Navigating the Changing Landscape of E-Discovery

A Roundtable Discussion

Top row, from left: Paul Weiner, Frank Conley, Stephanie A. "Tess" Blair, Michael Adler. Bottom row, from left: Mark Sidoti, Gerry Boccuti, Karen Schuler

Michael Adler, Moderator, Hotwire Communications
Stephanie A. "Tess" Blair, Morgan Lewis & Bockius, LLP
Gerry Boccuti, Wyeth Pharmaceuticals
Frank Conley, Littler Mendelson, P.C.
Karen Schuler, Onsite[3] E-Discovery
Mark Sidoti, Gibbons, P.C.
Paul Weiner, Buchanan Ingersoll & Rooney, P.C.

MR. ADLER: I'm very pleased to be here this morning to serve as the moderator for this roundtable discussion on electronic discovery. Our goal today is to provide our readers with information about the latest trends in e-discovery, and to address some of the challenges it presents. We will provide practical insight for corporate counsel as well as plaintiffs' and defense attorneys. Our topics of discussion will include recent e-discovery amendments to the Federal Rules of Civil Procedure, litigation preparation and response strategies, document retention, technology and litigation support teams and the costs of e-discovery.

E-DISCOVERY AND THE FEDERAL RULES OF CIVIL PROCEDURE

MR. ADLER: Our first topic of discussion is how the Federal Rules of Civil Procedure have changed to address e-discovery issues. Tess, what recent changes have we seen in the federal rules?

MS. BLAIR: Effective Dec. 1, 2006, the rules were amended to accommodate electronic discovery. Prior to that time, the rules as a practical matter did accommodate e-discovery, but now they are explicit with respect to this process. The most fundamental change is the appearance of a new term, "electronically stored information," or what those of us in the business call "ESI." The new rules explicitly state that ESI is discoverable.

MR. ADLER: Mark, hasn't ESI always been discoverable?

MR. SIDOTI: Clients and many practitioners do believe that e-discovery is something new. But that is a misconception. Electronic information has always been discoverable under the federal rules. It's just more prevalent today than it was in the past. The amended rules now reflect that we often encounter electronic information during litigation.

MR. ADLER: Paul, why were the new rules needed? Was there a committee that reviewed this? And if so, what did they decide?

MR. WEINER: I think the approach to the new rules has brought to the forefront what was previously in the shadows. That is, everyone was always dealing with electronic discovery, but now it's more concrete. The rules now require people to address upfront basic matters such as how they will approach electronic discovery, how they will produce ESI and the interplay between e-discovery and the attorney-client privilege.

This E-Discovery Roundtable was produced and paid for by the participating law firms in cooperation with the advertising department of *GC Mid-Atlantic*. It was produced independent of the editorial staff of *GC Mid-Atlantic*.

In general, I think that companies need to have thought about their electronic data well in advance of the threat of litigation.
— FRANK CONLEY

Because ESI presents some unique challenges, a committee studied e-discovery for more than five years before the new rules went into effect. The three primary challenges that ESI presents are its dynamic characteristics, the fact that unlike words on paper, ESI may be unintelligible when separated from the system that created it and the sheer volume of electronic information that is out there. It has been estimated, for example, that 60 billion e-mails are generated every day. With this type of immense volume, producing relevant information will likely mean reviewing a much larger data set than you would review in a case that simply involves traditional paper discovery.

MR. CONLEY: And I think what is interesting about the rules and the timing of the rules is that a lot has changed from the time that we first saw the need to modify them to their actual implementation. E-discovery is a continuum. For example, Intel just announced a new product that is a super computer on a thumbnail-size chip. As you can see, the way that information is created and stored and delivered is going to change constantly. So while it's nice to think of these rules as addressing a problem that we currently have, like any of the other federal rules, they really provide more of a framework for handling ESI.

MR. WEINER: I think the rules have also brought some sanity to the process. There is now some business rationale to the process where obviously you have to get the electronic information, but it should not be at the expense of your business. Before, courts and litigants were literally asking for and sometimes getting everything. Now the courts and the parties themselves have a little bit of a framework to guide them and there are some real checks on the process. For example, the comments and the drafting history make it clear that we should look for active data first before going to things like backup tapes, which are usually created for disaster recovery purposes and not indexed or easily searchable.

MR. ADLER: Tess, Paul just referred to active data versus backup data. What's the difference between the two?

MS. BLAIR: Well, the new rules distinguish between information that is reasonably accessible and information that is not reasonably accessible. Parties are obligated to produce information that is reasonably accessible. That would be information that is used in the ordinary course of business and is easily obtained through active e-mail or through file or exchange servers, for example. Inaccessible data is characterized as information that is offline or in some sort of media that makes retrieval difficult. Backup tapes are the classic example of inaccessible data. Another example is "legacy data," which is information that was created or stored in a computer system that is no longer in use. While parties are obligated to disclose the existence of inaccessible data, they may object to its production.

MR. ADLER: Mark, under the new rules, at what point can the parties first discuss potential ESI problems?

MR. SIDOTI: Essentially, the first opportunity is whenever you make it. Under the new rules you need to have these discussions very early on, within the first 30 to 60 days after the lawsuit is filed. It is incumbent upon the parties to cooperate and do this as soon as possible.

MR. ADLER: Tess, the federal rules were amended on Dec. 1, but I'm wondering if we'll soon see some changes in the state courts. Will state courts begin to follow some of the new federal rules?

MS. BLAIR: The Conference of Chief Justices, which represents the top jurists in all 50 states, the District of Columbia and the U.S. territories, recently issued guidelines that look a lot like the federal rules. State courts are also adopting some of the fundamental principles that the federal courts follow. I'm not predicting that there's going to be uniformity across the country, but it's clear that the state and federal courts are going to handle electronic discovery in a similar fashion.

MR. ADLER: Gerry, how might having different rules in different jurisdictions affect a large multinational corporation like Wyeth?

MR. BOCCUTI: It does keep us on our toes. It seems as if most states are adopting the general principles espoused by the federal courts, but many of them do have their own nuances. A good example of this is in the area of waiver of privilege.

MR. ADLER: Shifting gears, it seems that with so much data it would be easy to mistakenly fail to produce all of the required discovery because you didn't know everything that existed, like backup data for example. Is there a provision in the new rules to account for this? Paul?

MR. WEINER: Actually, the new rules do not affect data preservation obligations. This is repeatedly stated throughout the rules and the comments. The rules are not meant to supplant common law duties of preservation. But the rules also repeatedly indicate that it is no longer appropriate to just walk in and have a general conversation with a member of your client's information technology staff. You really have to know your client's IT system. You need to ask your client where data is stored, how backups are generated, whether backup tapes are overwritten and what processes are in place to facilitate data searches. So I think that with the new framework – and particularly with the focus on knowing your client's specific system – more and more judges are going to find such failures inexcusable. I think that both parties and lawyers will face sanctions if they fail to adhere to the new framework.

MS. SCHULER: Do you think vendors will be affected as well? I've noticed that neither vendors nor consultants have necessarily had to account for missing documents or so-called missing evidence.

MR. WEINER: That's a great question, because one of the things that happened in the Morgan Stanley case a couple of years ago was that Morgan Stanley & Co. refused to use a neutral vendor to locate, gather and produce

its e-mails. In that case, *Coleman Holdings Inc. v. Morgan Stanley*, 892 So. 2d 496 (Fla.Ct.App. 2004), a Florida judge granted a partial default judgment against Morgan Stanley after the firm failed to turn over e-mails that had been stored on more than 1,000 backup tapes. So I actually counsel clients in certain situations to think about hiring a vendor upfront to get themselves the expertise, particularly with the early obligations specified in the rules. In *Morgan Stanley*, a vendor could have testified that it would have cost the company several million dollars to restore backup tapes. So I think it gives the party a chance to work with an expert and then the culpability is on the expert rather than the party.

MS. SCHULER: I agree. To avoid errors, I often schedule several planning and status meetings that bring together general and outside counsel and the vendors. The benefit of gathering all the parties around a table is that everyone comes to understand the overall processes, gaps, issues and potential risks involved with the relevant data.

MR. CONLEY: Using an outside vendor also addresses credibility concerns. Where you have complicated and easily modifiable electronic information and you're doing it in-house, you're creating witnesses with every IT person you use. There are privilege problems with conversations between your IT people and the executives who are calling the shots. It makes sense to avoid these problems by using a neutral vendor.

MS. BLAIR: I agree. Before this conversation started we were talking about some new tools that are designed to assist law firms and other companies with in-house discovery. I think there is a place for these tools, but you have to be concerned about instances where you're going to need to prove up your discovery efforts and you're going to need testimony and affidavits and so forth. In many cases, it's much better to have a disinterested third party who is willing to attest to how discovery was conducted.

MR. ADLER: Mark, if you do your best, is there any protection under the new safe harbor provision?

MR. SIDOTI: That's a very difficult question. I think the safe harbor provision is one of the most controversial aspects of the new rules. The question is, what constitutes good faith operation of electronic management systems? I think companies have the best chance of being protected when they do some of the preliminary work. Companies that maintain up-to-date document retention policies and actually follow them are far ahead of the curve. But I still think you have to be very careful with safe harbor because it is not as safe as people might think.

MR. BOCCUTI: I share that view. I think it is risky to formulate a discovery strategy around the safe harbor provision.

MR. CONLEY: Agreed. A consistent policy is better.

MR. ADLER: Frank, could you be more specific?

MR. CONLEY: Sure. A corporation should establish data destruction and retention policies before litigation is even on the horizon. The corporation should also ensure that the policies are consistently applied.

PREPARING FOR LITIGATION

MR. ADLER: Let's turn to litigation preparation. Tess, how can we make litigation more efficient for our clients?

Data sorting is a critical component for our clients because it is very difficult to identify meaningful trends within data.
— KAREN SCHULER

MS. BLAIR: Well, clients need to understand that they now have an obligation to make certain disclosures, and that they must be prepared to meet and confer with the opposing party. The client will need to arm the attorney with a lot of information before the complaint even hits the attorney's desk. It is important to understand that initial disclosure and scheduling conferences are usually 90 to 120 days out. For a large company, that is simply not enough time to prepare. It is very difficult to meet your obligations within that timeframe.

The client also needs to be able to articulate what its IT infrastructure looks like, where it's located, how it's stored, how it's managed and how it was created. Relevant data will also have to be inventoried and potentially problematic areas identified. These issues will need to be addressed with opposing counsel at the beginning of the matter.

MR. CONLEY: But the trick in a lot of that is that it's ongoing and you might hire new people or move to a new location, or allow someone to work part time and now that person is in and out of the office. Or you might buy a new computer system and wind up with different capabilities, and now you're storing data that you didn't have when you drafted your policy six months ago. It is therefore crucial to continually update your IT plan.

MS. BLAIR: To do address that concern, we create what we call an "IT map" for our clients. Legal and IT are in charge of the map because both have a significant interest in ensuring that it is up-to-date. Technology changes, people come and go, new systems are implemented and lots of things change over time. Your IT map thus needs to be regarded as a living document.

MR. ADLER: Karen, where else can you find data, other than someone's computer or hard drive? Where else would counsel and the IT department look for discoverable information?

MS. SCHULER: If you're identifying the complete environment of electronically stored information within an organization, you might consider the examination of not only hard drives, but also thumb drives, voicemail, DVD-ROMs, CD-ROMs, handheld devices and floppy drives. And as much as we'd all like to ignore paper records, we can't, so that is another consideration. In addition, organizations often address work-computer hard drives, but forget to mention that they allow their employees to work from home on home computers. Therefore, home computers have always been part of my line of ESI questioning. Of course an individual's privacy must always be considered when examining a home computer.

This long list of places to look more importantly leads to the question of managing electronic assets. If I'm an employee and I receive three different computers in one year, does the company know where to find my retired computers? Asset management is probably the biggest gap in the companies that I see. I've worked on many cases where the company says, "Oh, we only have 2,500 computers," but it turns out that there are an additional 4,000 computers that they no longer use. Or the company will allude to the fact that only 1,000 backup tapes exist for the relevant timeframe, when in reality it is closer to 7,000 tapes. For these reasons, ESI questionnaires are critical to ensure that you have accurate information during your planning sessions.

The rules now require people to address upfront basic matters such as how they will approach electronic discovery, how they will produce ESI and the interplay between e-discovery and the attorney-client privilege.
— PAUL WEINER

MS. BLAIR: And remember we're talking about this new term, "electronically stored information." The new rules have purposely left ESI undefined in order to accommodate emerging technology. So we're talking about instant messaging, metadata, systems data, login information, voicemail, video and anything else that's electronically stored.

MR. ADLER: Mark, Tess mentioned metadata. Can you briefly describe metadata and the dangers it presents?

MR. SIDOTI: Metadata is commonly described as the data behind a document. The best example is the information behind an e-mail that you send to a group of people, such as who was copied, when it was sent and when it was opened. The issue with metadata is that productions are sometimes made in what's called "native format," or the request is that production be made in native format, and that format is intended to produce not only the visual documents, but also the metadata. An interesting recent decision from the Eastern District in New York notes that parties that are routinely converting documents and thereby "losing" metadata before the documents are produced might be running afoul of the new rules. So they might, for example, convert a native file into a TIFF file and then produce it. This particular New York judge held that that procedure had potentially "degraded the searchability of the data," and therefore may have violated amended Federal Rule 34.

MR. WEINER: I'd like to mention an additional problem with metadata, which is the inadvertent production of information. We didn't talk about this when we discussed the rules, but there are actually reported cases in which a party did not understand what they were producing and as a result, through the metadata, actually waived the attorney-client privilege or produced some of the biggest smoking guns in their cases.

LITIGATION RESPONSE STRATEGIES

MR. ADLER: Now that we've talked about preparing for litigation, let's discuss responding to litigation. Frank, what kind of litigation response plan should a company have? How should you counsel your clients in terms of handling ESI as a defendant? Who should be on your team and what kinds of roles should these individuals play?

MR. CONLEY: In general, I think that companies need to have thought about their electronic data well in advance of the threat of litigation. They should know who their employees are and how they operate so that they have solid computer use and document retention policies in place. The problem I see in most cases is unanticipated data. You start a case and you think you know where it's going, but then something throws you for a loop. For instance, you might know that one of your employees took some confidential e-mails home, and so you focus on that. But then you find out the employee has a home computer and has deleted everything from it. Now the case is going to take a new turn. The lesson is that your game plan has to be flexible. You have to be prepared to respond to constantly changing information.

MR. ADLER: Gerry, if an in-house attorney wants to get started with a response plan, what other company personnel should be involved?

MR. BOCCUTI: That's a great question. A positive change I have seen is that companies are hiring people and creating positions to deal with e-discovery. This is preferable to overburdening existing personnel, such as paralegals and senior attorneys, who are already swamped. Companies and law firms are actually hiring e-discovery specialists and litigation support managers, or at least utilizing the services of an experienced law firm or vendor to provide these services. And I agree: companies have to be flexible. In some cases you're going to want to take a low-cost approach whereas in others, you're going to want to pull out all the stops and collect as much information as you can.

MR. ADLER: Mark, let's talk about litigation holds. What is a litigation hold and when would you anticipate putting one in place?

MR. SIDOTI: There are two kinds of litigation holds. One is an internal litigation hold, which a company sends out to its employees or other individuals who may have relevant information following a certain trigger. The other is an external litigation hold that we might send to an adversary's attorney. The external hold would describe certain documents that the opposing party should preserve.

I think the thing to remember about litigation holds is that they are living documents. They have to be created specifically for a particular case. That said, they can share certain fundamental elements. Litigation holds should always be issued by the same person in the company, such as general counsel or another high-ranking individual. They should clearly describe the data that needs to be preserved. And they should be simply worded. Tailoring the hold for the specific case will then become part of your litigation preparation. You should have a process in place such that, when a trigger hits, you will call in certain key people to formulate the hold for that circumstance.

Triggers, of course, are a whole separate discussion. Generally, if you knew or should have known that there was the potential for litigation, or for an investigation or audit, you should have acted accordingly to preserve the relevant documents. Many companies believe that only the filing of a lawsuit triggers a hold, but that is just not the case.

MR. WEINER: I think on Mark's point, one thing that is universally clear now in every jurisdiction is that it is the lawyer's duty to determine when the trigger occurs and to properly counsel the client regarding ESI preservation. It is not sufficient to simply call the IT department or your business contact and say, "We need to preserve information." It is now the lawyer's duty to actually understand the client's IT systems, to understand how relevant data and information are stored and purged from those systems, and to give concrete

advice about preservation.

MS. BLAIR: Readers should also note that a litigation hold alone is not sufficient to meet preservation obligations. There's a lot of monitoring that needs to take place. You need to interact with the IT department to identify any auto-purge functions that might undermine your preservation efforts, and you need to modify your legal hold as the case evolves.

MR. WEINER: Tess makes a good point: You have to monitor what your client is actually doing. It is not a matter of sending out the hold and a year later saying, "Where is the information?" You have to make sure that all of the relevant employees are complying with the hold.

MR. ADLER: Gerry, in-house legal serves a very important function before outside counsel is even retained. Could you comment on that?

MR. BOCCUTI: I take the view that we work together. When outside counsel goes in to interview employees, I make sure that they have a copy of the legal hold memorandum. The first thing they will do is talk about the employees' obligation to preserve documents and ensure that the employees understand the hold. One of the problems I've seen is where a corporation, because of the number and complexity of the hold orders, takes the view that it would be easiest to just hold onto everything.

MS. BLAIR: Which is good for vendors.

MS. SCHULER: You know, it is and it isn't, to be honest. It can cause just as many problems for us because data and records management are so critical when responding to a discovery request. The more information a company saves, the more complex the environment.

RECORDS RETENTION

MR. ADLER: Well, that leads into our next topic which is document retention. Tess, have the new e-discovery rules changed how companies approach document retention?

MS. BLAIR: No. Litigation should not drive records retention. Business should. An effective retention policy will reflect obligations imposed by applicable laws and regulations, as well as the business needs of the organization. E-discovery does, however, underscore the need for effective records management. The better organized you are, the more effectively you can respond to demands for ESI.

MR. BOCCUTI: Can I ask you all a question? When you are working with corporations, who typically owns the records management policy? What department or group is responsible for it?

MR. WEINER: That's a great question. Of course, first you're assuming that they have one.

MS. BLAIR: There is that.

MS. SCHULER: Or maybe they have one, but they never look at it.

MS. BLAIR: Or they wrote it in 1974.

MR. WEINER: More than you would think, very large corporations don't have them. So, number one, you have to have one. And then I think we're counseling people that it's a function of legal and IT working together. The IT people are in the business of maintaining your client's technology. They are not in the business of gathering documents and data for litigation. They are not in the business of deciding whether a certain backup policy needs to be halted because a litigation hold has been issued. Education is critical and that's where in-house lawyers and outside counsel can really work together.

> I think the safe harbor provision is one of the most controversial aspects of the new rules.
> **— MARK SIDOTI**

MR. CONLEY: Where I see document retention becoming problematic is in smaller companies. If you're a company that can afford to have an IT staff, that's great. But there are a lot of companies that cannot afford the extra employees, and the federal rules don't make any special allowances in that area. If you have electronic data, you have electronic data. I think it's really a challenge for smaller companies to figure out how they're going to manage their ESI.

MR. ADLER: Tess, should companies also have policies regarding document creation and mode of storage? Should there be limitations on using thumb drives and other technology?

MS. BLAIR: Yes. There should be policies that address appropriate computer use. Companies need to implement policies that dictate where it is and is not appropriate to store records. Personally, I believe the fewer archives you have, the better. For example, when I'm doing an assessment for a client, I ask them where their employees are permitted to store e-mails. I often find out that they store e-mails on the company server, on home computers, on their hard drives, on CDs, on thumb drives, on PDAs. Data is everywhere. And obviously you have an obligation to do your due diligence and look at all of those possible sources. And that just increases the volume of data and the cost and challenge of the investigation. So I am not a fan of local archiving.

MR. CONLEY: A big problem that a lot of plaintiffs are having fun with is Web-mail forwarding. A lot of employees don't want to take their work computers home, so they forward all of their business e-mails to their personal accounts. Suddenly a company's e-mail protections become meaningless.

MR. ADLER: Karen, are you similarly finding specific dangers with instant messaging in companies?

MS. SCHULER: Yes. Instant messaging is a dynamic type of communication, similar to the telephone, and depending on the type of IM software that is used activities may or may not be monitored. In companies where IM activities are monitored or logged, I think it is important to communicate this to the end-user who could potentially be a custodian.

MR. ADLER: Paul, what about ensuring that your opponent preserves their records?

> The most fundamental change is the appearance of a new term, "electronically stored information," or what those of us in the business call "ESI." The new rules explicitly state that ESI is discoverable.
> **— TESS BLAIR**

MR. WEINER: You can accomplish that with a preservation letter, particularly if you are representing the plaintiff. The plaintiff would send the preservation letter out with the complaint, subpoena or writ. The very first thing that goes out the door, a preservation letter goes with it.

MR. ADLER: What would be in that preservation letter?

MR. WEINER: You would advise the other party as to what their obligations are and what they need to preserve. Some people say that's redundant because the obligation is already stated in the rules and exists in the common law. But in reality, preservation letters can be incredibly helpful. We just had a case in which one of the main custodians on the other side died, unfortunately, and we sent a letter expressing our sympathy and asking the company to be sure to preserve the individual's computer. Many months after the fact we learned that someone had deleted information from that computer. Clearly the other side had an obligation not to do that, but the letter proved very beneficial because the court said, "OK, the obligation was there and you got a letter that asked you to preserve this computer. How in the world did you allow this to happen?"

MS. BLAIR: Paul makes a great point. But on the flip side, I have had clients receive massive preservation requests that would have necessitated shutting down their operations. So a well-defined preservation request is going to be much more useful than a blanket letter to which a party cannot possibly adhere. Depending on its tone and breadth, a letter either will or will not prompt a cooperative dialogue.

MR. ADLER: When is it appropriate to send the initial preservation letter? Is it after litigation starts or would you recommend sending it before you are certain there's going to be litigation?

MR. WEINER: I would say the earlier the better.

MR. CONLEY: I think Tess will hate me for this, but I have a more extreme view than Paul does. Depending on the claim, we often file an emergency motion for a preservation order when we file the complaint.

MS. BLAIR: You're right, Frank. I would hate you for that.

MR. WEINER: I would point out that while there are some situations where that is appropriate, the drafting history and the commentary to the new rules specifically address this issue. In particular, they dissuade courts from routinely entering preservation orders and further state that ex parte preservation orders should only be entered in exceptional circumstances.

MR. CONLEY: Again, it depends on the claim.

MS. BLAIR: I think protective orders are only appropriate when there is some real danger of losing data.

MR. CONLEY: Right. In the trade secret cases it's pretty important to seek a protective order because you have employees on the road or you have people working from home and if you don't have an order like that in place, people will start deleting data.

MS. SCHULER: And to add to Mr. Conley's point, it is common in those types of cases for our teams to forensically restore data that has been deleted and partially overwritten.

MR. CONLEY: I had a case last year where we had to recover data that way after a defendant was informed of a protective order and immediately started deleting files from his computer.

MS. BLAIR: There are consequences for that type of behavior, though. That's highly unusual.

MR. CONLEY: It's the nature of the claim. You can't do it routinely, but when you have a concern about the nature of the information, especially in trade secret matters, it's very important to have that kind of authority from the court above and beyond what the rules provide.

MR. ADLER: Shifting gears a bit, what should companies do with old computers that are no longer in use?

MS. BLAIR: Throw them away. If the data on the computers is not subject to a retention policy and is not being preserved for litigation purposes, you get rid of them.

MR. CONLEY: Of course before you destroy a computer, you should erase its contents.

MS. SCHULER: Oh, most definitely. Destruction should mean destruction.

MR. ADLER: Can anything really be wiped clean, Karen?

MS. SCHULER: Yes, believe it or not. If you have a standard within the IT department that allows you to wipe hard drives via U.S. Department of Defense standards, it is possible to completely erase a computer's contents. However, if the individual performing the wiping task is impatient and doesn't complete the job, often we will locate text fragments on the hard drive. And I've seen instances where those text fragments were potential smoking guns.

MR. ADLER: We talked about preserving and storing data, now let's say you have a discovery request. Karen, how do you sort through your data in an efficient manner?

MS. SCHULER: Data sorting is a critical component for our clients because it is very difficult to identify meaningful trends within data. We are therefore constantly seeking new means of data sorting, creating software tools to efficiently sift through data, creating algorithms to filter out data and working on sampling techniques. The sampling techniques, in my opinion, are a widely

overlooked aspect of e-discovery. If we establish a statistically significant sample, then we should be able to obtain a reasonable idea of the likelihood of finding relevant evidence. However, as a standard practice, our company regularly assists our clients with running keyword searches to identify unrelated or potentially responsive information.

MR. ADLER: Mark, do you have any additional suggestions?

MR. SIDOTI: I think the first step is to start a dialogue with the opposing side. You might be surprised at what your adversary is willing to leave out because there is not much use for it. You can also caution them that if they insist on production of every single hard drive image, it may end up costing them several million dollars because much of the production would unnecessary and you would seek to shift the search and production costs.

MR. BOCCUTI: I'd like to ask about search terms. Are they privileged work product?

MR. CONLEY: Yes.

MR. WEINER: I would say it depends. The way I sometimes approach it is through the dialogue with the opposing side. I'll indicate what I'm using and they might come back and say they believe I should be using something else. But if you are using the terms to facilitate your own data collection, I would say that those constitute work product.

MR. CONLEY: If it's your expert, that's work product. But if it's part of discovery, I don't think it is.

MR. BOCCUTI: So should that be part of the meet-and-confer dialogue?

MR. WEINER: Absolutely.

MS. BLAIR: But you may want to do some work in advance and that is where I think the work product comes in. Keywords used to test for over-inclusiveness, for example, would be work product.

MR. WEINER: Litigants should also note that sampling can be used offensively. I've had situations where we did a sample run and used the results to support a cost-shifting argument or to argue in favor of narrowing a discovery request. That's where it's useful to have an expert to say, "We did a sample run on five key custodians, searching only their personal share drive accounts and it took 100 hours, cost $35,000 and produced the equivalent of 10,000 pages of documents. To run it on the entire system would cost in excess of $5 million, so unless you are going to pay for it now or narrow your request, it's off the table."

PRIVILEGE REVIEW

MR. ADLER: Our next topic is privilege review. How can litigants review their ESI for privileged information before producing it?

MS. BLAIR: First, they should actually conduct the review. I'm not being facetious. One of the potential consequences of the claw-back provision that is included in the new rules is that it may entice companies to forego privilege review. A company may not want to hire scores of lawyers to conduct the review when they think they can simply have any privileged information returned to them after the fact. *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), is one example of that approach. That said there are some techniques that can be used in addition to having attorneys examine your records. Search, for example, is a great tool. At our firm, we run our client data through a keyword filter that's programmed to identify potentially privileged records. Keywords might be terms like "attorney-client," "legal advice" and "confidential." We still eyeball the records, but search is a good safety net.

If you are frequently involved in litigation, you probably would benefit from having a specialized discovery support person in the law department.
— GERRY BOCCUTI

MR. ADLER: Does that also include attorney names?

MS. BLAIR: Yes, we also run searches for attorney names, as well as law firm domain names, e-mail addresses and the like to try to identify as many of those potentially privileged records as possible. We don't ultimately rely on programmatic searches, however. Privilege determinations still need to be made by an attorney or someone whose task is reviewing documents. But these are programmatic means by which you can supplement and maybe even speed up that human review.

MR. WEINER: I'd just like to say that I agree with Tess on the claw-back provision. To clarify, a claw-back is where you have an agreement with your adversary that if privileged information is produced, the other party will return it. The problem, however, is that even if we have a private claw-back agreement among the parties, which the new rules specifically allow, that doesn't necessarily control what's going to happen with third parties or the interplay between the state court and the federal rules. So my feeling is that you still have to review your ESI.

MS. BLAIR: On the issue of inadvertent disclosure, the risk is not only lawyers missing privileged records, but also vendors running queries and accidentally burning privileged records onto production CDs.

MS. SCHULER: I think Tess is correct. One of the reasons that vendors are now looking to e-discovery experts is for quality control. That is why I asked about accountability earlier in our discussion. Consultants routinely call into question the actions of vendors. That may be why I'm seeing a new trend in which vendors employ consultants to better their practices and verify their findings.

PROVING AUTHENTICITY

MR. ADLER: Frank, how do we ensure that at the end of the day, our evidence is authentic and admissible? How can a lawyer actually prove that an electronic document was not altered and came from a particular place?

MR. CONLEY: There are a lot of ways to demonstrate authenticity. What you do is going to depend on the nature of your data. A forensic computer examination will preserve data without modifying it, for example. And your expert will be able to testify regarding the origin and preservation of your information.

MR. WEINER: I'd like to address the flip side of this. I had a case where we had to prove that e-mails that were produced during the litigation, which supposedly exonerated the defendants of all wrongdoing, had in fact never been sent. So I do caution clients never to assume that something is what it appears to be just because it was produced during discovery. You want to ask your adversary about chain-of-custody issues so you know where the information originated.

MS. SCHULER: We have actually used photographs and video of the evidence in question in chain-of-custody disputes. If you know chain of custody will be debated at some point, photographing the actual evidence and recording its handling is a smart approach. Our goal is to verify every step that the evidence takes after leaving its original location.

LOSS OR DESTRUCTION OF DATA

MR. ADLER: We've talked about what might happen if you inadvertently produce data. What happens if through the inadvertent or intentional purging of data you do something wrong? Mark, could you address misconduct such as spoliation?

MR. SIDOTI: In this context, allowing relevant electronic evidence to be deleted – whether it's in the normal course of business or intentionally – would constitute spoliation. Not surprisingly, this issue has come up in a number of cases. And courts have pretty broad latitude when addressing spoliation. Some of their remedies can be quite drastic, such as striking a pleading, or more commonly an adverse inference instruction. Some litigants will actually use spoliation offensively to turn around a weak case.

MR. ADLER: Frank, would you agree with that from a plaintiffs' perspective, that just the threat of spoliation can actually change the dynamics of litigation?

MR. CONLEY: I would. I would also add that spoliation is not just the destruction of data, but also the modification of data. Usually, data modification is inadvertent, but regardless, you will still have the problem of altered evidence. From a plaintiffs' perspective, that does change the case because if you don't know what was there originally, you don't know what kind of case you have.

MR. ADLER: Tess, what can clients do to reduce the risk of spoliation?

MS. BLAIR: Spoliation prevention is really about focusing on data preservation. If you get preservation right, that means that all of the relevant data is going to stay where it is until you define what the scope of production will be. So you've got to know where your data is before litigation strikes, and focus on preserving that data when it does.

MR. BOCCUTI: From a corporate perspective, one of the things I do with our IT personnel is to make sure that they understand what sanctions can mean to the company.

MR. WEINER: I think people sometimes use the words "spoliation" and "sanctions" too loosely. There are a variety of things that can happen if data is lost or destroyed and it is the party's culpability that controls the outcome.

MR. BOCCUTI: Good point. Spoliation does not equal sanctions.

MS. BLAIR: That being said though, outside counsel and other lawyers who are involved in the discovery process are also being targeted with sanctions.

SELECTING AND MANAGING AN E-DISCOVERY VENDOR

MR. ADLER: I'd also like to address vendor selection and management. Paul, what are your thoughts on bringing a vendor on board?

MR. WEINER: A vendor is like any other expert you hire. You want to interview them in person and review transcripts of past testimony. You need to get references and talk to other people who have used them. Some people think it is enough for a vendor to have a nice Web site, or to have a lot of industry certifications. In my view, that is not enough.

MR. BOCCUTI: One of the qualifications I have for the vendors I work with is that they understand that I'm not just hiring them for their computers and network cabling. They should be aware of critical issues such as spoliation and sanctions and understand that if there is just one weak link in the chain, then we are all going to have a problem.

MR. ADLER: When is the appropriate time to bring in a vendor? And do you maintain an ongoing relationship with just one vendor, or do you use different vendors?

MR. BOCCUTI: Your vendor strategy needs to be flexible. Just as importantly, before you are even hit with a lawsuit you should have a good understanding of what your in-house capabilities are, what outside counsel is going to do and where your vendor will fit into the picture. Then when a case comes in, you will profile that case against your vendor strategy to determine which vendor you want to hire.

MS. SCHULER: You almost have a matrix of qualifications to apply to certain types of cases. Some vendors or consulting firms might be very talented in one area, whereas others might specialize in something else. It really depends on the type of case and the level of expertise required.

MS. BLAIR: I think it depends on the case. Ninety percent of the cases that we litigate don't require forensic analysis. In most cases it's just straight e-discovery processing – culling, conversion, hosting and so forth. Nevertheless, because there are so many places where the processing can derail, you do need to have a vendor strategy in place. And it of course makes sense to have vendors who know you. For example, there are still companies that use very unique e-mail systems, and so they might want to line up vendors who are equipped to handle those systems.

MR. ADLER: Gerry, at what point does a company need an in-house litigation support manager for e-discovery issues?

MR. BOCCUTI: It partly depends on the corporation's legal circumstances. If you are frequently involved in litigation, you probably would benefit from

SPECIAL ADVERTISING SECTION

E-DISCOVERY • A roundtable DISCUSSION

having a specialized discovery support person in the law department. This person would provide significant input into e-discovery policy and procedures and manage the inevitable issues that arise. Also, the person would serve the critical role of acting as a liaison between the parties involved in the e-discovery process – namely the law department and the information systems department. A person who has the time and expertise to manage these issues would help the other lawyers remain focused on the substantive issues that their cases present.

MS. BLAIR: You also have some larger companies that are not just identifying a single person, but rather are developing an entire infrastructure to manage their discovery because they have so much of it. Again, that is something that should be driven by the size of the company's litigation portfolio.

THE COSTS OF E-DISCOVERY

MR. ADLER: Paul, do the federal rules address the costs associated with electronic discovery and ESI?

MR. WEINER: Rule 26(b)(2) addresses e-discovery costs. It's basically a two-tier approach. First you identify the information that is reasonably accessible, and then you determine what is not reasonably accessible. The court can still order you to produce information that is not reasonably accessible upon a showing of good cause. In determining whether "good cause" exists, and possibly shifting the cost of obtaining the harder-to-reach data, the commentary to the rules instructs that courts should look at the specificity of the request; the quantity of information available from more easily accessed sources; the likelihood of finding information on the less accessible sources; whether there are other places the information could be obtained; and the parties' resources. Not surprisingly, these criteria closely track the criteria set forth by the federal courts in some of the leading cost-shifting cases. I do think cost shifting is going to be one of the hottest areas to come out of the new rules. I think parties are going to find ways to argue, "If you want it, you're going to pay for it."

MR. BOCCUTI: I think there is still very much a gray area as to what constitutes reasonably accessible information. Is a third-party affidavit sufficient to persuade a judge that obtaining this data is in fact reasonable? Is it a cost model to retrieve one bit of information from a system?

MR. WEINER: That's a great point. Neither the rules nor the drafting history define the term "reasonably accessible."

MS. SCHULER: I'd like to ask the group what consultants and vendors can do to help with cost shifting. Is there anything we can do at the outset, or is that determination made on a case-by-case basis?

MR. WEINER: I have used vendors very successfully in making cost-shifting arguments. With a vendor backing me up, I'm not just saying, "This is going to be expensive." Instead I can say, "If you want e-mail from 500 employees and we have to take forensic images of 500 hard drives, here is what it's going to cost, and here is how much time it's going to take." With the vendor, you have concrete, specific data to present to the court in support of your argument.

MS. BLAIR: I hope Paul is right about increased opportunities to make cost-shifting arguments, but I'm not optimistic. I think that courts are going to look at reasonably accessible versus not reasonably accessible and, in the absence of a demonstrable need for backup data, limit a lot of requests to reasonably accessible information. Only then, and I think it's going to be rare, will cost shifting even become an issue.

MR. SIDOTI: I agree. Thus far, for the most part, only information such as the contents of disaster recovery tapes or other information that had to be forensically restored has been considered inaccessible. It seems that unless the definition of "reasonably accessible" changes over time, cost shifting will remain a rare occurrence. But the new rules seem to allow the leeway for this type of change to evolve, perhaps more quickly than we all anticipate. Speaking from a defense perspective, I look forward to this evolution.

MR. CONLEY: And of course the technology is changing so rapidly that what was once inaccessible is now becoming much more accessible.

MR. WEINER: I think one important point that dovetails here is that the new rules specifically allow your adversary to take discovery on these issues. So you can have a whole little sideshow regarding accessibility.

PARTING THOUGHTS

MR. ADLER: We are nearly out of time, so I'd like to give everyone an opportunity to make some final remarks about e-discovery. What do you all see as future trends in this area? Do you have any final words of advice on this topic?

MR. CONLEY: I think that this area is going to evolve rapidly, which will make it very difficult for companies to stay current. I think that one of the big pitfalls is going to be this concept of where data is located and what you have to produce. For instance, there are some companies that are aggressively dismantling the concept of having offices. They have found that their employees are more productive when they work from home, so they're very gung ho about it. This is going to cause problems because these companies will have data dispersed over a wide geographic area, making it difficult to control.

MR. ADLER: Paul?

MR. WEINER: I think there are obviously some challenges ahead and it's going to be interesting to see how the state and federal courts work through the new rules. But I look at the new rules and all of these e-discovery issues as a positive thing and an exciting opportunity for law firms and companies to address and re-evaluate how they handle ESI. I think if we all embrace the e-discovery rules, we can ultimately save money and make the discovery process more efficient. That might be a little idealistic, but I'm hoping that's how this will play out.

MR. ADLER: Karen, what about from a vendors perspective?

MS. SCHULER: I think two things in particular are up-and-coming: first, enterprise and e-discovery solutions will gain momentum in the marketplace. And second, data storage and management will become a major consideration for companies. Companies will need to look at data mapping, cataloging, inventorying techniques and asset management to better understand their electronic discovery needs.

MR. ADLER: Gerry, what about from a corporate perspective?

MR. BOCCUTI: I don't have a crystal ball, but if I were to project three or four years down the road, I think a lot of these issues are going to stabilize. Companies will by then have tools, personnel and processes in place for handling e-discovery.

MR. ADLER: Mark?

MR. SIDOTI: It's going to be very interesting to watch the courts feel their way through these new rules. Literally every day, we see new court decisions in this area. I think that all of us – attorneys, corporate leaders and the judiciary – are going to shape this whole area during the years to come. And I do think it will stabilize, but I think it's going to be a learning process for everyone.

MR. ADLER: Tess?

MS. BLAIR: I agree with Mark and Gerry. E-discovery really is in its infancy. We do not have a lot of guidance, but fortunately we do have a lot of focus on this area.

For companies, e-discovery is really a front-and-center issue. Organizations are beginning to focus on getting their houses in order. And for litigators, it's clear that the era of discovery gamesmanship is over. E-discovery is too important and too risky for lawyers to engage in the kind of conduct we saw before technology became so advanced. So my hope is that with the new rules, we will have more constructive conversations, agree more readily on the scope and conduct of discovery and see more reasonableness in the process.

MR. ADLER: I would like to thank all of the participants for a very enlightening conversation. I think we've all learned a great deal about this changing area of the law.

Michael E. Adler is general counsel of national telecommunications service provider Hotwire Communications LLC. A member of the American Bar Association's litigation and telecommunications sections, Mr. Adler recently served as the financial secretary of the Philadelphia Bar Association's young lawyers division. Mr. Adler is an active member of numerous organizations including the Temple American Inn of Court and the Philadelphia Bar Foundation. In addition, *The Legal Intelligencer* recently identified Mr. Adler as one of Pennsylvania's "Lawyers on the Fast Track."

Prior to joining Hotwire Communications, Mr. Adler enjoyed success as litigator in private practice, obtaining a $2.6 million jury verdict in a breach of contract action brought against a computer consulting company.

Mr. Adler received his juris doctor from Temple University School of Law in 1998.

A partner with Morgan Lewis, **Stephanie A. "Tess" Blair** leads the firm's electronic discovery and data management practice, Legal Logistics. As the head of Legal Logistics, Ms. Blair specializes in e-discovery and works with Morgan Lewis attorneys and clients to manage complex litigation matters. Ms. Blair has developed industry-leading best practices that are designed to provide clients with state-of-the-art records and discovery management, knowledge sharing and collaboration resources.

Ms. Blair also counsels and defends clients in product liability, toxic tort, construction and other matters.

Prior to earning her juris doctor from the University of Miami School of Law in 1997, Ms. Blair studied industrial design at the Philadelphia College of Art, where she concentrated on product development, computer-aided design and marketing.

Gerard "Gerry" Boccuti provides legal consulting services to U.S. and international corporations. Currently, Mr. Boccuti serves as a consulting attorney and litigation support manager for pharmaceutical and healthcare company Wyeth. As Wyeth's litigation support manager, Mr. Boccuti and his staff oversee all litigation support services and are responsible for developing electronic discovery strategies and procedures for Wyeth's law department. Other recent clients include several Fortune 100 companies from highly regulated industries such as mining, energy and public utilities.

Prior to launching his consulting business, Mr. Boccuti was vice president of Westchester Consulting Group, where he managed re-engineering and consulting initiatives for large and mid-size corporate legal departments. Mr. Boccuti is a frequent speaker and author on e-discovery and other information technology-related topics.

A member of the American Corporate Counsel Association, Mr. Boccuti earned his law degree from the Widener University School of Law and studied international law at the University of Padua, Italy.

Frank J. Conley of Littler Mendelson represents and counsels management clients in connection with labor and employment matters arising under federal and state law. He works with clients on a variety of matters including Title VII harassment issues, the Family and Medical Leave Act, the Americans with Disabilities Act and workplace privacy.

Prior to joining Littler Mendelson, Mr. Conley was an associate with Miller Alfano & Raspanti, where he handled a variety of disputes ranging from contract issues to immigration to ERISA litigation. Mr. Conley has also served as an assistant city solicitor in the Philadelphia law department's labor and employment unit.

Mr. Conley is a 1998 graduate of the Temple University School of Law. As associate notes and comments editor of Temple's *International and Comparative Law Journal*, Mr. Conley authored an article addressing the effects of electronic communications on service of process.

As vice president of consulting with global litigation support provider ONSITE[3], **Karen Schuler's** recent engagements have included working for a boutique litigation consulting firm, serving as a senior computer forensic examiner for the U.S. Securities and Exchange Commission and lending her expertise to Navigant Consulting Inc. Ms. Schuler brings consulting experience with large-scale and complex litigation and regulatory requests to her position with ONSITE[3].

Mark S. Sidoti is a director at Gibbons P.C., a leading full-service law firm with offices in Philadelphia, New York and New Jersey. Mr. Sidoti concentrates his practice in products liability and business and commercial litigation. He also chairs Gibbons' internal electronic discovery task force and its information management and e-discovery client service group. Mr. Sidoti frequently publishes and lectures on e-discovery and document management best practices.

A member of the Sedona Conference Working Group on Electronic Document Retention and Production, Mr. Sidoti earned his juris doctor from Fordham University's school of law in 1988.

A shareholder in the Philadelphia office of Buchanan Ingersoll & Rooney PC, **Paul D. Weiner** is a member of the firm's litigation section. Mr. Weiner concentrates his practice in complex business litigation, including trade secret, patent and copyright disputes, as well as electronic discovery counseling and project management. Mr. Weiner also counsels clients regarding software development and implementation matters.

Mr. Weiner is a frequent author and speaker on a variety of topics including trade secret and e-discovery issues. In 2004, *The Legal Intelligencer* named Mr. Weiner one of Pennsylvania's "Lawyers on the Fast Track." Mr. Weiner serves on the executive committee of the Temple American Inn of Court and is a member of the Pennsylvania Bar Association's civil litigation section.

Mr. Weiner graduated from the Temple University School of Law in 1994.