey of electronic discovery consultants. *See* http://www.socha consulting.com/2007survey.htm. The survey evaluates the top 20 electronic discovery service providers by experience, capacity, corporate rankings, and law firm rankings. A brief public report is available on their Web site. A very detailed report of the 2007 survey is available for $5,000.

The American Bar Association (ABA) also has Web pages devoted to electronic discovery; however, some of the resources are available only to members, while others are available for purchase. *See* http://www.abanet.org/tech/ltrc/fyidocs/ediscovery.html. The ABA electronic discovery site includes links to articles, books, and consultants. Several practice articles are available from the Section on Litigation, but only ABA members can access them. *See* http://www.abanet.org/litigation/issuecenter/issue_ediscovery.html. The ABA has also published several books on electronic discovery that are listed on the site. One book, *The Electronic Evidence and Discovery Handbook*, is particularly useful as a resource for forms, checklists, and guidelines, which are conveniently included as Microsoft Word document files on a CD-ROM. SHARON A NELSON, BRUCE A. OLSON & JOHN W. SIMEK, THE ELECTRONIC EVIDENCE AND DISCOVERY HANDBOOK (2006).

There are also treatises available on electronic discovery law that are periodically updated. One of the most popular treatises is by a former AUSA, Michael R. Arkfeld, *Electronic Evidence and Discovery*. MICHAEL R. ARKFELD, ELECTRONIC EVIDENCE AND DISCOVERY (2d ed. 2007). The treatise comes with a companion CD-ROM and a practice guide. MICHAEL R. ARKFELD, ARKFELD'S BEST PRACTICES GUIDE FOR ELECTRONIC DISCOVERY & EVIDENCE (2007). Another treatise that is updated annually is *eDiscovery & Digital Evidence*. This treatise also comes with a CD-ROM of practical forms. JAY E. GRENIG, WILLIAM C. GLEISNER, TROY LARSON & JOHN L. CARROLL, EDISCOVERY & DIGITAL EVIDENCE (2005).

Last, but certainly not least, an excellent source of secondary materials on electronic discovery is the Federal Judicial Center (FJC), which is the educational and research agency for the federal courts. The FJC offers resources and publishes guides for federal judges. Thus, AUSAs who frequently practice before federal judges would be wise to consult these resources. The FJC maintains a page on its Web site entitled "Materials on Electronic Discovery: Civil Litigation." *See* http://www.fjc.gov/public/home.nsf/autoframe?openform&url_r=pages/196. The page "contains links to articles, PowerPoint slide presentations, and other items of interest on electronic discovery." Additionally, as noted on the site, the materials listed "were prepared by Federal Judicial Center staff for use in judicial and continuing legal education programs and are not subject to copyright." Accordingly, the materials may be downloaded and republished without permission. The site also includes some sample electronic discovery forms and orders from various sources, including cases, as well as the *Manual for Complex Litigation* (4th ed. 2004). Perhaps the most useful publication on electronic discovery is part of the FJC pocket guide series, the recently published *Managing Discovery of Electronic Information: A Pocket Guide for Judges*. BARBARA J. ROTHSTEIN, RONALD J. HEDGES & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES (2007). This concise, 27-page guide is an excellent primer on electronic discovery, with a glossary of terms and is available online at http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

IV. Sources for staying current on electronic discovery developments

In addition to the sources discussed above, there are several ways to stay current with

developments in electronic discovery law. Several sources provide periodic e-mail updates on electronic discovery law.

- Michael Arkfeld sends out a biweekly update designed to provide a "snapshot of electronic discovery activity." To receive it, sign up for the e-mail updates at http://www.arkfeld.blogs.com.
- BNA offers a free weekly e-mail on electronic discovery called the "Electronic Evidence Update." Subscribe to this newsletter at http://www.pf.com/ddeePD.asp.
- Kroll Ontrack provides a monthly e-mail update. Subscribe to this e-mail update at http:///www.krollontrack.com/newsletters.
- LexisNexis provides a monthly e-mail "case summary alert service" for recent cases dealing with electronic discovery. Sign up for this e-mail alert service at http://www.lexisnexis.com/applieddiscovery/default.asp.

Another source of current information on legal developments is the "blawg." A blawg is a Web site containing current news, sites, and events that is maintained in reverse chronological order. Blawgs provide news and commentary on particular legal topics and usually include links to other related Web sites. There are several blawgs devoted to electronic discovery.

- The law firm of Kirkpatrick & Lockhart Preston Gates Ellis LLP maintains a blawg called "Electronic Discovery Law." *See* http://www.ediscoverylaw.com. The blawg is billed as a "blog on legal issues, news, and best practices relating to the discovery of electronically stored information published by the E-Discovery Analysis and Technology group at K & L Gates." This blawg is typically updated several times each week. Subscribe to the site to receive an e-mail every time there is a new entry.
- Michael Arkfeld also maintains a blawg on electronic discovery, "Electronic Discovery and Evidence." *See* http://arkfeld.blogs.com. This blawg, advertised as a "daily digest of cases, comments and other matters related to electronic discovery and electronic evidence," is actually updated about once per week.
- The law firm of Quarles & Brady LLP also has a blawg, amusingly entitled "E-Discovery Bytes: A Practical Resource for Issues in E-Discovery." *See* http://ediscovery.quarles.com. The blawg is updated about once per week. Subscribe to the blawg to receive e-mail updates.
- For a "team approach" to electronic discovery, browse the "e-Discovery Team" blawg, touting the "team approach to electronic discovery combining the talents of law and IT." *See* http://ralphlosey.wordpress.com. This blawg includes in-depth discussion of recent cases and topics concerning electronic discovery management.
- Finally, an attorney and former IT consultant maintains the "Electronic Discovery Blog," which is updated about once per month and has a subscription feature. *See* http://www..electronicdiscoveryblog.com.

To learn more about blawgs generally, Justia.com and the ABA each maintain a directory of blawgs. *See* http://blawgsearch.justia.com; http://www.abajournal.com/blawgs. The ABA Journal also ranks the 100 best blawgs by category. *See* http://www.abajournal.com/blawgs/blawg100.

V. Internal sources of information on electronic discovery

The AUSA should also consider internal sources of information on electronic discovery. The Department of Justice Virtual Library offers many electronic discovery resources. The Virtual Library home page has a link to "Information by Subject" and from that page there is a link to e-discovery resources. It includes links to books, law review articles, training materials, video presentations, Web sites, and many other resources. In fact, most of the sources of information on electronic discovery described in

this article are available on this page, with convenient hyperlinks.

Finally, an AUSA should always check to determine whether his or her own office has developed a repository of information on electronic discovery or retained an electronic discovery consultant. An organizational resource can help the AUSA address electronic discovery issues that are specific to the organization's information technology system. Before diving head first into a difficult electronic discovery problem, it is best to check with the organization's information technology and litigation support personnel to see if resources are already in place to assist with the issue.

VI. Conclusion

The federal civil rules changes regarding ESI are easily overcome because of readily available resources, which are accessed by a few mouse clicks. The authors of this article have attempted to alert AUSAs to the breadth of these available resources. The use of these resources, along with legal education, training, and experience, will enable AUSAs to meet the challenges of electronic discovery.❖

ABOUT THE AUTHORS

❑**Adam Bain** is a Senior Trial Counsel in the Environmental Torts Section of the Civil Division. He has lectured frequently in Washington, D.C. and at the National Advocacy Center on the rules amendments relating to electronic discovery and periodically gives a class with the Department of Justice librarians on finding, using, and investigating expert witnesses with online resources.

❑**Jennifer L. McMahan** has been with the Justice Libraries for 9 years and currently serves as the head librarian for the Civil, Criminal, and Civil Rights Divisions. She has given numerous presentations in Washington, D.C. and at the National Advocacy Center on expert witnesses, public records research, and searching the Web.✠

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all federal law enforcement personnel who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete shipping address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-705-5659. Your cooperation is appreciated.