INSIDE THE MINDS

e-Discovery Best Practices

Leading Lawyers on Navigating e-Discovery Requests, Evaluating Existing Policies, and Identifying Best Practices

ASPATORE

First Printing, 2009
10 9 8 7 6 5 4 3 2 1

The Pain and Discomfort Caused By Discovery of Electronic Information in Litigation Can Be Managed and Reduced

Michael Anderton

Counsel

Tucker Ellis & West LLP

ASPATORE

Keeping a Client Out of Litigation May Be More Valuable Than Prevailing In Litigation

I am a trial lawyer and I focus primarily on employment litigation, commercial litigation, and product liability litigation. Essentially, I defend companies when they are involved in lawsuits over disputes with their employees or former employees, business disputes, and lawsuits arising out of allegations that their product has somehow caused injury or harm to someone.

I also work with those same companies when litigation is not active, to try to give guidance to help them avoid litigation, if possible. In my mind, I add the most value for a client when I can help keep the client out of litigation up front by giving the client guidance on the best way to accomplish its business goals without putting it in harm's way from a litigation perspective. I often can save the client substantial time, energy, and resources by giving the client advice on how to get the business results it wants without generating litigation. This is particularly true in the employment law context, where there often are opportunities to develop long-term relationships with clients and to have conversations with them outside the context of litigation where you can talk to them and be proactive without the pressure of a lawsuit.

The best situation for the client and me is when the client will pick up the telephone when they are uncertain and call me before they act. The client almost always benefits, because that phone call will often allow them to avoid making the wrong decision, which may turn into more than a short phone call. For example, when a client wants to hire someone who may be subject to some type of restrictions (non-compete, non-solicitation, etc.) in his or her current employment contract, I guide the client on whether they can hire that person, the risks associated with doing so, and how to minimize the risks if they choose to go forward with the hire. I also guide the client in how to limit the new employee's activities, if necessary, and how to maximize the integration of that employee into their business operations as quickly as possible without violating the restrictions the employee is subject to under his or her contract. Those clients who do not call me in that situation before they hire the new employee almost always call me after they hire the new employee, often because the client and the

employee have been sued. At that point, the client is almost certainly going to spend a lot more than they would have spent on the up-front phone call.

In those unfortunate situations where litigation cannot be avoided, the advance counseling and guidance still can be extremely beneficial to the client, because I usually can guide the client on how to best posture itself if litigation occurs. Perhaps the worst situation is for a client to find itself in litigation it did not anticipate in advance. In those situations, there will almost always be facts that hurt the client that could have been set up differently with advance discussion between the client and me.

All of the same rules and concepts apply with respect to electronic discovery. A company can be proactive in advance of litigation and anticipate some of the problems that typically arise in the context of electronic discovery. A smart, active attorney can guide the company through the steps that can be taken in advance of litigation that will reduce or minimize the costs and, particularly, the burden of complying with electronic discovery obligations once a lawsuit starts. The benefits of this advance planning can be substantial. If a company becomes involved in litigation, there is almost no way around electronic discovery, and participating in the process of securing and producing electronic information can be incredibly burdensome and expensive. Often the threat of enduring the costs and burdens associated with electronic discovery will be the sole reason that a company pays money to settle a claim it otherwise would vigorously contest—and lawyers for the company's opponent usually know this. If the company has taken the right steps in advance of litigation, you can significantly reduce the burdens associated with electronic discovery and thereby reduce the leverage those burdens give to your opponent—they may actually have to work their case and present it on the merits instead of just hammering you with the costs and disruption of electronic discovery, and you are in a much better posture as a result.

The Current State of e-Discovery

There are three current issues on the front of e-discovery. The first is the scope of the duty to try to preserve electronic information when a company is in litigation or when it faces the threat of litigation. The issue is: what information needs to be preserved and when does the obligation to

preserve that information arise? Second, and somewhat related to the first issue: if an obligation to preserve electronic information arises—either before litigation starts or once it commences—and electronic discovery takes place, what needs to be produced, what needs to be produced solely at the cost of the producing party, and what must be produced only if some or all of the costs associated with producing the information are shifted to and shared by the requesting party? The third key issue at the front of e-discovery is the form in which electronic information is produced: when responding to discovery requests, what form is the information in when it is produced—its native format, a PDF file, a TIFF file?

All of this flows from the recent amendments to the Federal Rules of Civil Procedure, which were modified specifically to address and deal with electronic information. Most states are now following along and amending their rules to largely track the Federal Rules and specifically address electronic information. Because of those amendments, issues such as when you have to start preserving, what you have to produce, and what form you produce it in, are expressly covered by the rules, even though they may have been implicitly covered before. With the continued and increased incorporation of electronic information into litigation, issues that were substantially unresolved until the last several years continue to evolve as the new rules are applied going forward.

The biggest impact of these amendments to the Federal Rules and state rules is clearly to change the place where electronic information and discovery of electronic information fits into the context of a lawsuit. Prior to the amendments—when discovery was primarily or exclusively dealing with paper documents and only with limited electronic documents or information—you would typically initiate a lawsuit by filing a complaint, and the other side then would respond to the complaint by filing an answer, and only then would the parties serve discovery on the other side. Prior amendments to the Federal Rules required that you provide limited "initial disclosures" consisting of a general description of (1) the types of records you might have that you might use to support your claims or defenses and that might be responsive to discovery requests, and (2) the people who might have relevant information. But the new amendments to the Federal Rules moved more of the substance of what you have to do with respect to electronic information in the context of discovery up to the very front of a

lawsuit. The company's lawyer must start contemplating it and discussing it with the other side immediately. The lawyer cannot do that unless he has a complete understanding, from talking to his client, of all the information he will eventually need to properly and effectively have those conversations with opposing counsel and the court.

This is a very important, substantive topic that has to be addressed almost immediately, where before it was pushed further back into the litigation. The significance of it flows from the fact that electronic information makes up an overwhelming proportion of all business communication and information. The simple reality is that most of us now communicate, live, and essentially exist electronically. More than 90 percent of all documents and information exist in some electronic form, and a significant portion of that information exists only in electronic form. Logically, if there is a business dispute between two companies and 90 percent of the information that both companies maintain in the ordinary course is maintained electronically, and perhaps 30 percent of that 90 percent is maintained only electronically, it might be true that virtually all of the information that is relevant to the dispute is maintained in some electronic form. If that much information relevant to litigation is in electronic form, there is no way around the reality that discovery of electronic information will be critical to whatever you do in litigating that issue.

We already are at the point where a substantial portion of discovery in some lawsuits is electronic. We may not be too far from having cases where the only discovery that occurs is discovery of electronic information. Unfortunately, the courts and lawyers are still trying to catch up to the business world—despite the scope of electronic information that is potentially subject to discovery, there still is substantial uncertainty surrounding the scope and breadth of the obligations of the parties to a lawsuit regarding discovery of electronic information, and standards still are evolving.

Moreover, when you combine the scope of electronic information that is subject to discovery with the nature of how electronic information is handled, processed, and stored, and with the way people approach electronic communication and information, the importance of electronic discovery is magnified substantially. If an employee gets up, walks down the

hall, has a conversation, and says something inappropriate, it is possible that the content of that conversation will someday come to light, because someone can ask the employee (or the other party to the conversation) what was said. But that recall always is subject to some level of uncertainty. If you ask someone the contents of a brief conversation that occurred two years ago, how much of that will be recalled correctly? A lawyer always can challenge or attack what someone says they heard or said. With e-mail, it is much more difficult to challenge. People simply forget or ignore the fact that e-mail communication is effectively written communication, and that there likely will forever be a record of any comment made in an e-mail.

Because they ignore this aspect of e-mail communication, my experience is that people act and "speak" in electronic communication a lot differently than they would if the communication was going on paper. It is easy for an employee—who otherwise would have to pick up the phone or perhaps wait until lunch to make a comment to another employee on another floor—to just type a comment into an e-mail and send it. We all have seen and been involved with these virtual "conversations" where there are six or seven e-mails in the string, and we all know that not all of this communication is harmless. If employees had to write down all of the comments they make in e-mail and send them to the recipient in a memo, most of the comments would not be made until the two people were face to face or perhaps were on the phone. But the ease of e-mail communication prompts people to let their guard down and act as though no record is being made of the comment they make in an e-mail. The things people say in e-mail communication routinely astonish me—that someone would be foolish enough to effectively write down some of these things is remarkable. I have seen circumstances where litigation is ongoing and someone is alleging that a certain employee is a bad actor and treated him or her inappropriately, and yet, while that is ongoing, the alleged bad actor still sends e-mail communication containing comments that will compromise the company's legal position. If communication still had to be in memo form most of these comments would not be made.

Nor does it appear likely that people will change the way they communicate electronically any time soon. Company e-mail policies typically state that e-mails are intended for business use and can be reviewed by the company, and usually also expressly state that employees should have no expectation

of privacy in e-mails they send and receive using the company's system. The legality of such policies and of acting in accordance with them is pretty well established, except in some states with aggressive privacy protection laws. In most states, if your policy says you can look, then you can look, and there is not much the employees can do about that. Therefore, the company can monitor use of the system and an employee should not be surprised when someone from management tells him to stop sending sexually charged e-mails he is sending on the company's system to another employee or to someone outside the office. Some policies even are written to the extreme of saying no non-business e-mail communication is allowed. Yet employees still routinely use their company's e-mail system to send (and create a permanent record of) damaging content.

The problem is enforcement. If you simply fired everyone who did not comply, then you likely would not have any employees. How you manage employee use of your electronic systems can be critical. Are you proactive and do you have someone assigned to implement and monitor it regularly? Do you deal with improper conduct in an appropriate manner, even if it involves a key employee or someone who is well liked? Companies must find the right balance between doing so in an overly aggressive manner—strict policy terms and strict enforcement of the policy—and effectively letting the employees do what they want. Overly strict monitoring and enforcement may drive off good employees, while insufficient monitoring and enforcement may help foster the relaxed attitude regarding electronic communication that results in an employee saying something electronically that substantially damages the company's legal position.

The enforcement problem is not always an easy problem to fix. Most companies simply do not dedicate enough time or energy to policing use of their electronic systems by their employees. One result of this is that employees still feel little or no incentive to change the way they look at and use the company's electronic communication systems, and still say things they would never say in a memo. When you combine that with the reality that electronic communication and information makes up such a large component of the information that is out there, electronic discovery takes on greater importance.

e-Discovery Standards

The typical legal standards for electronic discovery now generally are set forth in the rules—the Federal Rules of Civil Procedure and the appropriate state court rules. There also may be applicable local rules that are issued by and apply only in a specific local court. The standards are not necessarily substantively different from the standards that always have applied and still apply to non-electronic discovery. If information is relevant to litigation, it is subject to discovery, and that does not change because it is in electronic form. For example, with paper documents, a requesting party has never been entitled to receive all information in the universe no matter the cost of producing it. There is a reasonableness standard the court should apply. Electronic information is subject to the same standard—the producing party is not required to spend unreasonable amounts of time, energy, and resources locating and producing electronic information. The biggest issues in electronic discovery today revolve around trying to set the reasonableness line.

The question is how to apply those historical standards to electronic information, which has some substantive differences compared to non-electronic information. Most obviously, electronic information typically is much more voluminous than non-electronic information. In addition, electronic information is more easily lost or corrupted, and there are many characteristics electronic information has that paper documents do not have. The issues revolve around the huge burdens that flow from these realities and determining what to do with respect to preserving, searching, and producing the electronic information and how to allocate the often substantial costs associated with these activities and/or how much disruption is appropriate to impose on the producing party.

Goals of e-Discovery

From a lawyer's perspective, the primary objective or goal of electronic discovery almost always is maximizing the likelihood of success in the litigation. The lawyer obviously wants the right outcome for the client, but not always at any cost. Most litigation is not worth an at-any-cost approach. Clients often view litigation from a strictly business perspective, and they should. As a result, the lawyer must be expressly aware of the client's

business objectives specifically with respect to the litigation and must try to find the balance between getting the right outcome and at the same time minimizing the disruption and economic impact on the client. The client's objectives may be different from one client to the next—one client does not mind the disruption, one client wants to stand on principles, and one client does not want to spend a nickel. The client and the lawyer need to explicitly discuss the client's goals and then the lawyer must be very frank and open with the client about the substantive impact and burdens associated with lawsuits.

In particular, the lawyer should have an explicit discussion with the client about the burdens of electronic discovery. Certain larger companies may have a litigation portfolio and may be involved in litigation every day—litigation may be inherent in the industry where they operate. These clients may have a little more tolerance for the fact that litigation means lawyers are now involved in every aspect of their electronic document creation, maintenance, storage, and destruction practices. Companies that do not have that experience usually look at it as an incredibly intrusive and distasteful process and often do not want to hear that they have to disrupt any aspect of their business because a lawyer tells them they have to suspend document destruction, or the IT department has to spend some of their time dedicated to issues that arise only as a result of the litigation. The lawyer must ask and the client must be open with the lawyer about its tolerance for these disruptions. Otherwise, the client and the lawyer will likely end up at odds with each other. That will likely make everyone unhappy and, as several very large, high-profile cases demonstrate, may put the lawyer and the client in line for significant adverse consequences that easily could have been avoided.

Enforcement of e-Discovery Obligations

The current enforcement issues relating to electronic discovery typically center around what has to be preserved, what has to be produced, what happens if something that should have been preserved and produced is not, and who pays the costs associated with preserving and producing. Like any discovery issue, if the parties cannot agree they end up taking that before the court for resolution. These disputes are essentially typical discovery disputes—parties cannot agree about whether something must be or should

have been preserved or produced. In addition, it can be very expensive to process electronic information for discovery. As a result, parties also now argue over whether some of the costs associated with producing the information should be shifted to the other party. What is evolving now is how the courts are supposed to look at these issues when they are confronted with these disputes.

There are some very influential cases that set the standards for what has to be preserved and when, as well as a set of guiding principles from what is effectively a standing committee on electronic discovery with representatives from all segments of the legal community. These cases and the guidelines issued by the committee have become the benchmarks followed by most courts, and should be looked to by most lawyers.

The most significant opinion is actually a series of opinions written by Judge Scheindlin of the United States District Court for the Southern District of New York in the case of *Zubulake v. UBS Warburg, LLC*. In the *Zubulake* case, there were what can only be described as a series of mistakes by the client and counsel in the context of preserving and producing electronic information in discovery. As a result, not all of the relevant information was preserved and not all of the information that was preserved was searched and produced. The result was a series of motions by the plaintiff seeking to compel discovery and asking for various sanctions. Judge Scheindlin, who had a strong interest and some knowledge and familiarity regarding electronic discovery issues before the case, took it upon herself to formulate a test for determining the scope of the information that has to be preserved and produced and also for potentially shifting the costs associated with production in appropriate circumstances. Judge Scheindlin's test quickly became the standard used by most courts looking to resolve these issues.

Another major source for standards that will be applied to resolve electronic discovery disputes and issues is what commonly are referred to as the *Sedona Principles*. The Sedona Conference effectively is a standing committee consisting of representatives of various segments of the legal community that meet periodically and issue guidance on significant topics. Judge Scheindlin was a key participant in the Sedona Conference on electronic discovery issues. The various guidance documents issued by the

Sedona Conference are referred to as *Sedona Principles*. The Sedona Conference first issued guidance concerning electronic discovery in 2003, and the guidance has been updated several times since then. The key document in this area is *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, and the current version is the second edition, which was most recently updated in June 2007 to incorporate the December 2006 changes to the Federal Rules of Civil Procedure. The substance of this document is the actual "principles" that are set forth on a variety of relevant electronic discovery issues—*The Sedona Principles for Electronic Document Production*. These fourteen principles provide brief guidance on important topics such as the scope of the preservation obligation, scope of discovery, cost shifting, form of production, and sanctions for non-preservation. The body of the document then goes on to provide detailed commentary and analysis of each individual principle and how the guidance reflected in the specific principle was developed by the committee.

The significance of the *Sedona Principles* probably cannot be overstated. Many judges simply do not have the technological knowledge and/or sophistication necessary to deal with and effectively resolve issues that arise regarding electronic discovery. Most of them have only really been forced to deal with these issues in the last five to ten years and, for many judges, their experience long pre-dates the relevance and advent of electronic information. Nevertheless, they usually recognize their deficiencies and they want to be fair and evenhanded in ruling on these issues and get the correct result. They are and will be looking for guidance and help in this area, and the *Sedona Principles* typically are viewed by judges as a good neutral source for guidance on resolving electronic issues and imposing burdens and costs on the parties, and for determining how to apply the recent amendments to the Federal Rules to real-life litigation situations. Any trial lawyer that is doing a lot of electronic discovery—and very few are not—must be very familiar with all aspects of the various documents issued by the Sedona Conference on electronic discovery and should stay current as they are updated.

Five Key Steps for Effectively Dealing with Electronic Discovery

The foundation for my five keys or steps to electronic discovery best practices comes from my approach to the practice of law. We have a lot of long-term, ongoing client relationships. We do not like to wait until our clients get sued and then react. We are always looking for ways to be proactive on behalf of our clients and for ways that we can keep them from being sued. My approach to electronic discovery reflects this philosophy. I want to take steps long before my client is sued that will prepare my client for electronic discovery and minimize the actual impact once the client must actually start preserving and producing information. I also want the client to take steps in advance of litigation that enable me to take certain positions with the opponent and make certain arguments to the court on behalf of my client that may further reduce the burdens of electronic discovery and may actually shift some of those burdens to the opponent. With some advance planning and anticipation, the significant costs of electronic discovery can be managed and the threat of shifting those costs can be used and may create leverage once litigation begins.

The first—and perhaps the most important—key to effectively dealing with electronic discovery is to make document retention a priority, not an afterthought. The company's document retention plan must be carefully drafted to satisfy regulatory and statutory requirements. For example, if you are subject to SEC or SOX regulations, you have to maintain documents in compliance with those laws. Your document retention policy also should go beyond minimum statutory requirements and incorporate company practices and preferences. You should get your lawyers to participate in the drafting process, if possible, and have them sign off on the plan. The lawyers then should be involved with any future changes to the document. The company should know about information that might be stored by individuals outside the ordinary system operation. Do employees keep random files on their local drives? If so, does the company want that to happen, or do you want to discourage it and encourage people to keep things only in the system? The document retention plan should consider and address these issues.

The plan also should explicitly consider and address backup mechanisms. The key is to make sure that backup tapes are not used for garden variety

archiving and/or intermittent information retrieval purposes. Backup tapes should be used only as a disaster recovery mechanism, unless there is some compelling reason to not do it this way. This aspect of the document retention system can be critical; one of the key distinctions often drawn by courts when deciding whether a company is going to be forced to bear the cost and burden of producing information on backup tapes—or whether the company is going to be directed to stop recycling backup tapes, another potentially significant burden or expense—is whether the company uses the backup tapes as disaster recovery only or as an extra storage archive. If the tapes are used solely for disaster recovery, the company is going to be in a better position to argue that the information on the tapes is inaccessible and not subject to discovery or, at a minimum, that the information is subject to discovery only if the other side pays the substantial costs associated with restoring the backup tapes and retrieving the information. How a company uses its backup systems speaks to the distinction between active and inactive information. Courts will generally force parties to litigation to search and produce active information at their own costs, and will usually be reluctant to force a party to search and produce inactive information without the opposing party sharing some or all of the costs. When you use your backup tapes for other than disaster recovery, you treat the information on the backup tapes more like active information and less like inactive information.

This is not just about the cost and burden of producing the information in the first instance. Courts may shift some or all of the costs of producing the information to the requesting party if they insist on discovery of what is deemed inaccessible information. But courts almost never shift the cost of reviewing the information that the producing party will almost certainly bear. Thus, even if you successfully argue that the opponent should pay for the cost of restoring dozens of backup tapes, you still will have to pay your lawyers to review the information for privilege and/or damaging information. That could be a substantial expense, and it is potentially very dangerous to just turn the information over to the other side without knowing what is there. So the key is to keep the opponent from having access to the information, and that perhaps can be accomplished by properly implementing the document retention plan.

Once you have the document retention policy in place, the company must police compliance actively and regularly. You cannot allow people to disregard the policy. If your policy says you are going to destroy documents at certain intervals, then you need to destroy documents at those intervals and comply with your own policy. If you properly craft your document retention policy and then comply with it going forward, you will go a long way toward having a much more pleasant electronic discovery experience. A key issue in many cases over the loss or destruction of evidence is whether the loss or destruction was willful or deliberate. Most courts recognize that it is acceptable for a company to destroy even documents that may have been relevant if they were destroyed pursuant to the document retention policy (except as they are subject to a litigation hold). It can be a problem if it ends up that the company did not preserve or produce relevant information. To the extent you have the policies in place and follow them and then you end up dropping the ball, it may not be as severe a problem. You can save yourself a lot of heartache and the severity of sanctions you face for losing electronic evidence can be reduced if you can convince the court you did not do it willfully but rather inadvertently. That will be much easier to do if you have an appropriate document retention policy in place and have a demonstrated history of following it.

The second key to effectively dealing with electronic discovery is to create a comprehensive map of your electronic information systems and equipment—what software is being used, who is using it, who has access to what information. The map should contain as much detail as possible about your electronic information systems. The map also should include some consideration and reference to the non-system use of local drives if that occurs, and you should know about it if it does. Portable electronic equipment also must be documented and tracked—laptops that are not part of the network system or PDAs and cell phones with voice mail, etc. Essentially, all the toys and gadgets that people now have need to be indexed and tracked on your electronic systems map if they are using them for business purposes in any way, because they may ultimately have relevant electronic information.

The map needs to be updated and modified as necessary. If you install new software or any new system or equipment, or if an employee leaves, the map must be updated. Any event that would affect the map should be

updated and reflected on the map. In my opinion, you need a dedicated person who is assigned responsibility for this task, and you should involve your lawyer in creating and updating the map, or at a minimum, you should send your lawyer a new copy of the electronic systems and equipment map every time it is updated in any way.

The third key to effectively dealing with electronic discovery is to consider litigation holds before litigation starts. The company should designate someone in the legal department in advance as the person responsible for dealing with litigation holds. That person needs to meet with outside counsel and talk about concepts with respect to litigation holds. The designated person must know what events trigger a litigation hold obligation and must be familiar with the general framework of the electronic operating system. He or she should be on the electronic systems map distribution list and should always have a current copy of the map. The general standard is that a litigation hold must be implemented any time litigation is even a remote possibility. The designated person must clearly understand when there is even the possibility that a hold should be in place, and they should be expressly given responsibility for contacting in-house counsel and outside counsel to discuss consequences. This means they will have to be on some type of distribution list for information relating to pending or threatened litigation against the company. The designated person should be trained to err on the side of caution—you always can lift a litigation hold and reinstate document destruction policies; you may not be able to recreate electronic information if the hold is not issued when it should be or as it should be in terms of scope.

The litigation hold advance planning process also should involve the IT department with the systems map. They should be involved in periodic discussions regarding litigation holds so they know in advance what the process might look like and have an understanding of what might be subjected to a hold and how it looks on the map. All of this is so the company does not have to scramble to educate people on the process when the lawsuit has started.

The fourth key to effectively dealing with electronic discovery, once you have the litigation hold in place, is to actively implement and manage the hold. This task is not overly difficult, but it must be given extremely high

priority. The person who is responsible for implementing and managing the hold must have the necessary training and background and also must have the appropriate authority within the company to do so—it is not sufficient if the person assigned this task cannot get cooperation from relevant employees. The person responsible for managing the hold should be the direct contact with outside counsel concerning the hold and the must have open access to outside counsel, and vice versa. Once the need for a hold becomes apparent, the appropriate person should work with counsel (outside and inside as appropriate) and determine the appropriate scope of the hold, looking at relevant IT maps, figuring out the departments that need to get the hold and how to communicate it to them, and then following up with them. The designated person must be in charge of making sure that every appropriate person (1) gets the hold; (2) acknowledges they got the hold and understands the hold; and (3) is actually complying with and implementing the hold. The company cannot let compliance with the hold fall through the cracks.

Perhaps no area relating to electronic discovery creates more potential exposure for companies than the area of litigation holds, and the wounds usually are self-inflicted. There are cases where a litigation hold was issued once and people do not follow up in any respect—initial compliance or continued compliance—and then a critical piece of information sits on a hard drive somewhere that somehow falls through the cracks and nobody sees it and the company suffers a huge consequence in the litigation. This can be avoided with proper monitoring and managing. The litigation hold needs to be expressly reissued and expressly re-acknowledged periodically.

In certain circumstances, the person managing the hold should turn key information over to counsel regularly. If you believe information could be lost at any point in this process, or if the information is simply deemed to be crucial to presenting the claims or defenses, it is probably a good idea to turn the information over to outside counsel.

In addition you may need to consider third parties when issuing the hold. The company might use vendors or other third parties that have some role in day-to-day operations and that might have relevant information, and the company may need to get them involved in the litigation hold process as well.

Finally, with respect to litigation hold implementation and management, you must keep detailed records of all the steps you take regarding the litigation hold. The records should reflect whom you communicated the hold to, how you monitored compliance, and how it was implemented. If you run into a problem with information being lost or not preserved, your lawyer will have to explain the process you followed to the court. If he cannot do that, his persuasiveness with the court likely will decrease substantially.

The fifth key to effectively dealing with electronic discovery is for the lawyer immediately to gather current information that will help support any arguments the lawyer may make on your behalf. The lawyer must determine as quickly as possible whether something is not reasonably accessible, and therefore should not be subject to discovery. The lawyer should already know some of this information if the first four steps are followed, but there will always be a need to get the most current information and apply what the lawyer already knows to the specific, currently existing circumstances, which may not be known until the lawsuit is initiated. This process will require that the lawyer get from you full and accurate information about how information is stored, where it is stored, and what it is used for. The information categories that typically are deemed inaccessible are disaster recovery backup tapes and things that are characterized as fragmented, erased, or damaged. To the extent the lawyer can categorize various repositories of information as falling in one of these categories, he is taking a step toward protecting the client from having to endure the burden and expense of producing the information.

The lawyer also should be gathering cost information along the way. This is critical, and should not be left until later in the process. The second part of the discovery argument (after arguing you should not have to produce it) is that the other side should pay for it. The lawyer must be able to accurately educate the court regarding the costs of producing the information and then be willing to ask the court to impose cost shifting if the opponent insists on expensive, time-consuming production. The lawyer also needs to be able to have a comprehensive discussion with the client and talk about priorities: What are your goals in this litigation? Do you want to spend as much as it takes to not let the other side win, or do you want to minimize spending or spend nothing? The lawyer must speak about costs associated

with electronic discovery and discuss prospective strategies and how they fit into the company's stated overall goals.

Aggressively Shop for Electronic Discovery Service Vendors

One thing that is obvious to me after being involved in electronic discovery circumstances over the last several years is that some of the expense associated with participating in electronic discovery probably can be saved. There are a host of vendors that provide the various services related to the act of retrieving and producing electronic information that often become necessary in the context of electronic discovery—backup tape restoration, searching, processing, data conversion, etc. Some of these vendors are national players, others are local or regional. Clients must make sure their lawyer aggressively shops among these vendors for the right to provide your electronic discovery related services. In my experience, these vendors charge incredibly expensive fees and rates to perform the services they provide. I believe many of them simply are used to dealing with very large accounts where the value of the litigation is large, the volume of information is perhaps overwhelming—where there is no way the company can do any of it in-house—and where the company is big enough that the costs associated with electronic discovery are not closely scrutinized and, in fact, where it is probably assumed that these are simply very expensive activities. Not all clients and cases warrant that type of approach, yet most of these vendors make no adjustment from one case to the next in their cost and fee structure. As a result, they charge a company of fifty-five employees the same rates and fees as they would charge GM. Moreover, the rate structure for these tasks usually is simply outrageous. Often, they are charging $200 or $300 per hour for the time of non-degreed personnel who are performing simple information recovery-related tasks, such as copying hard drives and recovering data, that require nothing more than two or three basic Microsoft training courses and little or no other education.

If at all possible, this should not be tolerated. More push back is needed from lawyers and businesses if these costs are going to come down. I have had success negotiating the costs and rates charged by the e-discovery vendors. Make sure you inquire about these issues with your lawyer and insist on shopping your electronic discovery vendor services needs among

several potential providers and monitor the process closely with your lawyer.

Challenges and Changes

The hardest part of best practices is getting companies to comply with monitoring of and compliance with various requirements that do not benefit the company's bottom line. For example, the litigation hold and the document retention policy do not generate any revenue. We all have 1,000 things to do, and companies often will issue a litigation hold and then wash their hands of it. If they have not dedicated someone and do not monitor and ensure ongoing compliance, then suddenly twelve months go by and nobody has done anything to follow up and see if the hold is being observed. Companies want to run their business and make money and they do not want to dedicate their time and resources to things that do not make them money. A litigation hold does not make the company money, but non-compliance with these obligations certainly can cost the company substantial money. Counsel must make their clients understand this reality and ensure compliance.

Similar concepts apply regarding document retention policies. Different companies that operate in different fields are subject to different requirements. Many requirements flow from government regulations and various obligations that arise in the specific industry where they operate. But once a company properly crafts its document retention/destruction policy to comply with industry requirements, the company is subject to the same standards as everyone else in the context of litigation. Companies often struggle with effective implementation and monitoring of the document retention and destruction policy, and sometimes they retain too much information before litigation arises and then cannot purge the information because of the litigation hold.

These concepts often prove much more difficult to put in place than one might think would be the case. Even when there are huge dollars at stake and very sophisticated and large companies involved, they often still do not have a clue how to implement a litigation hold, or they simply do not do it, and it often costs them money in the long run.

Because all of this is relatively new, the issues that are changing the most rapidly are those that are the current hot topics in electronic discovery: when do you have to preserve information; what do you have to preserve and what do you have to produce; and, if you have to produce certain information, who pays for it? The recent amendments to the Federal Rules of Procedure allow parties to argue about whether they have to produce something if they want to argue about it, and the court ultimately will decide the issue. The manner in which the courts resolve those issues is a long way from being definitively established, and each situation likely will be resolved based, at least in part, on its specific facts. Everyone's electronic system is different, the uses of information are different, and the access to information is different. This is why it is critical for lawyers to have detailed, accurate knowledge of the client's electronic information—every time a case turns on its facts is an opportunity for a lawyer to present those facts in a light that benefits his client and persuade the court to rule in favor of his client. It is also why advance planning and taking some relatively simple steps before you get sued can save untold money or resources.

Michael Anderton is a trial lawyer for Tucker Ellis & West LLP and practices mainly in the areas of business litigation and employment and labor law and litigation. He primarily represents businesses in commercial disputes, including those involving non-competition agreements, trade secret claims, and business-related torts, as well as employment lawsuits involving alleged discrimination, wrongful discharge, and compliance with federal and state employment laws. Mr. Anderton has represented service providers, banks and financial institutions, real estate investment firms, and a broad spectrum of manufacturing businesses, as well as a wide variety of Ohio public entities. He also counsels and represents various benefit and pension plans and plan administrators in litigation of claims arising out of ERISA-covered plans and represents various entities in product liability claims.

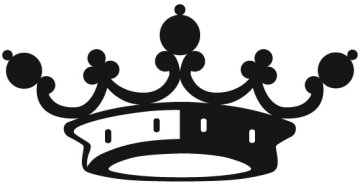
ASPATORE

www.Aspatore.com

Aspatore Books is the largest and most exclusive publisher of C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies and law firms. Aspatore annually publishes a select group of C-Level executives from the Global 1,000, top 250 law firms (Partners & Chairs), and other leading companies of all sizes. C-Level Business Intelligence™, as conceptualized and developed by Aspatore Books, provides professionals of all levels with proven business intelligence from industry insiders – direct and unfiltered insight from those who know it best – as opposed to third-party accounts offered by unknown authors and analysts. Aspatore Books is committed to publishing an innovative line of business and legal books, those which lay forth principles and offer insights that when employed, can have a direct financial impact on the reader's business objectives, whatever they may be. In essence, Aspatore publishes critical tools – need-to-read as opposed to nice-to-read books – for all business professionals.

Inside the Minds

The critically acclaimed *Inside the Minds* series provides readers of all levels with proven business intelligence from C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies. Each chapter is comparable to a white paper or essay and is a future-oriented look at where an industry/profession/topic is heading and the most important issues for future success. Each author has been selected based upon their experience and C-level standing within the professional community. *Inside the Minds* was conceived in order to give readers actual insights into the leading minds of business executives worldwide. Because so few books or other publications are actually written by executives in industry, *Inside the Minds* presents an unprecedented look at various industries and professions never before available.



ASPATORE