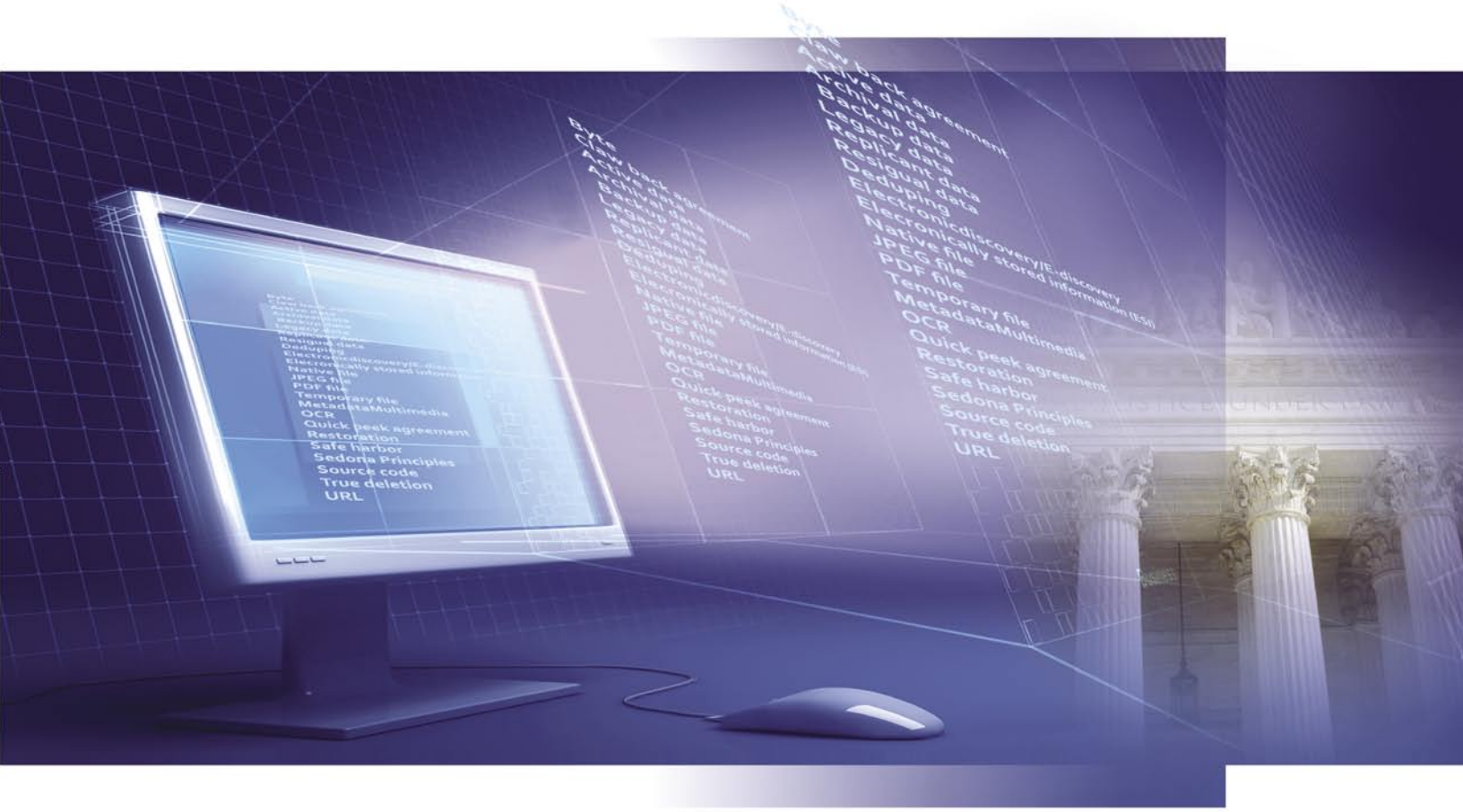
The Emerging Challenge of Electronic Discovery:

STRATEGIES for AMERICAN BUSINESSES



INSTITUTE FOR THE ADVANCEMENT
OF THE AMERICAN LEGAL SYSTEM

The Emerging Challenge of Electronic Discovery:

STRATEGIES FOR AMERICAN BUSINESSES

Institute for the Advancement of the American Legal System

at the

University of Denver

Institute for the Advancement
of the American Legal System

at the

University of Denver

2044 E. Evans Avenue, HRTM Building, Suite 307
Denver, CO 80208

303.871.6600

The Institute for the Advancement of the American Legal System (IAALS) at the University of Denver is a national, non-partisan organization dedicated to improving the process and culture of the civil justice system.

For more information about us please visit our website at www.du.edu/legalinstitute. We greatly appreciate your interest.

STAFF

Rebecca Love Kourlis Executive Director

Pamela A. Gagel Assistant Director

Jordan M. Singer Director of Research

Dallas Jamison Director of Marketing & Communications

Erin Harvey Manager of Marketing & Communications

Michael Buchanan Research Analyst

Jason Prussman Research Analyst

Patricia Daly Project Manager

Hilary Watt Office & Development Manager

IAALS would like to thank Richard Baer, John Frantz, Daniel Girard, Andrew Holleman, Richard Holme, Robert Kann, Linda Kelly, Don McLaughlin, Patrick Meyers, Patrick Oot, Ken Stafford, Stefan Stein and Malcolm Wheeler for their feedback and assistance in preparing this publication.

For reprint permission please contact IAALS.

Copyright© 2008 Institute for the Advancement of the American Legal System.
All rights reserved.

CONTENTS

EXECUTIVE SUMMARY

This publication contains important information to prepare your business or organization for the possibility of litigation. Specifically, it focuses on the risks and rewards of electronic discovery—the exchange of electronically stored information such as e-mails, spreadsheets and word processing documents—before trial. You need to think about electronic discovery now, in order to prevent potentially enormous costs and problems if you become involved in a lawsuit. The first half of this report explains why electronic discovery can be so expensive, time-consuming and nerve-wracking. The second half provides some practical steps that you should take now to prevent problems from occurring in the future.

INTRODUCTION

In the business world, ideas travel fast, and the next big thing is never out of sight for very long. And whether your business makes high-tech components, sells party favors or does something in between, one of the next big things is electronic discovery in litigation. You already know the power of computers and electronic devices to make your work more efficient. What you may not know is that failure to store the electronic information generated by those devices in the right way could severely affect your business should it ever be involved in a civil lawsuit of any kind, including a simple contract dispute, employment case, patent or trademark litigation, or warranty dispute. Among other things, being caught unprepared could:

- Cost your business thousands (or even millions) of dollars and hundreds of employee hours to retrieve electronic information;
- Require you to pay for costly restoration of old e-mails and electronic documents that you thought had been deleted and were gone forever;
- Subject you to claims of destroying evidence ("spoliation" claims), which could result in your losing a case even if you had a better position on the merits; and
- Pressure you into settling the case, regardless of the merits, because of the ongoing costs it places on your business.

Virtually every business and organization, regardless of size, needs a strategy for dealing with the possibility of electronic discovery. This report is designed to help you prepare such a strategy.

What is electronic discovery, and why does it pose such dangers? Electronic discovery (or e-discovery) is a shorthand term for the exchange of electronically stored information (ESI) that frequently occurs during the course of a lawsuit. ESI can include most of the information you generate each day, such as e-mail, electronic invoices, electronic personnel files, internal memos and voice mail. If you have not yet thought about whether the way you manage your ESI could affect you in litigation, you are not alone. A recent study found that only 43% of U.S. companies have a clear strategy for managing electronically stored information.[1] The real number may even be lower, since the survey included only businesses with in-house lawyers. But being among the many who have not developed an ESI management strategy will not help your business in the event of litigation. Actually developing a strategy will.

This report is written primarily to help small and mid-size businesses—generally those with fewer than 500 employees. It is a population that is underserved with respect to information on the impact of e-discovery, although that information is just as critical to small businesses as it is to large corporations. The principles set forth here, however, are broadly applicable to businesses and organizations of any size. If you are a business of more than 500 employees and have not thought yet about electronic discovery, this is still a good place to start.

The aim of this report is to describe the current landscape of electronic discovery and to provide some practical advice about preparing for the risks of e-discovery well before you encounter them. To accomplish this, we enlisted the help of many of the best and brightest minds in the legal world who have been close observers of e-discovery trends and issues. They include a number of federal and state judges, attorneys from many of the top law firms in the country and in-house counsel at some of the biggest and most litigation-experienced corporations in America. We asked this "virtual advisory group" about current issues in e-discovery, where they thought the e-discovery phenomenon was going next and what you should do to prepare. Their observations heavily influenced this report. It is not legal advice; in fact, nothing is this report should be taken as legal advice. But it is sound strategic advice.

We begin with a brief introduction to the core concepts of electronic discovery and explain why it has become an issue of such concern. We then assess the current and future status of e-discovery based on the observations of our virtual advisory group and finally offer some ideas to help you prepare your business or organization. We have endeavored to keep the discussion as non-technical as possible. Where we have used technical terms, we have defined them in a glossary at the end of the report.

PART I: TERMINOLOGY AND ISSUES

The basics of electronic discovery

Generally speaking, discovery is the process by which parties in civil litigation exchange information relevant to their claims and defenses before trial. Discovery usually takes several forms, including the exchange of specific documents, oral depositions, written questions (known as interrogatories) and requests to admit certain facts. Electronic discovery concerns the subset of discovery that involves the production of ESI to opposing parties. ESI includes all information stored in an electronic medium, including audio and video files, e-mail messages, instant messages, voice mails, websites, word processing documents, databases, spreadsheets, digital photos, information created with specialized business or engineering software and backup or archival copies of that same information.

In a paper world, civil discovery is a relatively straightforward process (albeit too often a time-consuming, expensive and unpleasant one). As a litigant, you are asked to review the opposing party's requests for certain documents, collect files and information that are potentially responsive to those requests and make the files accessible to your attorney to review for relevance and privilege. If your paper documents are reasonably well-organized, retrieving them is not terribly difficult. Moreover, there is a certain finality to the document collection process; there are a limited number of paper copies of any document, and once papers have been physically destroyed, they are gone forever. You can only produce the documents you have.

In an electronic world, however, you often have to produce the documents you do not have—or do not think you have. Unlike a paper document that has been destroyed, ESI frequently can be recovered even after it is thought to be deleted from a computer system. And unlike old memos, which need only be retrieved from a file cabinet or warehouse, some older ESI (such as archived or legacy data from outdated computer systems) may be recoverable only at great expense. To add another layer of complication, some ESI may be created automatically by your computer system without your knowledge. Even information you know you have—such as e-mails—may be more challenging to produce because discovery requests frequently seek even slightly different copies of the same document, and the ability to forward e-mail easily often makes it difficult to determine how many copies exist.

The permanence of electronically stored information is good news and bad news for any potential litigant. The good news is that opposing parties in litigation are less likely to be able to hide evidence—if it exists in

some recorded format—because copies are likely to exist somewhere. The bad news is that in responding to requests, you too may be required to comb through layers and layers of electronic data in response to your opponent's requests—perhaps at great expense, intrusiveness and interference with ordinary business operations.

Challenges raised by e-discovery

The discovery of ESI poses several significant challenges to your business or organization. If not addressed thoughtfully and proactively, the costs of producing ESI can spin out of control. Should you anticipate a lawsuit, you will need to decide quickly what ESI must be preserved and how best to preserve it. You and your attorneys will have to determine in what form ESI should be produced, as well as screen ESI for privileged and work product communications that should not be produced. At best, these challenges are a nuisance. If these challenges are not addressed carefully, however, the result may be disastrous.

The cost of e-discovery

The most pressing concern with e-discovery is the extraordinary potential financial burden that any given case carries. Four factors contribute to the risk of high e-discovery costs. First, the volume of ESI is usually much higher than with traditional paper documents, in part because of the massive amount of e-mail and instant messages that are created and distributed to multiple recipients on a daily basis. According to one estimate, American businesses send 2.5 trillion e-mails each year. Second, most of this information is saved on backup tapes (to protect against a catastrophic computer failure), but all too frequently the tapes are not labeled, cataloged or organized properly, making the search for responsive information more difficult. Third, much of the information on backup tapes is difficult to recover, meaning it must be specially processed or translated before it can be used. Finally, the conversion of ESI into indexed and reviewable files often requires the assistance of technical experts.

These contributing factors have led to disturbing cost figures. In a published case from 2002, the cost to restore 200 backup tapes of information was approximately $9.75 million.[2] In another case, the cost of restoring 93 tapes came to $6.2 million, or nearly $67,000 per tape.[3] And costs are only expected to grow. One recent estimate placed the overall revenue for e-discovery vendors at $1.5 billion for 2006, growing to $4.8 billion by 2011.[4] Even a small ESI production may cost thousands, or tens of thousands, of dollars.

If not addressed thoughtfully and proactively, the costs of producing ESI can spin out of control.

PART I: TERMINOLOGY AND ISSUES

The disproportionate cost of e-discovery is raising eyebrows not just with the businesses and organizations that have to shoulder the financial burden, but also with the courts themselves. At a recent conference sponsored by e-discovery vendor H5, Supreme Court Justice Stephen Breyer was informed that discovery in a routine case might cost $4 million, and exclaimed, "We can't do that…. If it really costs millions of dollars, then you're going to drive out of the litigation system people who ought to be there."[5] At another conference, Magistrate Judge Paul Grimm from the U.S. District Court for the District of Maryland cautioned, "If you're spending $150,000 to produce the information and $250,000 for your lawyer to review it and the case is only worth $500,000…this is a problem."[6] To fix the problem, all stakeholders in the system—the courts, attorneys, litigants and the general public—will need to think innovatively and cooperatively. In the meantime, cost will continue to be the chief concern surrounding e-discovery.

Preserving information

As a general rule, you are required to preserve information that is even potentially relevant to a lawsuit as soon as you reasonably anticipate that litigation might occur. But while preserving paper documents is relatively straightforward, preserving ESI can be considerably more difficult. The reason? ESI can be changed easily, quickly and without your intervention. It may even be changed without you knowing. For example, e-mails may be automatically deleted after a set period of time, as may e-commerce transaction journals that record credit card purchases. Similarly, some databases update accounts receivable in real time, writing over previous information. Once written over or deleted, this information may be difficult and extremely costly to recover.

On the other hand, some ESI is created without human intervention—or even without you knowing it exists. One of the most common forms of these data is metadata—literally "information about information." Metadata are data about an electronically stored file, and they are hidden within the file itself or a linked database. Metadata usually include information such as the file's creator and creation date, and the dates on which the file was opened, read, modified or printed. Because metadata may be created and updated without the user ever knowing, humans may inadvertently alter relevant metadata just by opening a file.

Finally, ESI that is preserved through backup storage or archival storage poses its own special

challenges. Backup tapes contain a snapshot of all ESI on a computer or network at a given moment in time. This is good for restoring the entire system if it crashes, but it is highly problematic if you are trying to locate certain ESI, because the data generally are not organized or sorted. Similarly, archived ESI from software programs that are no longer in use (known as legacy data) is also a challenge to restore, because the computer systems or software used to create legacy data are frequently old, difficult to find and even harder to convert to current technology (think of data stored on 1980's-style 5¼-inch floppy disks). Therefore, even ESI that is preserved may be difficult to review or produce.

The many forms of electronic information

Information that is printed on paper historically has been shared or produced only on paper. But electronically stored information can be produced in a variety of forms, each with advantages and disadvantages. Native files, for example, are files in their original electronic format, which are read (and manipulated) by programs such as Microsoft Word, Excel and Outlook, WordPerfect or Lotus Notes. Native files can be easily searched or sorted and may include metadata and "hidden" comments. Due to this manipulability, however, native files are susceptible to accidental or intentional alteration. It is also difficult or impossible to remove confidential or privileged information (such as attorney-client communication) from native files, or to number individual pages, without first converting those native files into another format.

Other formats for producing electronic information, such as PDF files or TIFF files, create an image of the native file which may be redacted or numbered more easily. But these forms have their own drawbacks. The most important limitations are the inability to electronically search the document under most circumstances,[7] as well as lack of sortability. For example, an electronic spreadsheet may be nearly useless in PDF or TIFF form, because the spreadsheet cannot be sorted, manipulated or fully expanded.

Collectively, the issues of cost, preservation and form of production pose serious challenges for the business that finds itself embroiled in litigation. E-discovery can consume enormous time and resources, and force you to base your litigation strategy on cost concerns rather than the merits of the case itself. Careful planning, however, can rectify the balance and place e-discovery back into its rightful role as a tool for collecting relevant information rather than a weapon to bludgeon the unprepared and unwary. That preparation is both achievable and necessary and is the focus of the next section.

Careful planning can rectify the balance and place e-discovery back into its rightful role as a tool for collecting relevant information rather than a weapon to bludgeon the unprepared and unwary.

PART II: PLANNING FOR E-DISCOVERY

Like nearly any business challenge, e-discovery benefits heavily from advance planning. And while a standardized e-discovery process has not yet emerged, collective experience has provided some clear lessons about how to prepare for and handle e-discovery in as efficient and inexpensive a manner as possible. All of these lessons that follow share one central theme: be proactive about your e-discovery obligations. The more prepared and organized you are from the beginning, the more likely you are to weather a potential storm.

Accordingly, we offer below some basic principles to get your business or organization ready for e-discovery. Read them, think through them and work to understand them. Considering the issues—and potential solutions—before you face litigation could save you countless hours, dollars and business interruptions.

1. Prepare your business or organization for electronic discovery the way you would prepare for a catastrophic event—that is, calmly and well in advance.

For small and medium-size businesses and organizations, lawsuits generally and electronic discovery specifically can be unwelcome, surprising and threatening. There is the very real fear that a lawsuit will cost so much and take so long that the business itself will be severely affected. In order to avoid the immediate cost and use of resources to prepare for discovery, it may be natural to deal with this fear by ignoring the risk of a lawsuit or rationalizing that it is unlikely to happen. But as our virtual advisory group counseled, ignoring the problem now only increases the risk of a much more significant problem later.

Think of e-discovery planning as a form of insurance. Your business faces the risk of certain catastrophic events: natural disasters, computer or communications breakdowns, crimes or acts of terrorism and so on. Recognizing these risks, perhaps you have obtained insurance policies, developed emergency procedures to protect the safety of your employees or copied or backed up important files in a secure location. The chances of a catastrophic event actually occurring may be slim, but the potential consequences are high, and it is easier to sleep at night knowing that you are prepared if such a moment should come.

The same advance planning applies to lawsuits and e-discovery. A small effort now to understand your technology and develop procedures for dealing with it responsibly will help you rest assured that if you do experience litigation, you can handle it in the best way possible. You will not be scrambling to learn about the content of your company's ESI or where it is stored. You will have protocols in place for retaining ESI and will be able to speak knowledgeably about what your files contain. You will understand your obligations on a day-to-day basis. Our virtual advisory group emphasized that businesses and organizations that take time to prepare in advance save themselves much greater amounts of time and business disruption later.

There are several actions you can take right now to prepare your business or organization for encounters with e-discovery. First, either you or a designated person should learn your own technology and be comfortable with the electronically stored information that you generate and save every day. Second, your business should create and adhere to a regular document and ESI retention and

disposal policy that sets out exactly what information will be retained; what information will be discarded; how, and how often, the discarding will take place; and who will be responsible for monitoring and ensuring compliance with the policy. Third, you should develop a general plan of action in the event that you are sued, which would include contacting your lawyer immediately, and with his or her help, taking necessary steps to preserve information relevant to the lawsuit. We talk through each of these steps in further detail below.

2. Accept modern technology for what it is.

One of the lawyers in our virtual advisory group noted that some businesses and organizations may fear using certain software or technology because it may make them more susceptible to litigation, or at least enlarge the potential pool of ESI they will have to produce if they are sued. That is technically true, but the benefits of using technology every day almost certainly outweigh the risks that come with litigation. Indeed, there is little choice in today's world but to use electronics in your business, and good businesses internalize and accept the inherent risks of using technology because the benefits are so much greater. All the major advances in office technology of the past 50 years—copy machines, personal computers, fax machines, cell phones, PDAs, voice mail and the like—have expanded the pool of potential evidence in a lawsuit, but they have also generated economies of scale that have allowed businesses and organizations to be more efficient and productive. Do not shy away from technology if it makes business sense.

3. Inform yourself about the technology that you use every day.

Just as you know the names and capabilities of your suppliers and distributors, customers and clients, you or a designated employee should know the names and capabilities of your software programs. How do you generate and store information? Do you have a network or shared drive? Do employees use personal drives on their work computers? How frequently, if at all, is ESI saved to portable storage media like DVDs, CDs and flash drives? How often is data backed up, and how is that done? Similarly, how often is e-mail backed up, and how long are backup tapes preserved? If your e-mail is through one of the large web-based providers (AOL, Google, Microsoft, Yahoo, etc.), do you know their policies about preserving messages? If you have company voice mail, cell phones or PDAs, what are the provider's policies about retaining the data they generate? If you have a company website or blog, how often is it updated and are earlier versions stored or backed up?

If you have an information technology (IT) person or department, you may want to schedule some time for them to educate you and/or your lawyer(s) about the technology. You do not need to become a technology expert, but you should feel comfortable with how information is collected and stored, and for how long. Do not assume you know—in this area, too many commonly held assumptions prove to be wrong. Familiarity with your technology will help you make educated decisions should litigation arise.

Blissful ignorance of how your technology works is no longer an option for a business or its litigation

You do not need to become a technology expert, but you should feel comfortable with how information is collected and stored, and for how long.

attorneys. Indeed, the courts are making clear that unfamiliarity with one's own technology is not an excuse for failure to produce ESI in a timely and complete manner. In a recent case, plaintiff's counsel argued that his failure to produce approximately 4,000 e-mails contained on a DVD was due to "technology issues… which exceed[] Plaintiff's computer expertise."[8] The court was unimpressed, noting that

> *Perhaps* plaintiff's counsel can be heard to plead technical ignorance or mistake in his initial dealings with the DVD, but … upon the receipt of [a letter from defense counsel], he was on notice of the potential problem and was obligated to seek competent assistance to ascertain the truth about the contents of the DVD.[9]

Investing the time to know your technology now will pay significant dividends should e-discovery become an issue in the future. For businesses with in-house attorneys, consider tasking one of your lawyers with learning your electronic information systems and keeping up on the relevant law on ESI, so you can remain proactive and avoid conduct that may hurt you in litigation. When confronted with litigation, a business should also be prepared to educate its outside lawyers about its information systems, thus it is helpful to have an in-house attorney or other knowledgeable employee who is prepared to do so.

4. Be thoughtful about how you save—and preserve—electronically stored information.

The terms "spoliation" and "sanctions" send shivers up the spine of every potential litigant. No one wants to pay a fine or lose a case simply because some piece of information was inadvertently lost. However, our virtual advisory group also cautioned that the solution is not necessarily to save every piece of ESI that your business or organization creates or receives. The better approach is hands-on management of your ESI, through a routine retention and disposal policy prior to litigation or the threat of litigation, and a litigation hold once the prospect of litigation surfaces.

If you do not have a policy that specifically discusses retention and disposal of ESI, now is the time to create one. A recent survey showed that only 8% of companies with a fully implemented records program say their program addresses ESI very well.[10] Other companies and organizations do not yet have any formal retention program or policy. Put bluntly, this is a recipe for disaster. Several members of our advisory group suggest that implementing and following a standard retention policy is one of the most significant ways to keep costs down and prevent the risk of spoliation and sanctions. Work with your lawyer to create a suitable policy, and make sure your employees understand the policy and follow it.

You should also discuss retention and disposal policies with any outside contractors you use—for example, for accounting or human resources purposes, or web or database hosting. In a lawsuit, these outside contractors could receive a subpoena for records relating to your business. Even if they are not subpoenaed, the ESI they have relevant to the lawsuit may still have to be produced because it may be deemed to be under your "possession, custody or control"—and therefore subject to your business's normal retention obligations. Once you have a

set policy for how long you retain records internally, discuss implementing a similar or identical policy for retaining your records with outside contractors. To the extent possible, you should ensure that all your documents and ESI are working on a consistent life cycle.

You should make every effort to inventory the sources and storage media of the ESI you do retain, in order to make it easier to identify what ESI may be potentially responsive in a given matter, and where and in what form that ESI is stored. When data is well-organized, it can be searched and reviewed by computers in a fraction of the time—and with greater accuracy—than a review by hand. You place your important paper documents in files and know where to find them. Your treatment of your electronic files should be no different.

Once you have reason to believe that litigation is likely—even if a lawsuit has not yet been filed—you should implement a litigation hold. A litigation hold is different from an ESI retention policy. The latter should be in place constantly, and reflect the general approach of your business or organization to retaining and destroying documents and ESI. A litigation hold is specific to a particular dispute and is used only when litigation is known or anticipated. A litigation hold overrides the normal document retention policy and halts the disposal or deletion of documents and ESI that might be relevant to the litigation. For example, in a lawsuit involving a claim of wrongful termination, a litigation hold might require the preservation of (among other things) the terminated employee's personnel file; any internal or external e-mails and voice mails including, discussing or naming the employee; and the hard drive of the terminated employee's work computer. As soon as you anticipate litigation, you should consult your attorney to craft a litigation hold appropriate to the specific dispute.

Having an established retention and disposal policy and implementing an early, clear litigation hold are essential to protect you from the risk of spoliation claims. In addition to reducing the likelihood that a spoliation charge could be brought against you, clear preservation policies make it more likely that you will be able to fight off a spoliation claim that lacks merit. By contrast, the failure to implement a complete and consistent litigation hold has resulted in significant sanctions in many cases. In one recent case, for example, a large company failed to use a litigation hold to preserve ESI, and the court later ordered the company to retain an outside vendor at its own expense to collect and produce missing ESI, and imposed sanctions on the company of approximately $125,000.[11] The lesson here is: be thoughtful and proactive about the information you preserve and how you preserve it.

5. Do not assume that if ESI is deleted, it is gone.

Information deleted from an e-mail server or a computer's recycling bin may appear to be gone forever, but it is often recoverable. The act of deletion merely changes the file's status in the computer's disk directory to "not used," which permits the computer to eventually write over the file.[12] Unless and until that overwriting occurs, however, the file remains intact and may be recovered by searching the disk itself rather than the disk's directory.[13] Moreover, such "residual data" may be more difficult and costly to access than "active data"

Implementing and following a standard retention policy is one of the most significant ways to keep costs down and prevent the risk of spoliation and sanctions.

which are used every day. Stories abound of public and private sector employees (and executives!) who, thinking themselves clever, simply deleted critical e-mails on the assumption that the e-mails then could not be produced in a lawsuit.[14] In fact, this tactic—in addition to being in bad faith and potentially sanctionable[15]—only creates the greater expense to rescue the deleted e-mails from a hard drive or backup tapes.

6. Choose your professional assistance carefully.

In the last five years, scores of attorneys and "e-discovery vendors" have held themselves out as experts in electronic discovery practice. Some of them are very knowledgeable and efficient, but our advisory group warned that many others intentionally or unintentionally drive up the cost of e-discovery for their clients. Knowing what to look for is key.

The e-discovery phenomenon is moving very quickly. Unfortunately, many lawyers are not keeping up. One judge we consulted told us that the average attorney does not even know what to ask for with respect to ESI. Similarly, a lawyer told us that many attorneys, including most senior partners at law firms, do not pay much attention to e-discovery because they do not understand the technology and instead just hope that opposing counsel will similarly ignore e-discovery issues altogether. Still fewer lawyers are insisting that their clients take a proactive approach to e-discovery, which would save considerable cost. Younger lawyers are perhaps more likely to be comfortable with the technology at play, but most law schools still do not address specific issues of e-discovery in a meaningful way.

Lawyers also may face certain conflicts in advising you about the extent of warranted e-discovery, because electronic discovery (and discovery generally) is a profit center for law firms.

The good news is that more and more lawyers are recognizing the need to develop e-discovery acumen immediately. E-discovery experience has risen to the top of the priority list for potential clients seeking attorneys. An increasing number of law firms have attorneys or in-house IT staffers who are dedicated entirely to advising clients on e-discovery issues. Likewise, the role of the paralegal is changing; more paralegals are becoming internal experts on electronic evidence management software and the reputation and skill of outside IT vendors.

The familiarity with outside vendors may prove to be a significant boon for potential clients of the vendors, because at the moment the risk of vendor abuse runs rampant. Put simply, IT vendors offer an external source for facilitating production of ESI—from distilling the relevant ESI from a network or computer drive to loading that data onto media in the format requested. One lawyer we consulted explained that the use of vendors can drive up the cost of e-discovery because litigants do not specify what data the vendors should retrieve, or do not realize what products they are ultimately receiving from the vendor. It is becoming increasingly important that businesses look for a vendor who is efficient and trusted, and explain to the vendor exactly what material should be extracted and produced.

There are many vendors in the e-discovery arena today. Gather information before you select a vendor and compare their processes and pricing. You should know exactly what

services a vendor will provide and what those services will cost. A good vendor will explain the steps to be taken for data retrieval, data and document processing, the review process that you and your attorneys will have to perform, and ultimately the steps in the production of those documents and data. Knowledgeable attorneys and/or vendors can help devise focused searches that pull together the relevant ESI in a cost-effective manner. For example, through keyword searching, vendors can filter your ESI significantly before anyone begins to review it by hand. Search engines today can go through millions of documents in a few seconds, and many of the databases used to review ESI have the ability to tag or assign groups of documents—including duplicates and near duplicates—as responsive or not responsive to one or more issues with a few clicks of a mouse. This is a great improvement over the manual review of the past, where sticky notes were placed on hard copies to indicate the documents marked for production.

Good professional assistance also extends to forensic experts. Once a lawsuit has been filed or you have received a subpoena, you may be tempted to go into your company's computer system and start looking around for specific ESI related to the case. Several experts have cautioned to fight off the curiosity to examine the computers yourself and instead consult with your attorney to structure an appropriate investigation that protects the integrity of your business or organization's electronic information. One reason your attorney might recommend using a forensic vendor is that computer files are filled with information about the computer and its files (system data and metadata, respectively), which is usually hidden from plain sight. System data and metadata record when the computer was turned on, when a file was opened or altered, and other similar information. The mere act of turning on a computer and looking for files may alter the system data and metadata relevant to a party's claims and defenses. If necessary, you can have a forensic expert make a forensically sound copy of a hard drive before it is turned on and examined, so there is always a source capturing the original files and metadata. The right forensic expert can help not only to retrieve your data without manipulation but also can also provide witness testimony, if necessary, as to the chain of custody of the data.[16]

There are many vendors in the e-discovery arena today. Gather information before you select a vendor and compare their processes and pricing.

7. Control the tone of your own litigation.

Any litigation will ultimately be faster and less expensive if the parties stay focused on their claims and defenses rather than fighting about the discovery process. To promote this cooperation, the current Federal Rules of Civil Procedure and several similar state rules require the parties in every case to confer early in the litigation process on e-discovery issues, including the type and amount of ESI that each party anticipates requesting from the other. There is good reason for this requirement: early conferencing has been widely heralded as one of the most effective ways to keep discovery costs under control. By meeting early, the parties can discuss which computer systems should be subject to preservation and discovery, what the relevant time period for discoverable information should be, and the identities of individuals on both sides who are likely to have relevant ESI.[17]

When the parties agree to keep their e-discovery requests narrow and focused, and use available technology to cull electronic information to that which is truly relevant,

the process can be controlled. By contrast, unnecessarily broad requests require all parties to search through and produce unnecessary and marginally relevant information at great cost. If you become involved in e-discovery, work with your attorney early on to set the tone for all parties to act cooperatively. Even if you are not in a court that requires an e-discovery conference, it is recommended that you attempt to reach an early agreement with the other side on e-discovery issues.

It is almost always more cost-effective to resolve issues without the court's intervention. However, if you cannot reach a good faith agreement with the opposite side about how and when ESI should be produced, do not be afraid to ask the court to step in. An increasing number of courts are now issuing detailed orders governing the electronic discovery process, offering definitions of key terms and setting out specific procedures for the recovery, review and production of electronic data.[18] While most courts would prefer that the parties settle e-discovery procedures themselves, clear guidance from the outset—even in the form of a court order—may help prevent an expensive disagreement later.

8. Insist on proportionality.

Electronic discovery is paper discovery magnified. This can be both a positive and a negative. When parties focus on the narrow areas of dispute and request only information that is truly relevant to their case, the discovery process can be informative and useful, and can help promote an appropriate resolution. And when discovery requests are properly narrowed, the produced ESI may be much easier to search than traditional paper documents. But when one or more of the parties insists on extensive discovery purely because it is possible to do so, the result can be considerable delay, wasted employee hours and costs well-beyond the amount in controversy.

In other words, proportionality is key. One expert we talked to said he regularly sees the costs of e-discovery running three to four times the low estimate of liability and twice the high estimate of liability—a phenomenon known to some as "discovery extortion" because parties cannot afford to continue even with a meritorious claim or defense. Even worse, extortion sometimes turns into a suicide pact. A judge we spoke to told us about a case in which the parties sought judicial approval for their joint e-discovery plan. Each party had been so focused on how much ESI it could get from the other side that both agreed to a plan that would have cost them *five times* the total amount at issue in the case. As in this example, the courts may catch these types of overzealous oversights, but yours should never be the case that slips through. Insist on proportional discovery—with your own lawyer, with opposing parties and with the court.

9. Be precise about the ESI you request and insist on the same precision.

You can also reduce your own costs by requesting the ESI that is most likely to be relevant to the dispute and training your lawyers on the information systems in your business that are relevant to the dispute. Many attorneys are trained to ask for "any and all" materials related to a topic, even though most of those materials may be only tangentially relevant, for fear that they will miss a "smoking gun" document. But most cases do not have "smoking guns." Well-crafted requests, and the

subsequent application of appropriate search terms, can pull out the critical ESI without requiring your attorneys to sift through thousands or millions of pages of extraneous information. Putting more time and thought into crafting narrow but comprehensive requests at the front end could save considerable time and money in review of ESI later.

In any event, as one judge put it, the days of requesting "any and all" information are effectively gone.[19] There is simply too much ESI that could be asked for—even a small business, for example, may generate or receive hundreds of e-mails a day. Some courts are increasingly clamping down on overbroad requests in the e-discovery context, and insisting that the requesting party first explain why it needs every e-mail, or every electronic invoice, or every piece of metadata.[20] As for the courts that are more reluctant to limit discovery, litigants tired of excessive costs associated with marginally relevant ESI are trying to force the court's hand.

One area where the courts have been quite good about keeping e-discovery under control is the form in which ESI is to be produced. Under the Federal Rules of Civil Procedure, parties are encouraged to request ESI in a specific format—be it a native file, a document-like form such as a PDF or TIFF file, a physical printout, or some other form. Here is where it pays to know the details of your own ESI. Some information may present itself equally well in many formats, while other information may only be useful as a native file. The better you know the form or formats of ESI that you are best able to collect, review and produce efficiently, the better equipped you will be to respond to the other side's production requests.

10. Be ready to educate the court about your ESI.

Sometimes disputes about the form, cost or magnitude of ESI production simply cannot be worked out by the parties, particularly when one party bears nearly all the cost and burden of producing the information. There is now a provision in the Federal Rules of Civil Procedure and some state rules that allow the court to shift costs from the party producing ESI to the party requesting it, if the requested ESI if "not reasonably accessible"—which means essentially that the ESI is not stored in a format that can be used in the ordinary course of business.[21] With this rule in place, the business or organization that is able to prove or disprove reasonable accessibility quickly and efficiently will have an advantage.

Proving undue burden and cost can be a difficult process—particularly at a time when spending hundreds of thousands, or even millions, of dollars on discovery is commonplace—but the effectiveness of your argument will be increased by specific and precise evidence of how much the cost will be. Some large corporations that deal with lawsuits on a regular basis have begun careful tracking of all their e-discovery costs from case to case, which allows them to present a very precise picture to the court when arguing that compliance with all e-discovery requests is unduly costly and burdensome. Even if your business or organization does not have a wealth of litigation experience, knowing your technology and the expected production costs early in the process can strengthen an eventual cost-shifting argument or an argument to limit the scope of the discovery requests.

When one or more of the parties insists on extensive discovery purely because it is possible to do so, the result can be considerable delay, wasted employee hours and costs well-beyond the amount in controversy.

CONCLUDING THOUGHTS

The e-discovery diet starts with you. Businesses and organizations that take the time to know the information they are producing will find themselves better prepared in the event of litigation. Having a good handle on what ESI you create, and how you manage it, will allow you to calmly and thoughtfully gather your own information, and be confident that you are producing information that is complete, not privileged and does not include unnecessary or superfluous data. Acting now can save you time, money and headaches in the future.

Thinking about e-discovery now and addressing it early in a case not only gives you a competitive advantage with respect to producing ESI, but also with respect to requesting it from opposing parties. Familiarity with your own ESI can help you determine what information your adversary is likely to possess. It also allows you and your attorneys to craft discovery requests that are appropriately focused.

In the event of a discovery dispute, advance preparation can also help you in court. You can protect against spoliation claims by offering evidence of a document and ESI retention policy and a litigation hold. You can bolster cost-shifting and discovery limitation arguments by demonstrating exactly where the requested data is, why it is not reasonably accessible and why the cost of production is disproportionate to the overall amount in controversy. You can educate the judge about the ESI at issue.

Ultimately, advance thinking about your business or organization's ESI can help you get through the discovery process more quickly, which in turn can help you get through the entire litigation process more quickly. Put another way, efficient and cost-effective discovery is a key component of efficient and cost-effective civil litigation —and much of that efficiency is under your control. By protecting your information, you protect your business. And the time to start is now.

NOTES

1. *See* Sheri Qualters, *U.S. Companies Lack E-Data Strategy,* NAT'L L. J., December 14, 2007.

2. *Rowe Ent., Inc. v. William Morris Agency, Inc.,* 205 F.R.D. 421, 428 (S.D.N.Y. 2002).

3. *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.,* 52 Fed. R. Serv. 168 (E.D. La. 2002).

4. *See* Daniel Fisher, *The Data Explosion,* FORBES, Oct. 1, 2007, http://www.forbes.com/business/global/2007/1001/052.html.

5. Quoted in *id.*

6. Quoted in Jo Maitland, *Judges Speak Candidly on New E-Discovery Rules* (Jan. 31, 2007), *available at* http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1241499,00.html.

7. PDF or TIFF files are typically static image files that are not searchable. They may be searchable if the producing party also delivers the underlying text that is extracted from the native file during the process of converting the native files to PDF or TIFF.

8. *Garcia v. Berkshire Life Ins. Co. of Am.,* 2007 WL 3407376 at *5 (D. Colo. Nov. 13, 2007).

9. *Id.* (emphasis in original).

10. "Attorneys Face Nine Critical Challenges in Being Prepared for Legal Discovery, Groundbreaking Survey Shows," PR NEWSWIRE, Sep. 26, 2007.

11. *See Wingnut Films, Ltd. v. Katja Motion Pictures Corp.,* 2007 WL 2758571, *21 (C.D. Cal. Sep. 18, 2007).

12. For e-mail programs such as Microsoft Outlook, it takes multiple steps even to get to this stage. Upon initial deletion, items are placed in a "Deleted Items" folder, where they remain until the user empties the trash or until some date set by the administrator for automatic deletion. At that point, the messages go into a hidden folder called "Recovered Deleted Items" where they reside again until some date set by the administrator for automatic deletion. Therefore, even e-mails thought to be deleted twice by the user may still be easily recoverable.

13. *See* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Civil Litigation: Is Rule 34 Up to the Task?,* 41 B.C. L. REV. 327, 327 (2000).

14. *See, e.g.,* Dennis B. Roddy & Tracie Mauriello, *E-mails show how Dems tied staffers' bonuses to campaign work,* PITTSBURGH POST-GAZETTE, Dec. 16, 2007 (noting the deletion – and eventual recovery – of 31,000 e-mails); Rick Casey, *Who probes DA's deeds?,* HOUSTON CHRONICLE, Jan. 5, 2008 (quoting a district attorney's admission that his decision to delete over 2500 e-mails during a pending civil rights lawsuit was "an error in judgment").

15. Technology is now available that will scrub hard drives sufficiently to make ESI unrecoverable. There is continuing uncertainty about what courts will do when a company uses such technology not for ordinary business purposes, but solely to ensure that deleted ESI cannot be recovered if and when litigation occurs.

16. Some states are considering tightening the qualifications of forensic experts who will be permitted to gather ESI for use in a lawsuit, in part to protect and preserve the integrity of the evidence collected. Potential accreditation requirements provide yet another reason to choose forensic experts very carefully. See Deb Radcliff, *Computer Forensics Faces Private Eye Competition,* BASELINE MAGAZINE, Jan. 2, 2008, http://www.baselinemag.com/article2/0,1540,2242720,00.asp.

17. It is worth reiterating here that the early meeting is designed to flesh out the scope of ESI to be exchanged during discovery, not the information that should have been preserved during a litigation hold. Litigation holds generally include all potentially relevant information and are instituted no later than the initiation of the lawsuit—or sooner, if litigation is anticipated earlier.

18. For some particularly detailed orders, see *In re Genetically Modified Rice Litig.,* 2007 WL 1655757 (E.D. Mo. Jun. 5, 2007) (preservation order); *O'Bar v. Lowe's Home Ctrs., Inc.,* 2007 WL 1299180 (W.D.N.C. May 2, 2007) (production order); *Williams v. Taser Int'l, Inc.,* 2007 WL 1630875 (N.D. Ga. Jun. 4, 2007) (e-mail search protocol with explicit clawback provision); *In re Seroquel Prods. Liab. Litig.,* 2007 WL 219989 (M.D. Fla. Jan. 26, 2007) (production and preservation order).

19. Hon. John J. Hughes (United States Magistrate Judge, District of New Jersey), *Top Ten Tips for E-Discovery* (on file with IAALS).

20. *See, e.g., Heartland Surgical Specialty Hosp., LLC v. Midwest Division, Inc.,* 2007 WL 2122437 (D. Kan. Jul. 20, 2007); *Hedenburg v. Aramark American Food Servs.,* 2007 WL 162716 (W.D. Wash. Jan. 17, 2007) (denying request to create mirror image of plaintiff's hard drive because "Defendant is hoping blindly to find something useful in its impeachment of the plaintiff.").

21. Fed. R. Civ. P. 26(b)(2)(B); see also Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).

GLOSSARY

Byte—the basic unit of memory storage on a computer. Storage capacities on most computers today are measured in gigabytes (GB), or one billion bytes. Increasingly, storage is now being measured in terabytes (TB), or one trillion bytes.

Claw back agreement—an agreement that allows a producing party in discovery to demand the return of an inadvertently produced privileged document or electronically stored information within some reasonable time after the inadvertent production.

Data—

Active data—data that are easily and currently accessible on a computer or other electronic device.

Archival data—data that are stored separate from an active computer or network, but which can be retrieved in the ordinary course of business – the rough equivalent of off-site storage for paper documents.

Backup data—data that are saved onto a storage medium separate from a computer or computer network, specifically to assist recovery in the case of catastrophic failure. Backup data typically represent a "snapshot" of an entire computer system, and are not deliberately sorted or organized.

Legacy data—data from a computer system that is no longer in use.

Replicant data—data that are automatically created by certain computer systems and programs for short-term recovery in the event of system failure.

Residual data—data that still exists on a computer system even though it has been thought "deleted" by a user.

Deduping—the process of removing duplicate electronic files prior to production.

Electronic discovery/E-discovery—the discovery of electronically stored information.

Electronically stored information (ESI)—all information that is stored on an electronic medium, including audio and video files, e-mail messages, instant messages, websites, word processing documents, databases, spreadsheets, digital photos, information created with specialized business or engineering software, and backup and archival copies of that same information.

File—

Native file—electronic files in their original electronic format; that is, the format in which they are most commonly created, read and manipulated.

JPEG file—a file commonly used to store photographic images, particularly for use on the World Wide Web.

PDF file—a PDF (portable document format) file is created from a native file and depicts the same information, but in a less manipulable form that a native file. PDFs can be made searchable, but generally cannot be altered or manipulated. PDFs may be Bates numbered. They do not allow access to metadata unless the metadata is itself converted to a PDF file.

Temporary file—a file that is designed to store information for a short time, and typically deleted automatically by a computer after use.

TIFF file—a TIFF file is usually created by scanning paper documents, and acts essentially as a "screen shot" or "printout" of the native file. TIFF files can show text and graphics, and may be made text searchable. They do not show metadata. TIFF files may be Bates numbered.

Metadata—information about electronically stored files that is hidden within the files themselves. Metadata usually includes information such as the file's creator, creation date, and dates on which the file was opened, read, modified or printed. Accurate metadata can assist in the authentication of electronic files.

Multimedia—a combination of methods of presenting information, such as the combined use of audio, video, and text files.

OCR—an abbreviation for optical character recognition, a technology that allows a user to scan text into a computer and create a searchable document. This is usually done on a TIFF or PDF file that was not created from a native file. OCR technology is still improving, and does not have 100% accuracy.

Quick peek agreement—an agreement that allows a requesting party in discovery to inspect the producing party's documents or electronically stored information in order to identify the information it would like to have produced. The producing party then reviews the selected information for privilege before production.

Restoration—the process of regenerating data that has been lost or corrupted.

Safe harbor—in the e-discovery context, a term generally referring to rules that protect a party from sanctions when that party, in good faith, inadvertently loses or destroys electronically stored information.

Sedona Principles—a series of fourteen principles for electronic document production, developed by the Sedona Conference. The Sedona Principles have been influential in the growth and development of e-discovery rules and case law at the federal and state levels.

Source code—the code for a computer program, written in a programming language that is readable by humans. Source code may be relevant in certain cases, such as those involving intellectual property claims for a computer program.

True deletion—a process by which electronic files are permanently and irretrievably removed from a hard drive, and cannot be restored.

URL—an address on the World Wide Web, such as http://www.du.edu/legalinstitute.

INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM
UNIVERSITY OF DENVER

2044 E. Evans Avenue • HRTM Building • Suite #307 • Denver, Colorado 80208 • Telephone: 303.871.6600 • www.du.edu/legalinstitute