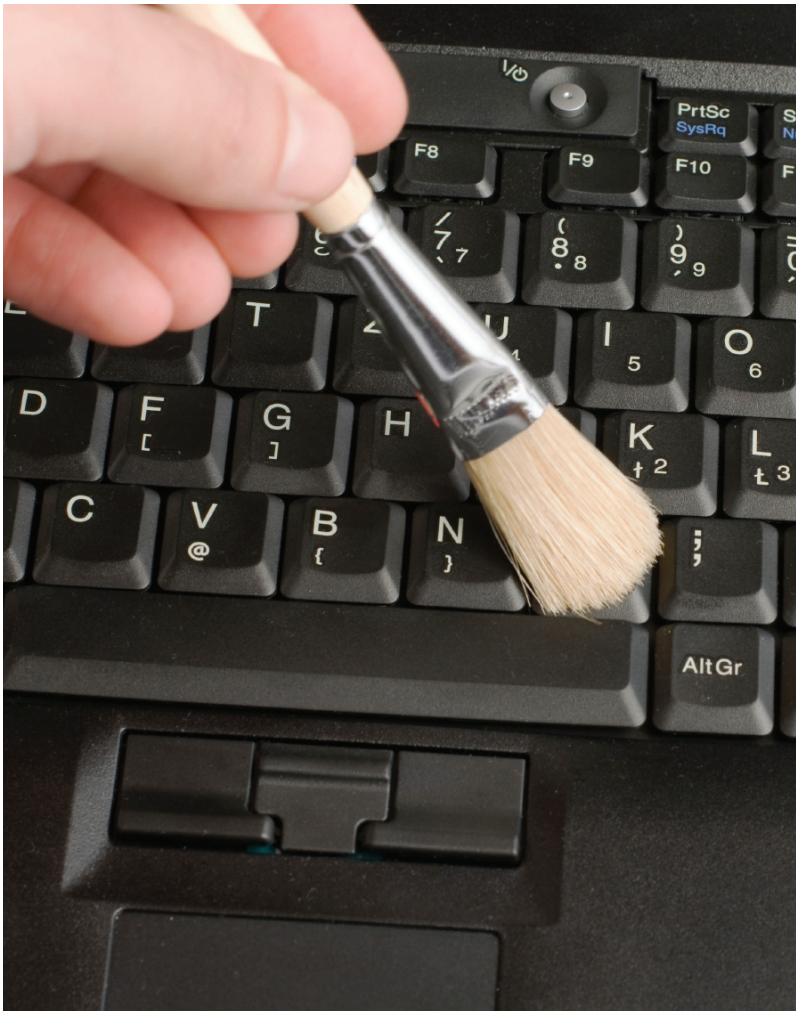
HAVE YOU EMBRACED THE NEW E-DISCOVERY RULES OR ARE YOU JUST HOPING YOU WON'T HAVE TO DEAL WITH THEM?

BY JOHN L. KRIEGER, ESQ.



The amendments to the Federal Rules of Civil Procedure governing electronically stored information (ESI) have been in effect for a little over two years now. Unfortunately, many attorneys still pay no attention to the new rules, or have only a rudimentary knowledge of how electronic information is stored, such that they do not know to ask for it. Given the ubiquitous nature of ESI in almost every facet of daily life, every lawyer needs to understand and know how to prepare for electronic discovery or risk sanctions, malpractice claims and/or discipline by the state bar.

What Is ESI?

Conventional paper documentation and evidence are quickly becoming relics of the past. More and more, companies and individuals are creating, exchanging and storing information electronically. ESI can take numerous forms, including, but not limited to, e-mails, Web pages, word processing files, databases stored in computers or on magnetic disks, DVDs, CDs and flash memory. ESI is likely located in multiple places on any given computer system (e.g., on various hard drives of an individual's computer, in various locations on a system's server). However, ESI may also exist in places that may not immediately come to mind, such as cellular telephones and personal digital assistants (PDAs), which may contain telephone numbers and addresses, photographs, logs of missed and received calls, recorded conversations, management notes, calendars and possibly faxes. ESI may also include hidden information, such as metadata and embedded data.

Invariably, ESI has the potential to be exponentially greater in volume than paper information. Moreover, producing ESI will inevitably become further complicated as new forms of technology are introduced and become part of everyday life. Consequently, it is important to understand at least what types of ESI your client has, even if you do not have a

complete grasp of the technology, as well as to anticipate the types of ESI the opposing party might have so that you can appropriately tailor discovery requests and deposition questions.

What Do You Need to Address at the Pretrial Conference?

Lawyers have an obligation to learn about their clients' electronic data and to be prepared to discuss it with opposing counsel at the outset of the case, primarily because the rules require it, but also because ESI can be altered or destroyed in the regular course of business. Rules 16(b) and 26(a) and (f) require lawyers to cooperate with each other and confront electronic discovery issues very early in the litigation. Rule 16(b) specifically places the burden on the lawyers to propose "provisions for disclosure or discovery of ESI," as well as "any agreements the parties have reached for asserting claims of privilege or protection as trial-preparation material after production" *in the scheduling order*. (The magistrate judges in Nevada still find that many scheduling orders filed with the court lack any reference to ESI or discussions between the parties regarding the same.)

Further, Rule 26(f) requires the lawyers to discuss and establish the protocol that will govern disclosure or discovery throughout the case, including the disclosure or discovery of ESI, preserving discoverable ESI and the manner in which ESI is to be produced, as well as issues of privilege regarding inadvertently disclosed information and "claw back" agreements. (A claw back agreement is intended to govern situations where a disclosing party inadvertently discloses documents that are privileged or protected. The receiving party is usually required to notify the producing party of the disclosure, promptly return the documents and not admit them into evidence and agree that no waiver has occurred.) A lawyer who does not understand what ESI a client has or stores could end up making embarrassing or sanctionable misrepresentations to the court or opposing counsel about a client's ability to comply with discovery requests or deadlines.[1]

CONTINUED ON PAGE 8 ▶

HAVE YOU EMBRACED THE NEW E-DISCOVERY RULES?

CONTINUED FROM PAGE 7

A checklist of ESI topics to be addressed at the 26(f) conference should probably include the following:

- steps each party will take to segregate and preserve electronic data,
- protocol for deleted information,
- protocol for back-up and archival data,
- file types and locations to be searched,
- number of relevant custodians,
- search terms for processing data,
- metadata and embedded data,
- accessible and inaccessible electronic data,
- the format and form of data production,
- whether to produce duplicate or near-duplicate documents,
- whether software will need to be purchased to read documents in native formats (e.g., engineering programs such as CAD, screenwriter programs),
- time periods for processing and production,
- allocation of costs between the parties (cost-shifting),
- preservation of information,
- selecting a common electronic discovery vendor, and,
- a "claw back" agreement regarding privileged or work-product production.

Early cooperation between opposing counsel on ESI will most likely reduce time, costs, and probably the risk of sanctions and will establish a cost-effective yet fair scope of discovery.

What Are the Scope and Limits of ESI Discovery?

In order to effectively serve a client, a lawyer must understand a client's electronic data, systems, storage, retrieval, archiving and retention policies and practices. For example, Rule 26(b)(2) exempts a party from being required to produce documentation that is not "reasonably accessible because of undue burden or cost." Lawyers, therefore, need to have good communication with the client, as well as the lawyers' IT staff and the client's IT staff, so that the sources and boundaries of what ESI is "not reasonably accessible" can be established.

Rules 33 and 34 have both been amended to address ESI. Rule 34 further recognizes the logistical differences between producing paper documents and ESI. For example, paper documents are usually Bates-numbered and produced. However, when it comes to ESI, the information may be maintained in several different native formats (e.g., TIFF, PDF or HTML) or in different programming formats (e.g., Microsoft Word, Microsoft Excel), all of which could be printed, copied or imaged differently and result in an extremely unmanageable and/or costly production. Rule 34 allows the requesting party to specify the form in which ESI is to be produced. The disclosing party is also entitled to object to the requested form and, in turn, offer production in a different format. If the requesting party fails to identify the format in which production is desired, the rule permits the disclosing party to decide how the documentation will be produced. If the parties are unable to reach an agreement, the court will ultimately resolve the issue and specify the form of production. In the absence of an agreement or court order, the rule allows a party to produce its ESI in the form "in which it is ordinarily

CONTINUED ON PAGE 10 ▶

HAVE YOU EMBRACED THE NEW E-DISCOVERY RULES?

CONTINUED FROM PAGE 8

maintained" or in forms that are "reasonably usable." Again, this rule underscores the importance that needs to be placed on the lawyer's obligation to understand the limitations of the client's and the lawyer's own IT departments, and what each is capable and not capable of doing.

What About Sanctions?

Parties have a duty to preserve potentially relevant data, which includes suspending routine data destruction.[2] This is known as a "litigation hold." A district court in the Ninth Circuit has indicated that the duty to preserve and institute a "litigation hold" begins when the party knows or reasonably should have known that evidence may be relevant to current litigation or "probable"/likely future litigation.[3] Events that may trigger a "litigation hold" include the filing or service of a complaint, a request to preserve evidence, or even a cease-and-desist letter. Failure to comply and institute a litigation hold may result in severe sanctions being levied against the client and/or the lawyer, which could include monetary sanctions, evidentiary sanctions, adverse inference instructions, dismissal or other adverse judgment.[4]

Due to the fact that ESI can be so easily destroyed in the normal course of business, companies and in-house counsel need to institute policies and procedures that govern ESI before any litigation ensues. Good policies and procedures may help a company avoid sanctions for spoliation should certain requested documentation have been inadvertently destroyed. For example, once litigation begins, the burden will invariably fall upon the shoulders of in-house counsel to institute the "litigation hold" and suspend any automatic destruction of documents, supervise and identify the distribution of and compliance with litigation holds, communicate and establish procedures about the location and preservation of ESI, and establish who will testify regarding ESI. In order to accomplish these tasks, in-house counsel must have a good understanding of the company's electronic data storage capability and procedures. Moreover, in-house counsel should act as a liaison between outside counsel, the company's IT department and company officers.

Outside counsel, however, cannot ignore their ethical obligations and simply rely upon the representations of the client or in-house counsel regarding the production of ESI. "[P]arties have a duty to provide true, explicit, responsive, and complete and candid answers to discovery, and their attorneys have a continuing duty to advise their clients of their duty to make honest, complete non-evasive discovery disclosures."[5] Probably the most surprising decision on the roles of in-house and outside counsel was rendered in the *Qualcomm Incorporated v. Broadcom Corp.* case.[6] The *Qualcomm* case was a complex patent infringement matter that involved millions of documents. However, it became apparent at trial that Qualcomm had failed to produce 46,000 e-mails and documents requested during discovery, which actually undercut Qualcomm's position at trial. A substantial amount of finger-pointing between in-house and outside counsel occurred once it became apparent the documentation had not been produced.

In the end, the court sanctioned Qualcomm for attempting to hide behind outside counsel and failing to conduct a proper search of its e-mail systems and produce the e-mails. The magistrate judge sanctioned outside counsel for failing to properly investigate and evaluate the inadequacy of the client's

document production as well as for ignoring evidence and warning signs that the client's production was inadequate. The magistrate judge imposed one of the highest monetary discovery sanction awards ever – over $8 million – and recommended six of the outside counsel for discipline by the state bar.

Rule 37(f), however, includes a "safe harbor" provision for ESI. "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide ESI lost as a result of the routine, good-faith operation of an electronic information system." But, does Rule 37 still apply if a party destroys ESI during litigation but before the court enters a discovery order? In a recent Nevada case, a plaintiff, during litigation and after defendant requested production of ESI, reformatted two hard drives due to alleged infection by virus and spyware.[7] Plaintiff failed to notify the defendant of the virus and his intent to reformat the hard drives, and failed to preserve an image copy and produce the backups showing all files had been restored. The court concluded that Rule 37 did not apply where a discovery order had not been entered, but that the court still had its inherent power to levy sanctions and issued an order requiring a jury instruction at trial in favor of defendant that plaintiff spoliated unfavorable evidence.

A Final Note

Lawyers and the courts are constantly required to interpret and apply the Federal Rules of Civil Procedure in an ever-changing technological environment. Ignorance of the rules and ESI is not an excuse and, more likely than not, will result in outcomes that are less than positive or favorable for the client or the attorney. Find out what you do not know – do not wait for a disaster to occur. Although there is certainly a "dark side" to e-discovery, there is also a "bright side." Think of how much more efficient and cost-effective discovery and trial preparation can be because of ESI and the technological advances we have experienced to date. It can, and will, only get better. NL

JOHN L. KRIEGER is a partner in Lewis and Roca LLP's intellectual property and technology practice group and concentrates his practice on intellectual property litigation in both state and federal court. Krieger formerly served as a lawyer representative to the Ninth Circuit Judicial Conference for the District of Nevada.

1 See *Mikron Indus., Inc. v. Hurd Windows & Doors, Inc.*, No. C07-532RSL, 2008 U.S. Dist. LEXIS 35166 (W.D. Wash. April 21, 2008) (denying motion for protective order because defendant failed to discharge meet and confer obligations in good faith regarding difficulty of producing ESI).

2 Duty to preserve relevant documents arises "[o]nce a party reasonably anticipates litigation." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). Courts in the Ninth Circuit have recognized that a party should "reasonably anticipate litigation" once a demand letter is sent. *See, e.g., Housing Rights Center v. Sterling*, No. CV 03-859 DSF, 2005 WL 3320739 *2 (C.D. Cal. Mar. 2, 2005).

3 *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1067 (N.D. Cal. 2006).

4 *In re Napster*, 462 F. Supp. 2d at 1070-1078 (assessing applicability of several options for sanctions for failure to institute litigation hold).

5 *Coburn v. PN II, Inc.*, No. 2:07-cv-00662-KJD-LRL, 2008 WL 879746 (D. Nev. March 28, 2008) quoting *Wagner v. Dryvitt Sys.*, 208 F.R.D. 606, 609-10 (D. Neb. 2001).

6 No. 05CV1958-RMB (BLM), 2008 U.S. Dist. LEXIS 911 (S.D. Cal. January 7, 2008). Overturned in part *Qualcomm Incorporated v. Broadcom Corp.*, 88 U.S.P.Q.2d 1169 (S.D. Cal. 2008).

7 *Johnson v. Wells Fargo Home Mortgage, Inc.*, No. 3:05-CV-0321-RAM, 2008 WL 2142219 (D. Nev. May 16, 2008). *But see Leon v. IDX Sys. Corp.*, 464 F.3d 951 (9th Cir. 2006) (upholding district court order dismissing plaintiff's case because plaintiff deleted 2,200 files from a company-issued laptop during the course of litigation).