Piecing together the e-discovery plan

E-discovery is challenging, but it needn't—and shouldn't—be complicated by a battle-zone mentality. Take advantage of the meet-and-confer process to ensure that your opponents know what electronically stored information they have and how they should produce it.

CRAIG BALL

Everyone wants e-discovery to be simple. The defendant's tech guru wants it to be simple because he's got too much to do. The defendant's in-house counsel wants it to be simple because she's got budget issues and thinks most claims are frivolous. Outside counsel wants it to be simple because he likes doing things the way he's always done them and doesn't like looking clueless about electronic information.

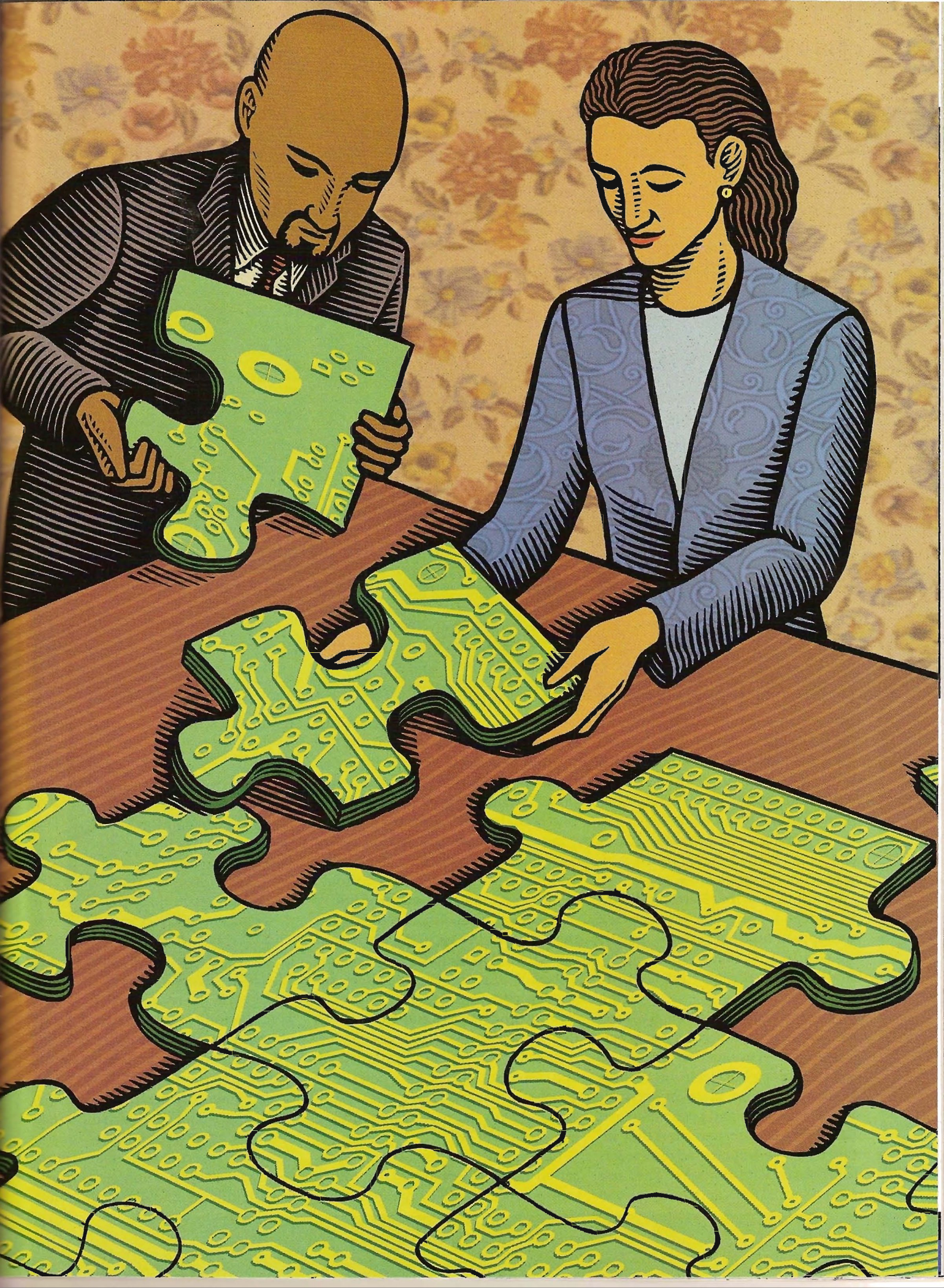
And you want it to be simple because you *need* it to be simple. Hiring experts and e-discovery vendors raises the stakes, and a misstep may result in significant cost-shifting to your client. Moreover, if you don't ask the right questions, you're not going to get the right information—and aren't courts starting to sanction lawyers for e-discovery foul-ups?

The problem is, e-discovery is *not* simple. It's complex, technical, and tricky. There are no shortcuts—no form, checklist, or script that's going to get the defendant to find the relevant information and turn it over in a reasonably usable way.

Face it: You've got to fight to get electronic evidence. You have to know what the defendant has, what you need, and how to ask for it. You must understand the capabilities and limitations of electronic search and the forms of produc-

CRAIG BALL *of Austin, Texas, serves as a special master in electronically stored information and a consultant on computer forensics and electronic discovery.*

GREGORY NEMEC



tion best suited to the evidence.

In 2006, Federal Rule of Civil Procedure 26(f) was amended to require parties to confer about preserving discoverable information and to develop a proposed discovery plan addressing discovery of electronically stored information (ESI) and the form or forms in which it should be produced.[1] This conference, and the overall exchange of information about electronic discovery, is called "meet and confer."[2]

Tell your opponents what you seek, plainly and clearly. They may show up empty-handed, but not because you failed to set the agenda.

The states are rapidly adopting rules of procedure and local practice like the Rule 26(f) provision for meet-and-confer;[3] but even in states without such a rule, judges often find the federal e-discovery model instructive and grant motions to compel parties to confer on ESI issues.[4]

In preparing for meet-and-confer, remember that it is more of a process than an event. Lay the foundation for a productive experience by communicating your expectations to opposing counsel.

Send a letter a week or two before each conference identifying the issues you expect to cover and sharing the questions you plan to ask. If you want client, technical, or vendor representatives to attend, say so. If you're bringing a technical or vendor representative, say so.

A cardinal rule for electronic discovery, indeed for any discovery, is to tell your opponents what you seek, plainly and clearly. They may show up empty-handed, but not because you failed to set the agenda.

The early, extensive attention to electronic evidence in discovery may perplex lawyers accustomed to the pace of paper discovery, but electronic records are now ubiquitous. Electronic records are more dynamic and perishable than their paper counterparts and they involve more voluminous and diverse formats than paper documents. They also require special tools and techniques to locate and process. These differences necessitate immediate action and unfamiliar costs. And courts harshly judge those who shirk their electronic evidence obligations.

Don't forget that e-discovery duties are reciprocal. Even if your client has little electronic evidence, you must nonetheless act to preserve and produce it. At the meet-and-confer session, be prepared to answer many of the same questions you'll pose.

Questions for meet-and-confer

The following questions address the types of matters you should discuss at a meet-and-confer session. These queries are neither exhaustive nor tailored to any unique issues. They're offered as talking points to stimulate discussion, not as a rigid agenda, and certainly not as a form for discovery.

What's the case about and who are the key players? Relevance remains the polestar for discovery, no matter what form the evidence takes. The scope of preservation and production should reflect both claims and defenses. Pleadings only convey so much. Be sure the defendant understands your theory of the case and the issues that you believe should guide its retention and search of ESI.

Cases are still about people and what they did or didn't say or do. Begin your quest for ESI by identifying the people whose conduct is at issue. These key players are the custodians of ESI, so determine what devices and applications they use and target their relevant electronic documents, application data, and communications. Also, determine whether assistants or secretaries served as proxies for key players in handling e-mail or other ESI.

Like so much in e-discovery, identification of key players should be a collaborative process, with the parties sharing the information needed to make informed choices.

What events and intervals are relevant? The sheer volume of ESI necessitates seeking sensible ways to isolate relevant information. Because the creation, modification, and access dates of electronic documents tend to be tracked, focusing on time periods and particular events helps identify relevant ESI, but only if you understand what the dates signify and when you can or can't rely on them. When a document was created doesn't necessarily equate to when it was written, nor does "accessed" always mean "used." For ESI, the "last modified" date tends to be the most reliable.

When does the duty to preserve ESI begin and end? The parties should seek common ground concerning when the preservation duty attached and whether it is ongoing. The duty to preserve documents generally begins with an expectation of litigation, and the facts and issues of the case dictate whether there is an ongoing obligation to preserve.[5]

Sometimes, events like plant explosions or corporate implosions define the endpoint for preservation, whereas a continuing tort or loss may require periodic preservation for months or years after the suit is filed. Even when a defendant's preservation duty is fixed, the plaintiff's ongoing damages may require ongoing preservation.

What data is at greatest risk of alteration or destruction? ESI is both tenacious and fragile: It's hard to obliterate but easy to corrupt. Focus first on fragile data, like backup tapes slated for reuse or e-mail subject to automatic deletion, and ensure their preservation. Address the rotation intervals of backup tapes, the disposal of legacy systems (that is, obsolete systems headed for the junk heap), the reassignment of computers among employees, and the replacement of aging hardware.

What nonparties hold information that must be preserved? ESI may reside on computers that are in the possession of the defendant's former employees, attorneys, agents, accountants, outside directors, Internet service providers, contractors, application service providers, family members, and other non-

parties. Some may retain copies of information the defendant discarded. If you don't mention these sources, the defendant may focus on its own data stores and fail to take steps to preserve data held by others over whom it has some right of direction or control.

What data requires forensically sound preservation? "Forensically sound" preservation of electronic media saves, in a reliable and authenticable manner, an exact copy of all active and residual data, including remnants of deleted data residing in unallocated clusters and slack space. When there are issues of data loss, destruction, alteration, or theft, or when a computer is an instrumentality of loss or injury, computer forensics and attendantspecialized preservation techniques are required. Skilled forensic examination is expensive, but off-site, forensically sound preservation can cost less than $500 per system.

What metadata is relevant, and how will it be preserved, extracted, and produced? Metadata is evidence, typically stored electronically, that describes the characteristics, origins, use, and validity of electronic documents.

Some metadata is crucial evidence and some is just digital clutter. You need to consider what kinds of metadata exist, where it resides, and whether it's potentially relevant so that it must be preserved and produced. Understanding the difference—knowing what metadata exists and what evidentiary significance it holds—is an essential skill for attorneys dealing with electronic discovery.

The most important distinction is between application metadata and system metadata. Application metadata is used by a software program like Microsoft Word to embed tracked changes and commentary in documents. Unless redacted, this data accompanies native production (that is, production in the form in which a file was created, used, and stored by its associated application). With the production of images, you'll need to ensure that application metadata is made visible before imaging.

System metadata is information like a

States weigh e-discovery rules

Electronic discovery is much more prevalent in some state courts than others. E-discovery amendments to the Federal Rules of Civil Procedure went into effect in 2006, and since then, many states have amended or considered amending their own rules.

But do states need new rules specific to electronic discovery? Some lawyers say no, because e-discovery disputes are not significantly different from traditional discovery disputes, and existing state rules of civil procedure are sufficient. Because the types of cases on the docket in federal courts and state courts vary, they say, the rules might make sense in federal court but not in every state court.

"There's a place for this in certain courts with certain cases, but to say this kind of rule is needed in the tens of thousands of state trial courts throughout this country is just patently ridiculous," said Marc Silverman, a Bellevue, Washington, lawyer, who chairs a court rules committee for the Washington State Trial Lawyers Association.

About 15 states have changed their e-discovery rules in some way, and about a dozen more, including Washington, are considering it. Some lawyers are concerned that applying the federal rules in state courts across the board would unnecessarily complicate litigation, requiring expensive forensic experts even in simple cases.

"The defense bar is pushing hard" for federal-style e-discovery rules, which would make litigation harder for plaintiffs and for small players in general, said John Vail, vice president of the Center for Constitutional Litigation in Washington, D.C.

"The plaintiff knows only what happened to him or her, not why, and is trying to find out why from the employer or insurer," Silverman said. These defendants "can set up roadblocks to make it a difficult, expensive process," and adopting the federal rules would leave the plaintiff with expenses that are prohibitive. "The person just won't be able to bring a case," he said.

To help judges make informed decisions about e-discovery, the Conference of Chief Justices in 2006 issued Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information. The conference stated that the guidelines "should not be treated as model rules that can simply be plugged into a state's procedural scheme."

The drafters noted that although the guidelines "acknowledge the benefits of uniformity and are largely consistent with the revised federal rules, they also recognize that the final determination of what procedural and evidentiary rules should govern questions in state court proceedings . . . [is] the responsibility of each state, based upon its legal tradition, experience, and process."

In February, the American Bar Association's House of Delegates approved the Uniform Rules Relating to Discovery of Electronically Stored Information, promulgated in 2007 by the National Conference of Commissioners of Uniform State Laws. They are substantially similar to the federal rules and are made for the states to adopt as law.

In Arkansas, another state considering changes, e-discovery is a new issue, said David Williams, a Little Rock lawyer and a member of a task force that has proposed model rules. Typically, in Arkansas courts, "the disputes don't lend themselves to electronic discovery, and state court judges would simply be overwhelmed if all of a sudden they're asked to implement a rule, while some judges have not yet had an opportunity to get up to speed on electronic data," he said.

The task force started with the Uniform Rules and proposed changes to address concerns about their application in Arkansas courts, Williams explained. Those concerns include whether the bar and the courts have enough experience with e-discovery to predict how

file's name, size, location, and modification date that a computer's file system uses to track and deploy stored data. Unlike application metadata, computers store system metadata outside the file. It's information essential to searching and sorting voluminous data, and therefore it should be routinely preserved and produced.

Try to get your opponent to agree on the metadata fields to be preserved and produced, and be sure your opponent understands the ways in which improper examination and collection methods corrupt metadata values. Also discuss how the parties will approach the redaction of metadata holding privileged content.

changes will play out; whether the meet-and-confer rule would apply automatically to every case, or only after a party signals the need for it; and whether the new rules should supplement the Arkansas Rules of Civil Procedure, or the other way around.

Adopting the federal rules wholesale "would create more difficulty for both sides" in litigation, Williams said.

In effect, he said, "we put a set of electronic-discovery training wheels on the Arkansas Rules of Civil Procedure." The Arkansas Bar Association is now considering the proposed rules.

In Washington, "there is not a scintilla of evidence that this is a problem," Silverman said. "Would it be so terrible for the plaintiff and defendant to sit down and craft a discovery plan that deals with this when you have the appropriate case?"

Silverman attended an April rules committee meeting of the Washington State Bar Association as a stakeholder—along with judges and access-to-justice groups—to discuss possible changes. Attendees expressed "considerable opinion that there's no emergency—and that awaiting further experience with the federal system makes complete sense," he said. ■

—Allison Torres Burtka

What are the defendant's data-retention policies and practices? A retention policy might fairly be called a destruction plan, and there's always a gap—sometimes a chasm—between an ESI retention policy and reality. The more onerous the defendant's purge policy, the greater the ingenuity its employees will use to evade it in order to hang on to their e-mail and documents. Consequently, you shouldn't trust the defendant's statement that ESI doesn't exist because its policy says it should be gone.

Moreover, even companies that are diligent about rotating their backup tapes and that regularly overwrite old contents with new may retain complete sets of backup tapes at regular intervals. They also may fail to discard obsolete tape formats when they adopt newer formats.

To meet its discovery obligations, the defendant may need to modify or suspend certain data-retention practices. Discuss what it is doing and whether it will, as needed, agree to pull tapes from rotation or modify purge settings.

Are there legacy systems to be addressed? Like backup tapes, old computers and servers tend to stick around even if they've fallen off the defendant's radar. Discuss whether potentially relevant legacy systems exist and how they will be identified and processed. You may also need to address what happens when a key custodian departs. Will the system be reassigned, and if so, what steps will be taken to preserve potentially relevant ESI?

What are the current and prior e-mail applications? An e-mail system is Grand Central Station for ESI. Understanding a defendant's current e-mail system and other systems used in the relevant past is key to understanding where evidence resides and how it can be identified and preserved.[6]

How will voice mail, instant messaging, and other challenging ESI be handled? Producing parties routinely ignore short-lived electronic evidence like voice mail and instant messaging (IM) by acting too late to preserve it or deciding that the retention burden outweighs any benefit. Though it's not especially challenging to preserve voice mail or IM logs, the defendant may demand that you identify a particularized need before doing so.

What relevant databases exist and how will their contents be discovered? From research and development to human resources, from finance to the factory floor, businesses run on databases. When databases hold relevant evidence, you'll need to know the platform (for example, SQL, Oracle, SAP, or Documentum) and how the data is structured before proposing sensible ways to preserve and produce it.

Because databases are always changing, ask, "Does the database ESI have a concrete beginning or ending date, or is it a 'rolling' database where data is added and deleted on a continuous basis?"[7] Database discovery is challenging and contentious, so know what you need and articulate why and how you need it. Be prepared to propose reasonable solutions that won't unduly disrupt the defendant's operations.

Are there attorney-client privilege issues unique to ESI? Discussing privilege entails more than just agreeing to return privileged items that slip through the net. It's important to address practices that overreach.

If your opponent uses keywords to sidetrack potentially privileged ESI, consider whether the search terms it used were absurdly overbroad. For example, simply because a document has the word "law" or "legal" in it or was copied to someone in the legal department doesn't justify the defendant labeling it as privileged.

The attorney-client privilege should be narrowly construed to protect either genuinely confidential communications exchanged for the purpose of seeking or receiving legal counsel or counsel's thinking and strategy. Moreover, even documents with privileged content may contain nonprivileged material that should be parsed and produced.[8]

What search techniques will be used to identify responsive or privileged ESI? Opposing counsel may resist sharing the details of the automated search and filtering system they use to identify or exclude information, characterizing it as privileged work product. Certainly,

the terms and techniques facilitating an attorney's assessment of a case are protected, but the search and filtering mechanisms that effectively eliminate the exercise of attorney judgment by excluding data as irrelevant should be disclosed so that they may be tested and, if flawed, challenged. Redaction may be appropriate to shield searches tending to reveal privileged information.

Can the parties agree on keywords for searching? If you've been to Las Vegas, you know keno, the game where you pick the numbers: If enough of your picks light up on the board, you win. Keyword searching of ESI is like that. Opposing counsel has you pick keywords and then goes off somewhere to run them through the data. Later, he tells you he looked through the matches and, sorry, you didn't win. As a consolation prize, though, you may get a million jumbled images of nonsearchable nonsense.

Perhaps because keyword searching performs so well in online legal research, lawyers and judges have a lot of confidence in it. That confidence is misplaced, thanks to misspellings, acronyms, synonyms, IM-speak, noise words, optical character recognition (OCR) errors, and the peculiar "insider" lingo of colleagues, companies, and industries. Despite the fact that, in reality, keyword searching performs far below most lawyers' expectations, finding perhaps only 20 percent of responsive material on first pass,[9] keyword searching remains the most common method employed to tackle large volumes of ESI.

Keyword searches are invariably more effective when employed in an iterative way, as part of a cooperative and informed process.[10] So, never allow opposing counsel to position keyword search as a single shot in the dark. You must be afforded the opportunity to use information gleaned from the first or subsequent efforts to narrow and target succeeding searches.

Use the early searches to acquaint yourself with the argot of the case. Then ask, for example: What shorthand references and acronyms should be used in the search? Should products be searched by their trade or technical names?

How will duplicate data be handled? ESI, especially e-mail, is characterized by enormous repetition. A message may appear in the mailboxes of thousands of custodians or be replicated dozens or hundreds of times through periodic backup. De-duplication is the process by which identical items are reduced to a single instance for purposes of review. De-duplication can be vertical, meaning the elimination of duplicates within a single custodian's collection, or horizontal, where identical items of multiple custodians are reduced to single instances.

Candor and cooperation in e-discovery aren't signs of weakness but rather hallmarks of professionalism.

If production will be made on a custodial basis—and depending on the review platform employed—it may be desirable to request re-population, or replacing, of content that was de-duplicated horizontally so that each custodian's collection is complete.

What forms of production are offered or sought? Notably, the 2006 amendments to the federal rules gave requesting parties the right to designate the form or forms in which ESI must be produced. A responding party may object to the designated form or forms, but if the parties don't subsequently agree and the court doesn't order the use of particular forms, the responding party must produce ESI as it is ordinarily maintained or in a form that is reasonably usable.[11]

Moreover, responding parties may not simply dump ESI in the form of their choice on the requesting party. Instead, they must disclose which forms they intend to use so the requesting party may ask the court to compel production in another form.[12]

Options for forms of production include native file format; quasi-native forms, such as a partial export of data from a database; imaged production, such as portable document format (PDF) or, more commonly, tagged image file format (TIFF) images that are accompanied by files that contain searchable text and metadata; hosted (online) production; and paper printouts for small collections.

It is unnecessary—and rarely advisable—to employ a single form of production for all items. Instead, tailor the form to the data in a hybrid production.

If you are uncertain of what ESI you need to request, you'll play into opposing counsel's hands. You must be able to articulate both what you seek and the form in which you seek it. And, before asking for production, know how you'll house, review, and use the ESI. That means you must "know your review platform." That is, know the needs and capabilities of the applications or tools you'll employ to index, sort, search, and access electronic evidence.[13]

How will you handle the redaction of privileged, irrelevant, or confidential content? Defendants often seek to redact ESI in the way they once redacted paper documents: by blacking out text. To make that possible, ESI is converted to nonsearchable TIFF images in a process that destroys electronic searchability. So after redaction, electronic searchability must be restored by using OCR to extract text from the TIFF image.

A TIFF-OCR redaction method works reasonably well for text documents, but it fails miserably when applied to complex and dynamic documents like spreadsheets and databases. The inevitable errors introduced by OCR make it impossible to have confidence in numeric content or reliably search the data. In addition, converting a spreadsheet to a TIFF image strips away its essential functionality by jettisoning the underlying formula that distinguishes a spreadsheet from a table.

For common productivity applications like Adobe Acrobat and Microsoft Office, it's now feasible and cost-effective to redact natively so as to preserve

the integrity and searchability of evidence. Consequently, where it's important to preserve the integrity and searchability of redacted documents, you should determine what redaction methods are contemplated and seek agreement on methods best suited to the task.

What ESI will be considered not reasonably accessible? Under federal Rule 26(b)(2)(B), a litigant must show good cause to discover ESI that is "not reasonably accessible," but the burden of proving a claim of inaccessibility lies with the party resisting discovery. So it's important for the defendant to identify the ESI it claims is not reasonably accessible and furnish sufficient information to let you gauge the claim's merit.

The meet-and-confer session is an opportune time to resolve inaccessibility claims without court intervention—to work out sampling protocols, cost-sharing, and filtering strategies—or, when agreements can't be reached, to at least secure commitments that the disputed data will be preserved long enough to permit the court to resolve issues.

Transparency and collaboration

Courts and commentators uniformly cite the necessity for transparency and collaboration in electronic discovery, but old habits die hard. Too many defendants treat meet-and-confer as a perfunctory exercise and are reluctant to offer a peek behind the curtain.

Some defendants pay dearly for their intransigence, either through sanctions for obstructive conduct or through the extra cost to find data that might never have been sought had there been communication and candor.[14] Others have begun to understand that candor and cooperation in e-discovery aren't signs of weakness but rather hallmarks of professionalism.

The cost and complexity of e-discovery will diminish as electronic records management improves and ESI procedures become standardized, but the meet-and-confer process is likely to endure and grow within federal and state procedure. Accordingly, learning to navigate meet-and-confer—to consistently ask the right questions and be ready with the right answers—is an essential advocacy skill. ■

Notes

1. The Rule 26(f) conference must occur "as soon as practicable—and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b)." Fed. R. Civ. P. 26(f)(1).

2. *Hopson v. Mayor of Baltimore*, 232 F.R.D. 228, 245 (D. Md. 2005), details some of counsel's duties under Fed. R. Civ. P. 26(f).

3. Noted e-discovery commentator Thomas Allman, who was a founding member of the Sedona Conference and co-chair of the E-Discovery Committee of Lawyers for Civil Justice, reports that seven states have adopted e-discovery rules hewing closely to the federal rules (Arizona, Indiana, Louisiana, Minnesota, Montana, New Jersey, and Utah); another 14 states are considering changes to their court rules to address e-discovery. *See* Brett Burney, *Mining E-Discovery Stateside*, L. Tech. News (Jan. 18, 2008), www.law.com/

jsp/legaltechnology/pubArticleLT.jsp?id=1200594602161.

4. *See e.g.* Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* §3 (2006), www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf (a judge should "encourage" counsel to meet and confer in an effort to agree on e-discovery issues and to exchange information).

5. *See* Craig Ball, *The Perfect Preservation Letter*, TRIAL 28 (Apr. 2007), www.justice.org/publications/trial/0704/ball.aspx.

6. A changeover to a new e-mail system or to a new e-mail client server may result in a large volume of "orphaned" e-mail that the defendant may fail to search. Also, if employees' personal e-mail accounts and home or laptop computers are involved, the parties should agree on how to preserve and produce that data.

7. Michael R. Arkfeld, *Arkfeld on Electronic Discovery and Evidence* (2d ed., LexisNexis 2007).

8. *See e.g. Muro v. Target Corp.*, 243 F.R.D. 301, 306-07 (N.D. Ill. 2007); *In re Vioxx Prods. Liab. Litig.*, 501 F. Supp. 2d 789, 799 (E.D. La. 2007).

9. *See e.g.* The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, The Sedona Conf. J. 189, 199 (Fall 2007), www.thesedonaconference.org.

10. *See e.g.* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?*, 13 Rich. J.L. & Tech. 10 (2006), http://law.richmond.edu/jolt/v13i3/article10.pdf; *see also* The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, cmt. 11.a (2d ed. 2007), www.thesedonaconference.org.

11. Fed. R. Civ. P. 34(b).

12. *Id.*

13. Knowing your intended platform allows you to designate proper load file formats and determine if you can handle native production. Choosing the right review platform for your practice requires understanding your work flow, your people, the way you'll search ESI, and the forms in which the ESI will be produced. There are many review platforms on the market, including the familiar Concordance and Summation applications, Internet-accessible hosted review environments, and proprietary platforms.

14. Courts have sanctioned various types of ESI discovery abuse. *See e.g. Finley v. Hartford Life & Accident Ins. Co.*, 2008 WL 509084 at *3 (N.D. Cal. Feb. 22, 2008) (negligence); *Qualcomm, Inc. v. Broadcom Corp.*, 2008 WL 66932 at *9-10 (S.D. Cal. Jan. 7, 2008) (intentional deception); *In re Seroquel Prods. Liab. Litig.*, 244 F.R.D. 650, 661 (M.D. Fla. 2007) (purposeful sluggishness); *Phoenix Four, Inc. v. Strategic Resources Corp.*, 2006 WL 1409413 at *6 (S.D.N.Y. May 23, 2006) (gross negligence); *United Med. Supply Co. v. U.S.*, 77 Fed. Cl. 257, 274 (2007) (reckless disregard). Increasingly, courts regard the duty to preserve and produce ESI as one shared by client and counsel and refuse to accept ignorance on either's part as an excuse. *See e.g. Qualcomm Inc.*, 2008 WL 66932 at *9; *Phoenix Four, Inc.*, 2006 WL 1409413 at *6.