CHAPTER 1

Discovery: The New Philosophy

1.1 The Prominent Role of Electronically Stored Information

Electronic communication in all forms is pervasive in every aspect of our modern society. Chances are pretty good that you have thought about the implications of this new reality on the practice of law more than once—as evidenced by the fact you are reading this book. Chances are also pretty good that you know the 2006 revisions to the Federal Rules of Civil Procedure by heart, and you may have even attended a CLE or two on the topic of e-discovery. After all, there is at least one presentation on the topic in every major city nearly each month. At a minimum, you have probably exchanged an e-mail as evidence in printed form for discovery in at least one of your cases. You might be thinking right now that you know enough and that you really do not need a better understanding of the electronic discovery process unless you are a big firm lawyer representing Fortune 500 clients, or that you know all there is to know on the subject.

The truth of the matter, however, is that electronic discovery affects all lawyers involved in civil litigation in an increasingly significant
way. As a testament to the prevalence of e-discovery across the board in modern legal practice, seventy percent of in-house legal counsel in the US and fifty-three percent in the UK now say that their companies have a policy in place to govern what the federal rules now refer to as electronically stored information (hereinafter “ESI”). Second Annual ESI Trends Report, Kroll Ontrack (2008). The pace of change in the law and technology associated with e-discovery means, however, that even if you knew all there was to know last year, your knowledge may now be obsolete and your client’s ESI policies may need to be revised.

The advancement of technology in the past decade has catapulted the prominence of electronic evidence. Take a moment to consider a few facts to help you grasp exactly how prominent of a role electronic evidence plays in the legal landscape of today and tomorrow. First, 99.9 percent of information created is created digitally and only 0.1 percent is created in paper format, according to Craig Ball in a “Law Technology News” article published in October 2007. More than seventy percent of that information is never printed.

E-mail traffic volumes are expanding at rapid rates. E-mails can be particularly important and culpable evidence because of people’s tendency to communicate informally and reveal facts they never would memorialize in writing on a piece of paper containing their signature. One of the earliest public illustrations of the candor that often accompanies e-mail communication occurred in 1996 in an e-mail exchange within the Wyeth-Ayerst pharmaceutical company regarding the side-effects of the Phen-Fen diet drug: “. . . can I look forward to my waning years signing checks for fat people who are a little afraid of a silly lung problem?” See Alicia Mundy, Dispensing with the Truth: The Victims, the Drug Companies, and the Dramatic Story Behind the Battle over Fen-Phen, (St. Martin’s Press, Inc., April 2001). More recently, the N. Y. Times published an article titled, “E-mail blunders: Top 10 dumbest moments of 2008.” Among the examples of remarkably candid (i.e. dumb and dumber) e-mails was one accidently sent to staffers alerting them that their jobs could be in peril—the e-mail was intended only for senior management. Also, Angel-O-Lantern Countrywide CEO Angelo Mozilo hit reply rather than forward when identifying a customer’s e-mail as “disgusting”; the reply was noted by both the media and the investor community. E-mail blunders: Top 10 dumbest moments of 2008, N. Y. TIMES, Oct. 27, 2008.

E-mail, word processing documents, spreadsheets, and databases contain discoverable information that is nearly impossible to destroy as computer forensic technology can frequently retrieve data that has been deleted, wiped, defragmented, or otherwise “destroyed.” Today,
there is usually not a “paper trail” to establish a chain of events. Instead, electronic footprints and fingerprints often provide the clues to determining past conduct. Today’s lawyers and investigators must understand computer forensics and e-discovery best practices as they mine metadata and electronic files for digital clues and evidence to support a case.

The inescapable conclusion from all of this is that it is just a matter of time before you are confronted with a substantial e-discovery exercise—if it has not happened already. You are likely to encounter, at some point in the foreseeable future, an electronic discovery matter that involves tens or hundreds of custodians, multiple hard drives, a box of backup tapes, 100 DVDs, and the contents of one or two servers. E-discovery is an inevitable reality for any civil litigator in the early twenty-first century. Are you ready?

The key to being prepared for electronic discovery is to understand how technology interacts with the law to form the current discovery landscape. This book has been drafted to provide its readers with up-to-date and practical information regarding both the legal and technological aspects of the electronic discovery process in the real world, and is intended to serve as a guidebook to lawyers and litigation support personnel navigating the electronic discovery landscape. While other books focus solely on the law, the technology or academic exercises, this book brings it all together for you—as a lawyer—needing no-nonsense advice upon which you can act.

As you read this guidebook, remember that the waters of electronic discovery are not stagnant, but are constantly changing. Every day new orders and opinions are released that further evolve the law’s treatment of electronic evidence. If you roll up your slacks and wade into the electronic discovery waters on two consecutive days, it will not be the same water that you step into. The electronic discovery experience from a few months ago could be drastically different than the electronic discovery experience you would face today, and the experience next week may be more different yet. Different laws may govern. Different technologies may be available.

Understanding the current state of the industry including the governing laws and presently available technologies is a necessary and vital step to being prepared to zealously advocate on behalf of your client today. Make no mistake about this fact—as a lawyer, you are expected to know how to navigate the e-discovery process. This book will provide you with the knowledge to confidently manage discovery in your case. This knowledge is your compass that you can turn to as a baseline when you encounter uncharted waters in the future. Those new waters will make sense if you make an effort to stay informed and place that new knowledge in the context of the information you will possess after reading this book.
1.2 Current State of Affairs: The Intersection of Law and Technology

The reality of today’s electronic discovery is that the developing law reflects the technology currently available. It is a bit of a chicken and egg scenario: technologies and best practices for their use are being developed and molded to conform to legal requirements and expectations. Similarly, developing case law tends to reflect the state of available and known technological solutions. Electronic discovery law and technology move together as if in a dance. It is critical that you understand that this interplay exists in order to form best discovery practices and make compelling discovery arguments in court. The remainder of this section provides an overview of the issues that will be discussed in the remainder of this book (divided topically between legal and technological considerations) while highlighting the connection that exists between the law and technology. This connection is so strong that is functions like the spine in the nervous system—the heart cannot function without the brain to provide it instructions and the brain cannot survive without fresh blood pumped by the heart—and likewise modern electronic discovery practices would not be what they are without input from both law and technology.

DISTINGUISHING COMPUTER FORENSICS AND ELECTRONIC DISCOVERY

As a threshold matter, it is absolutely essential to understand that electronic discovery and computer forensics are distinct disciplines. These terms are mistakenly used interchangeably in both legal and technical circles; however, these disciplines differ greatly and knowing when to use the proper vernacular will set you apart in meetings with your client and the court. Perhaps the confusion between these terms arises because elements of electronic discovery and computer forensics frequently interact in a single matter. Both disciplines are encompassed within the concept of electronic evidence.

Electronic evidence describes all technology-based evidence, no matter how it is retrieved or for what purpose it is used. Electronic discovery is the process of preserving raw electronic data contained on a storage media somewhere, collecting the data, filtering and processing the data to cull out that which is non-responsive or privileged, and producing the relevant data as electronic evidence. In contrast, computer forensics deals exclusively with forensic collection and analysis of data contained on computer storage devices.
The quick reference chart in Figure 1.1 and the text that follows help distinguish the differences between computer forensics and electronic discovery.

Figure 1.1 Computer Forensics v. Electronic Discovery

Computer forensics is an art and a science that takes years of experience to master. Typically a forensic investigation involves analyzing Internet history, file dates and times, and recovering deleted data. As discussed in further depth in chapter five of this book, because of the way that computer systems store information, when a file is deleted, it is not actually physically removed from the computer system until another file is stored in precisely the same location. Thus, a computer forensic expert can recover all or part of that “deleted” information. Likewise, electronic evidence can frequently be recovered by a computer forensics expert from a hard drive that has been physically damaged (e.g., dropped, fire-damaged, water-damaged, etc.). In short, unlike in the paper evidence world where a paper document is destroyed once it has been shredded, burned, or otherwise destroyed, “delete does not mean delete” in the context of electronic evidence. The ability of computer forensics consultants to frequently retrieve data even after it has been “destroyed” has heavily influenced the development of the law regarding preservation duties, reasonableness limitations on discoverability, and sanctions for spoliation, as discussed in depth in chapter three. Counsel involved in electronic discovery must understand the computer forensics process so that he or she can effectively craft legal arguments and convey the information to the opposing counsel, judge, and jury—this means learning
how to speak the same language as the technical experts when discussing the facts of the case and the desired outcome.

Another example of how computer forensics technology is interrelated with the development of e-discovery law can be found by examining the relationship between proper computer forensics chain of custody and the legal requirement of authentication, as discussed further in chapter three. Any evidence admitted into trial must first be authenticated, which means that some showing that the evidence is what it purports to be must be made before the court will allow a jury to consider the evidence. In the context of electronic evidence that has been forensically collected or analyzed, proper chain of custody protocols and documentation must occur to meet the authentication burden.

THE CURRENT STATE OF ELECTRONIC DISCOVERY LAW

The law governing electronic discovery has been developing at a breakneck speed, and the authors of this book are not aware of any signs that this pace will slow anytime soon. There are two means through which discovery law develops—regulations and case law. When the last edition of this book was published five years ago, there was a near-total lack of regulations governing electronic discovery. For example, the last edition of this book dedicated only a single page to the Federal Rules of Civil Procedure, as the only relevant passage then in the Rules was a reference to “data compilations” being discoverable. Between then and now, the Federal Rules of Civil Procedure have been amended to make specific reference to the treatment of ESI in discovery, and an entire chapter of this book (chapter two) is now dedicated to the Rules.

The Federal Rules of Evidence were also recently amended and signed into the law by the president on September 19, 2008, to include Rule 502. Rule 502 is titled “Attorney-Client Privilege and Work Product; Limitations on Waiver” and governs the inadvertent waiver privilege protecting communication or information in federal courts. Furthermore, five years ago only a few states (e.g., California and Texas) had passed regulations to govern electronic discovery in state courts. Now, many states have passed regulations specifically concerning electronic discovery. Please see Appendix B for a complete listing of the current status of electronic discovery laws by state.

The most dramatic development of law regarding electronic discovery, however, is the rapid evolution of the case law. In the last edition of this book, we included an appendix with a citation to every electronic discovery case known to the authors totaling approximately sixty pages in length. Today, out of pure necessity, we have limited the appendix to the most crucial or influential ESI cases so that the book
can remain reasonably portable! Nonetheless, the current appendix is still approximately thirty pages long and reflects only a small percent of the total available case law on these issues at the time of printing.

The rapid evolution of e-discovery case law is no surprise to anyone who has dealt with electronic discovery on even a semi-frequent basis for two principle reasons. First, electronically stored information plays an extremely prominent role in modern society, and the characteristics unique to ESI were not adequately addressed by the case law that had developed around paper discovery. Second, the technology in the last several years to aide in electronic discovery has advanced rapidly and its impact (both when utilized by savvy practitioners and when non-savvy practitioners ignored the technology) has been felt by the courts who deal with discovery disputes. In a nutshell, the law is catching up to the realities of modern practice.

The following is a “Top Fifteen” list of cases that every practitioner must be familiar with before engaging in electronic discovery. This list contains critical information for all practitioners and is a must-read.

**Top 15 E-Discovery Cases (in alphabetical order)**

1. **Appellate Court Reverses $1.58 Billion Jury Award Based on Spoliation**  
   *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005). In this fraudulent sale of stock lawsuit, the plaintiff filed a motion for an adverse inference instruction against the defendant for destroying e-mail and failing to comply with a court order to compel e-mail. Despite an SEC regulation requiring e-mail retention for two years, the defendant overwrote its e-mail every twelve months. Based on this, the trial court ordered the defendant to produce backup tapes, review e-mails, conduct searches, produce responsive e-mail and a privilege log, and certify compliance with the order. The defendant issued the compliance certification in spite of having more than 1,400 backup tapes containing data not yet processed or produced. The trial court granted the motion for an adverse inference instruction and ordered the defendant to continue complying with an early discovery order and to pay costs associated with the plaintiff’s motion after finding that the plaintiff did not receive relevant e-mail. The trial court noted, “[t]he conclusion is inescapable that [the defendant] sought to thwart discovery.” The trial court also noted that the defendant “gave no thought

Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc., 955S0.2d1124 (Fla. App. 4th Dist., 2007). The defendant appealed the decision of the trial court and the state appellate court reversed the $1.58 billion judgment against the defendant upon the grounds that the plaintiff failed to prove compensatory damages, and the court held that the jury must not speculate as to the stock value. The $1.58 billion award stemmed from the court’s jury instruction sanction that made the jury aware of the defendant’s attempt to “thwart” e-mail discovery. The court reversed both the compensatory and punitive damage awards and remanded the case to enter judgment for Morgan Stanley.

2. Court Upholds Discovery Order Classifying Data Stored in RAM as Discoverable

Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007). In this copyright infringement litigation, the defendant sought review of a magistrate’s order requiring production of server log data stored in random access memory (RAM). The defendant argued that data stored in RAM is too ephemeral and temporary to be considered electronically stored information (ESI) within the meaning of Fed. R. Civ. P. 34(a). Citing the Advisory Committee Notes to the Rules, the court explained that Fed. R. Civ. P. 34(a) was to be read expansively and denied the motion. Responding to concerns about the potential impact of the decision with respect to individual and business record-keeping obligations, the court held the decision was limited to the defendant in this case, who, only after the issuance of a court order, was obligated to preserve and produce the server log data.

3. Court Orders Defendant to Restore Backup Tapes Based on Good Cause Showing

Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth., 242 F.R.D. 139 (D.D.C. 2007). In a suit alleging violations of the Americans with Disabilities Act, inter alia, the plaintiff motioned the court to order the defendant to restore and search backup tapes for discoverable information. The plaintiff claimed discovery of the backup tapes was necessary because the defendant’s e-mail system was programmed to
automatically delete all e-mail after sixty days, and the defendant did nothing to stop the obliteration since the filing of the lawsuit, over three years earlier. The defendant argued that such an order would create undue burden and expense, and that there was little reason to suppose that the backup tapes would produce relevant information. The court granted the plaintiff’s motion, noting that while, “the newly amended Federal Rules of Civil Procedure initially relieve a party from producing electronically stored information that is not reasonably accessible because of undue burden and cost, I am anything but certain that I should permit a party who has failed to preserve accessible information without cause to then complain about the inaccessibility of the only electronically stored information that remains.” The court also ordered the parties to meet and confer to reach an agreement as to how the backup tape restoration, search, review, and production would be conducted. The court suggested concept searching as opposed to keyword searching as a more efficient search method, likely to produce more results.

4. Court Refuses to Allow Defendant to Take Advantage of Rule 37(f) Safe Harbor Clause When Party Failed to Act Affirmatively to Prevent System from Destroying or Altering Information

*Doe v. Norwalk Cnty. Coll.*, 248 F.R.D. 372 (D. Conn. 2007). In this suit brought under Title IX of the Education Amendments of 1972, the plaintiff moved the court to sanction the defendants for discovery misconduct and spoliation of evidence. The plaintiff claimed that the defendants scrubbed or wiped the hard drives of relevant individuals and altered, destroyed, or filtered relevant data. For example, one witness’s e-mail PST file contained no deleted items and only one sent item. The defendants argued that their production was sufficient. The defendants further argued that scrubbing hard drives was their normal business practice, and therefore they should be protected by the safe harbor of Federal Rule of Civil Procedure 37(f). The court held that in order to take advantage of the good faith exception in the new FRCP, a party needs to act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business. As the defendants failed to suspend their destruction process at any time and such destruction was not due to the routine operation of the information system, the court found the plaintiff was entitled to an adverse
jury instruction with respect to the destroyed evidence as well as reimbursement for costs associated with filing the motion.  
Note: Rule 37(f) was amended in December 1, 2007, and is now 37(e).

5. **Court Orders Parties to Meet and Confer Regarding Scope of Discovery and Privilege Issues, Cautioning Reasonable Pre-Production Review Is Not Excused by Negotiated Non-Waiver Agreements**

*Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005). In this race discrimination case, the plaintiffs filed a motion to compel hard copy and electronic records. The defendants claimed undue burden and expense based in part on concerns regarding pre-production privilege review. Referencing the proposed amendments to the Federal Rules of Civil Procedure, the court declared that both parties had a duty to negotiate a reasonable discovery plan and present it to the court. The court asserted, “The days when the requesting party can expect to ‘get it all’ . . . are long gone. . . . [I]t is incumbent upon the [requesting party] to have reasonable expectations as to what should be produced by the [responding party].” Accordingly, the court ordered the parties to meet and confer within thirty days regarding electronic discovery issues, including the scope of discovery and privilege review both pre- and post-production. The court noted that efforts to guard against privilege waiver “often become more acute when discovery of electronically stored information is sought” as the “volume of the information and the forms in which it is stored make privilege determinations more difficult and privilege review correspondingly more expensive and time-consuming . . . .” The court cautioned that a negotiated non-waiver agreement would not excuse parties from undertaking any preproduction privilege review, or doing less pre-production review than was reasonable under the circumstances.  
Note: *Hopson* was decided prior to the passage of Federal Rule of Evidence 502, which permits courts to grant orders regarding privilege waivers that are binding on third parties and subsequent proceedings and permits parties to enter into privilege agreements that are binding on themselves. The effect, if any, of Rule 502 on the issue of non-waiver agreements has not been flushed out by the courts yet at the time of the printing of this text.

6. **Magistrate Judge Finds E-Mail Exhibits Inadmissible and Outlines Standards for Electronic Evidence Admissibility**
In this action, the plaintiffs brought suit to enforce an arbitrator’s award determining that damages to their yacht were the result of a lightning strike and motioned the court to award a judgment of $36,000. The defendant’s insurer counterclaimed, seeking to enforce part of the arbitrator’s award that concluded that damages were limited to $14,100. In support of their cross-motions for summary judgment, both parties offered copies of e-mail as parol evidence that were attached as exhibits to the summary judgment motions. The Magistrate Judge determined that the copies of e-mail were not authenticated properly and thus both parties had failed to support their motions with admissible evidence as required by the Federal Rules of Evidence. The Magistrate Judge stated the admissibility of ESI as evidence is determined by “a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence.” The Magistrate Judge stated that for electronically stored information to be admitted into evidence it must be: (1) relevant, (2) authentic, (3) not hearsay or admissible hearsay, (4) the “best evidence,” and (5) not unduly prejudicial. Addressing the first issue, the Magistrate Judge found the parties’ e-mail exhibits were relevant to the suit. However, both parties failed to authenticate the e-mail as they were simply attached as exhibits; the “complete absence of authentication stripped the exhibits of any evidentiary value because the Court could not consider them as evidentiary facts.” Lastly, the Magistrate Judge found that the parties failed to address the last three hurdles of admissibility; the parties did not resolve any potential hearsay issues, did not comply with the original writing requirement, and did not demonstrate the absence of unfair prejudice. The Magistrate Judge explained the legal standard for each admissibility hurdle before cautioning, “it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, [and] counsel should know how to get it right on the first try.” The Magistrate Judge dismissed both parties’ summary judgment motions without prejudice to allow resubmission with proper evidentiary support.

7. **Magistrate Judge Determines Scope of Backup Tape Search and Cost-Shifting Dependent on Results of Data Sampling**

*McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001). In this employment sexual harassment litigation, the plaintiff sought to force the defendant to search its backup tape system for data that
was deleted by the user. The defendant argued that the remote possibility of yielding relevant evidence could not justify the costs involved. The Magistrate Judge noted the complicated questions presented and lack of precedential guidance governing the production of backup tapes and cost-shifting. The Magistrate Judge stated, “The more likely it is that the backup tapes contain information that is relevant to a claim or defense, the fairer it is that the [responding party] search at its own expense. The less likely it is, the more unjust it would be to make the [responding party] search at its own expense.” Instead of ordering recovery and production of relevant documents from all of the existing backup tapes, the Magistrate Judge ordered the defendant to restore and produce responsive e-mail from one individual’s computer over a one year period. After this sample data was produced and accessed, the Magistrate Judge stated he would permit the parties to argue whether a broader search is warranted given the burden and expense.

8. **Court Grants Sanctions for Party’s Failure to Preserve Electronic Documents or Engage in Discovery Process**

   *Metropolitan Opera Assoc., Inc. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003).* In this labor litigation, the plaintiff filed a motion for judgment and attorneys fees. The court granted the plaintiff’s motion for severe sanctions including a finding of the defendants’ liability and attorneys’ fees necessitated by the discovery abuses.

The court found that lesser sanctions, such as an adverse inference or preclusion, would not be effective in this case “because it is impossible to know what the [plaintiff] would have found if the [defendants] and its counsel had complied with their discovery obligations from the commencement of the action.” Noting the extent of the discovery abuses, the court stated, “both the [defendants’] lawyers and the [defendants] exhibited utter and complete disregard for the rules of the truth-seeking process in civil discovery.” Specifically, the court noted that the defendant “failed to search for and produce documents and, indeed destroyed evidence . . . .” Moreover, the court noted that the defendant’s counsel failed to meet their duty to make discovery responses based “upon reasonably inquiry under the circumstances.” Specifically, the court stated, “[C]ounsel (1) never gave adequate instructions to their clients about the clients’ overall discovery obligations . . . .; (2) knew the [defendant] to have no document retention or filing systems and yet never implemented a systematic procedure for
document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who . . . did not even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had ‘establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests,’ . . . . . and (5) in the face of the [plaintiff’s] persistent questioning and showings that the production was faulty and incomplete, ridiculed the inquiries, failed to take any action to remedy the situation or supplement the demonstrably false responses . . . and, instead, made repeated, baseless representations that all documents had been produced.”

9. **Court Finds Self-Defense Exception to Attorney-Client Privilege Applies and Allows Attorneys to Fully Defend Themselves Against Individual Sanctions for Spoliation**

*Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 638108 (S.D.Cal Mar. 5, 2008). In this underlying patent infringement case, cross examination of the plaintiff’s witness revealed over 200,000 pages of undisclosed relevant e-mail during one of the last days of trial. The court, displeased with the “organized program of litigation misconduct,” ordered the plaintiff’s counsel to show cause as to why individual sanctions should not be imposed against the attorneys. The attorneys filed a motion shortly thereafter seeking application of the federal common law self-defense exception that would have allowed disclosure of attorney-client privileged information at the hearing. On January 7, 2008, the Magistrate Judge denied the motion and this appeal followed. The Senior District Court Judge, Rudi M. Brewster, vacated the trial court’s decision as violating the due process rights of the attorneys to fully defend themselves and found the self-defense exception to apply.

10. **Court Remands Motion for Sanctions Back to Trial Court**

*Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002). The defendants appeal the trial court’s denial of the defendants’ motion for sanctions, specifically in the form of an adverse jury instruction, for the plaintiff’s failure to produce e-mail in time for trial. The Second Circuit held that where a party breaches a discovery obligation by failing to produce evidence, the trial court has broad discretion in fashioning an appropriate sanction, including the discretion to delay the start
of a trial, to declare a mistrial, or to issue an adverse inference instruction. Sanctions may be imposed where a party has not only acted in bad faith or gross negligence, but also through ordinary negligence. Vacating the trial court’s sanctions order, the circuit court reversed and remanded with instructions for a renewed hearing on discovery sanctions.

11. **Court Refuses to Issue Sanctions Where Party Fails to Establish Relevance of Destroyed Evidence, But Orders Restoration and Search of Additional Backup Tapes**

*Treppel v. Biovail Corp.*, 249 F.R.D. 111 (S.D.N.Y. 2008). In this defamation suit involving numerous ongoing discovery conflicts, the plaintiff moved the court to compel production of additional electronic information and for sanctions for failure to preserve evidence. The plaintiff sought restoration and search of all backup tapes from two servers and one employee’s laptop, arguing that the defendant’s search was insufficient and possibly overlooked relevant data. The defendant argued its recovery and search of the December 2003 and March 2005 backups was sufficient as the events giving rise to the litigation occurred in the spring of 2002 and the complaint was filed in May 2003. For the most part, the court agreed with the defendant that the likelihood of finding additional relevant documents was exceedingly remote and therefore held that the burden outweighed the likely benefit. However, the court ordered restoration and search of one e-mail server for three specific days as well as two separate backups of another file server and e-mail server.

12. **Court Finds Voluntary Production of Privileged ESI Constitutes a Waiver and Provides Suggestions for Avoiding Inadvertent Waiver**

*Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D. Md. 2008). In this copyright infringement case, the plaintiff sought a ruling that 165 electronic attorney-client privileged and work-product protected documents produced in discovery were discoverable. The plaintiff claimed privilege was waived because the defendants failed to conduct a reasonable privilege review prior to production. The defendants claimed the waiver of privilege was inadvertent, since they conducted a reasonable search using seventy keyword search terms to review potentially discoverable documents. Noting “all keyword searches are not created equal”, the court used the intermediate test mentioned in *Hopson v. Mayor and City Council of Baltimore* balancing several factors to determine
whether the waiver of privilege was inadvertent. Determining the defendants did not take reasonable precautions to prevent inadvertent disclosure, the court found the defendants waived their privilege. Additionally, the court noted several measures could have helped prevent this waiver, including the usage of a clawback (or other non-waiver) agreement the defendants voluntarily abandoned and/or complying with the Sedona Conference Best Practices for use of search and information retrieval.

13. **Court Orders Native Production of Excel Spreadsheets Despite Lack of Specific Request for Metadata But Denied Motion to Order Native Production of E-Mail Based on Pre-Trial Party Agreement**

*Williams v. Sprint/United Mgmt Co.*, 230 F.R.D. 640 (D. Kan. 2005). In this employment discrimination class action, parties had several disputes over production of metadata. In an early dispute, the plaintiffs objected to the redacted form in which the defendant had produced Microsoft Excel spreadsheets and requested native production of the spreadsheets so they would be able to determine if the documents “had any actual other columns or types of information available on a spreadsheet.” Moreover, the defendant had locked certain cells and data in the spreadsheets, thus preventing the plaintiffs from accessing those cells. The court ordered the defendant to show cause why it should not produce the spreadsheets in native format and why it should not be sanctioned for its behavior. The defendant argued that the plaintiffs never requested production of the metadata and claimed the metadata was irrelevant and contained privileged information. Although the court did not sanction the defendant, it ordered the defendant to produce the spreadsheets’ metadata and to produce “unlocked” versions of those spreadsheets. The court held, “when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.”

*Williams v. Sprint/United Mgmt Co.*, 2006 WL 3691604 (D. Kan. Dec. 12, 2006). In a discovery dispute more than a year later, the plaintiffs moved the court for native production of e-mail that had been previously produced by the defendant in a hardcopy format. In the original production, the e-mail
had spreadsheets that were detached and provided as separate documents in their native, electronic format. Without the native e-mail, the plaintiff was forced to match the hardcopy e-mail with the corresponding electronic spreadsheet attachment using a correlation table, causing the plaintiff to incur more time and expense. The defendant countered that the parties agreed during pre-trial conferences that any e-discovery would be produced as TIFF images and not in a native file format. Furthermore, producing native e-mail files would increase the risk of privileged information being disclosed since native files cannot be redacted. The court reasoned that the prior production of e-mails was not a deliberate attempt by the defendant but the result of an agreement between the parties. The court held the plaintiffs failed to give an adequate reason to compel the native e-mail production and denied their motions to produce native e-mail files.

14. **Court Orders Forensic Search and Production of Missing E-Mail and Denies Cost-Shifting Argument Citing Responding Party’s Insufficient Discovery Efforts that Caused Need for Forensic Investigation**

*Peskoff v. Faber,* 2006 WL 1933483 (D.D.C. July 11, 2006). In this contract litigation, the parties engaged in a prolonged discovery dispute over production of e-mail. The plaintiff first brought a motion to compel the defendant to produce additional e-mails written by or addressed to the plaintiff while employed by the defendant. During discovery, the defendant produced computer disks that the defendant asserted contained “all [plaintiff’s] electronic files, including documents stored on his computer hard drive, e-mail, and any other [plaintiff] electronic documents.” However, the production did not include two years worth of e-mail received or authored by the plaintiff from mid-2001 through mid-2003. The plaintiff argued the defendant failed to adequately explain the missing e-mail. Countering, the defendant maintained no documents had been withheld, and if any e-mail was missing, the e-mail no longer existed. The court observed there were several possible locations where the missing e-mail could be located, including: the plaintiff’s work e-mail account, other employee accounts, the hard drives of company computers, and on backup tapes from a law firm’s server where the defendant stores its electronic files. The court ordered the defendant to provide a detailed affidavit specifying the nature of the search the defendant conducted in locating the responsive e-mail. The court further ruled the plaintiff
would then have ten days to respond to the adequacy of the search described in the affidavit, and at that point the court would consider whether additional searches were necessary.

*Peskoff v. Faber*, 240 F.R.D. 26 (D.D.C. Feb. 21, 2007). The plaintiff again moved the court to compel discovery of the missing e-mail seven months later. The plaintiff argued that the two year time gap in e-mail produced suggested a complete and accurate search was not conducted by the defendant. The defendant argued that he would be willing to submit his hard drive for imaging by the plaintiff, but that he would not endure the costs of production. After supplemental submissions by the parties regarding the extent of the search, the court determined the defendant only searched two of the five places where e-mail evidence may be found and that this was not a sufficient search. The court ordered: (1) the defendant “to conduct an additional search all depositories of electronic information in which one could reasonably expect to find” e-mail containing the plaintiff’s name; (2) the defendant to file a statement under oath by the person who conducted the additional search regarding the search methodology; and (3) an evidentiary hearing. The court further ruled that the defendant must endure the costs of production contained on his hard drive, citing the newly amended Federal Rules of Civil Procedure. The court stated that accessible data must be produced at the cost of the producing party and that “cost-shifting does not even become a possibility unless there is first a showing of inaccessibility.”

*Peskoff v. Faber*, 244 F.R.D. 54 (D.D.C. 2007). The court considered, in a follow up order to the plaintiff’s motion to compel, the adequacy of the defendant’s search for the missing e-mail. The court noted that the defendant failed to appear at the evidentiary hearing and failed to submit a statement under oath by the person who conducted the additional search that was previously ordered. The defendant’s attorney submitted an affidavit stating the defendant “separately searched his files and produced responsive documents and electronic mail.” The defendant’s counsel continued to insist that any e-mail not already produced was no longer in existence. The court ordered the parties to seek estimates from “qualified forensic computer technicians to perform an examination” for a search of the relevant computers and network server and production in TIFF or PDF format to determine the importance of the discovery to the issue in the litigation.
After the previous ruling, both parties submitted a joint bid resulting in a vendor proposal of $33,000. Determining the forensic examination was justified, the court considered whether the burden or expense justified a shift of cost to the requesting party. Finding the defendant’s inadequate search efforts, failure to preserve electronically stored information, and overall unwillingness to take “discovery obligations seriously” caused the need for a forensic examination, the court refused to shift costs since the problem was one of the defendant’s “own making.”

Court Issues a Series of Landmark Decisions in Ongoing Saga over Production of E-Mail That Creates Gold Standard Seven Factor Cost-Shifting Test, Illuminates Preservation Duties and Appropriateness of Sanctions, and Provide Guidelines Regarding Counsel’s Duties in Electronic Discovery

In this gender employment discrimination lawsuit against her former employer, the plaintiff requested that the defendant produce “[a]ll documents concerning any communication by or between UBS employees concerning the plaintiff.” The defendant produced 350 pages of documents, including approximately 100 pages of e-mail. The plaintiff knew that additional responsive e-mail existed that the defendant had failed to produce because she, in fact, had produced approximately 450 pages of e-mail correspondence. She requested that the defendants produce the e-mail from archival media. Claiming undue burden and expense, the defendant urged the court to shift the cost of production to the plaintiff, citing the *Rowe* decision. Stating that a court should consider cost-shifting only when electronic data is relatively inaccessible (such as in this case), the court considered the *Rowe* eight-factor cost shifting test. The court noted that the application of the *Rowe* factors may inappropriately result in disproportionate cost shifting away from large defendants, and the court modified the test to the following seven factors: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issue at stake in the litigation; and (7) the relative benefits to
the parties of obtaining the information. The court ordered the
defendant to produce, at its own expense, all responsive e-mail
existing on its optical disks, active servers, and five backup
tapes as selected by the plaintiff. The court determined that
only after the contents of the backup tapes are reviewed and
the defendant’s costs are quantified will the court conduct the
appropriate cost-shifting analysis.

In the restoration effort that occurred according to previous
e-discovery decisions in the matter, the parties discovered that
certain backup tapes were missing and that e-mails had been
deleted. The plaintiff moved for evidentiary and monetary
sanctions against the defendant for its failure to preserve the
missing tapes and e-mails. The court found that the defendant
had a duty to preserve the missing evidence, since it should
have known that the e-mails may be relevant to future litiga-
tion. Although the plaintiff did not file her charges until August
2001, by April of that year, “almost everyone associated with
Zubulake recognized the possibility that she might sue,” the
court wrote. The court also found that the defendant failed to
comply with its own retention policy, which would have pre-
served the missing evidence. The judge found that although
the defendant had a duty to preserve all of the backup tapes
at issue, and destroyed them with the requisite culpability, the
plaintiff could not demonstrate that the lost evidence would
have supported her claims. Therefore, it was inappropriate to
give an adverse inference instruction to the jury. Even though
an adverse inference instruction was not warranted, the court
ordered the defendant to bear the plaintiff’s costs for re-depos-
ing certain witnesses for the limited purpose of inquiring into
the destruction of electronic evidence and any newly discov-
ered e-mails.

The plaintiff contended in this current motion that the defend-
ant, who recovered some of the deleted relevant e-mails, prej-
udiced her case by producing recovered e-mails long after the
initial document requests. Furthermore, some of the e-mails
were never produced, including an e-mail that pertained to a
relevant conversation about the employee. As such, the plain-
tiff requested sanctions in the form of an adverse inference
jury instruction. Determining that the defendant had willfully
deleted relevant e-mails despite contrary court orders, the
court granted the motion for sanctions and also ordered the
defendant to pay costs. The court further noted that defense counsel was partly to blame for the document destruction because it had failed in its duty to locate relevant information, to preserve that information, and to timely produce that information. In addressing the role of counsel in litigation generally, the court stated that “[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.” Specifically, the court concluded that attorneys are obligated to ensure all relevant documents are discovered, retained, and produced. Additionally, the court declared that litigators must guarantee that identified relevant documents are preserved by placing a “litigation hold” on the documents, communicating the need to preserve them, and arranging for safeguarding of relevant archival media. See also Zubulake v. UBS Warburg, LLC, 231 F.R.D. 159 (S.D.N.Y. 2005) (denying employer’s motion to assert an affirmative defense based on the delay in asserting the defense and the prejudicial effects it would cause the employee in re-opening discovery).

Zubulake v. UBS Warburg LLC, 382 F. Supp. 2d 536 (S.D.N.Y. 2005). The defendants moved in the instant motion to preclude various pieces of information from evidence at trial, including the court’s first five opinions relating to its deficient discovery. The defendants argued the earlier decisions – which included the court’s award of electronic discovery spoliation sanctions against the defendants – were irrelevant and unfairly prejudicial. The court agreed, noting “jurors will be told all they need to know through the evidence admitted at trial and my charge.” The defendants also requested preclusion of discovery correspondence among defense counsel and evidence relating to its failure to preserve monthly backup tapes. The court determined the plaintiff would be allowed to introduce this evidence only if the defendants opened the door by offering evidence regarding the reasonableness of their actions. Finally, the plaintiff indicated that she intended to elicit testimony from defendants’ counsel relating to its client’s e-mail and backup tapes preservation practices. The defendants sought preclusion of defense counsel testimony and argued the testimony would be cumulative since the defendants had already produced information relating to their document retention policy. The court granted the motion, stating it did “not see any legitimate need plaintiff may have for calling
opposing counsel given the extensive discovery on the issue of
\textit{e-mail and back-up tape preservation and retention}.”

As you can see after reading this top fifteen list, the legal issues
surrounding electronic discovery run the gamut of the discovery
process from retention to production, as fully discussed in chapter
three. All of these important concepts and developments can be sum-
marized in three important legal points. First, the discovery process
is supposed to be accomplished cooperatively between parties with
minimal judicial intervention. The amended Federal Rules of Civil
Procedure emphasize this discovery goal and seek to accomplish it by
requiring a more thorough discussion of discovery issues, explicitly
including issues related to ESI at meet and confer conferences prior to
the scheduling conference with the court. Second, all the statutory and
case law pertaining to discovery in general applies with equal force
to e-discovery unless it is expressly distinguished by more specific
law. Third, the law will continue to evolve as the manner in which
electronic discovery and computer forensic technologies continues to
advance. Practitioners must stay informed regarding the relevant law
and applicable technologies, as well as understanding how they inter-
act and will likely continue to develop in tandem.

\textbf{THE CURRENT STATE OF ELECTRONIC DISCOVERY
TECHNOLOGIES}

The purpose of electronic discovery technologies is to bring down the
total cost of litigation by adding efficiency to the discovery process.
Treating electronic discovery the same as traditional paper discovery
of yesteryear makes no sense when you consider the unique charac-
teristics of ESI that are fundamentally different from paper evidence,
and is at best extremely inefficient. Fortunately, e-discovery tech-
ologies have developed to efficiently address the unique nature of
ESI. Namely, e-discovery technologies exist that provide solutions to
tackle electronically stored information’s colossal volume, potential
inaccessibility, and dynamic nature.

The volume of ESI in existence dwarfs the volume of paper docu-
ments in existence, resulting in part, from the increased level of commu-
nication in which our modern society engages, the ease of creating ESI,
and the ease with which ESI is stored in perpetuity. In illustration, the
parties in a recent case recognized that discovery of ESI would be mas-
sive, resulting in the defendants’ production, presumably if produced
in paper format, “somewhere in the neighborhood of a pile 137 miles

The advent of e-discovery technologies allows practitioners to narrow the volume of data that needs to be included in the review set. Review is widely recognized as the most expensive part of discovery and, indeed litigation. For every dollar spent on filtering and processing electronic documents prior to review, approximately three to five dollars would be spent on review. For an example of how technology can cost-effectively assist in discovery, non-responsive documents as well as some privileged documents can be culled from the review document set through keyword searches, concept searches, de-duplication, removal of blank pages, removal of documents outside a relevant data range, etc. Furthermore, e-mail analytics tools can be used to analyze information early in the discovery process to make decisions on whether information should be excluded from the discovery process or included for further analysis of relevancy. These technologies can assist you in reducing volume, thus exponentially reducing costs associated with review and production, and are further discussed in chapter four.

Further complicating this increased volume of information is the fact that data is frequently being stored in an increasingly diverse number of formats and locations (e.g. backup tapes, online, hard drives, etc.) that can be difficult and costly to retrieve. The common law and Federal Rules of Civil Procedure have recognized that some evidence that is not reasonably accessible can be unduly burdensome to produce and is thus not discoverable. However, even evidence that is damaged or located in a format that requires significant technological efforts to retrieve can be deemed reasonably accessible, depending on the relative importance of the information sought. The available technologies to retrieve information are discussed in chapters four and five and the legal principles governing reasonable accessibility limitations to discovery are discussed in chapter three.

Another characteristic of ESI that is absent in paper documents is the existence of metadata. Metadata is “data about data,” such as information regarding the document’s creation, author, modification, size, last access date, etc. This information is automatically saved with the computer document by the applications that create the metadata. Metadata is discoverable and must be preserved when a litigation hold is triggered. Unfortunately, metadata is fragile and can be altered inadvertently by merely booting a computer system or opening a file. Thankfully, e-discovery and computer forensics best practices and technologies exist that can ensure preservation obligations are met. It is against the backdrop of sanctions for spoliation of evidence that these technologies and processes have developed to ensure electronic
In conclusion, e-discovery and computer forensics technologies are essential to fulfilling legal discovery requirements in a cost-effective manner during each stage of the discovery process: storage and retention, collection, filtering, processing, review, and production. Quite simply, a failure to utilize e-discovery and computer forensics technologies, when appropriate, is increasingly being seen as falling below acceptable standards of competent legal practice. As stated in a relatively early e-discovery case, “At some point, a party and/or its attorneys must be held responsible for knowing what documents are discoverable and where to find them.” Danis v. USN Commc’ns, 2000 WL 1694325 (N.D. Ill Oct. 23, 2000).

THE CURRENT STATE OF THE E-DISCOVERY INDUSTRY

Amidst all of the changes in the law and technology, the marketplace of service providers is also quickly coming of age. Five years ago when we published the first edition of this book, we listed the name of every e-discovery and computer forensics provider we could unearth. As with the maturation of any industry, many of those e-discovery providers have since gone out of business or merged into a different entity. In addition, hundreds more new providers have emerged on the scene. Today, we cannot list every player influencing the development of e-discovery and computer forensics law, technologies, or practices as there are literally hundreds. Perhaps even more indicative of the maturity of the industry than the number of players is the diverse variety of players in the industry, which can be subdivided as follows:

- Service providers (e.g., e-discovery vendors/consultants, computer forensics experts, software companies, document management consultants, ESI consultants, etc.);
- Think tanks and researchers (e.g., The Sedona Conference®, Gartner®, EddixSM, Socha-Gelbman Electronic Discovery Reference Model (EDRM), etc.);
- Tech-savvy judges;
- Lawyers, litigation support professionals, paralegals, and IT staff members with e-discovery responsibilities.

Within each of the categories of players in the e-discovery industry, there are a variety of strengths and weaknesses. There are providers that perform like economy cars, and there are high-end players that perform like luxury vehicles. Although there is a plethora of marketing material available to tell you whom to hire, we are not going to take the
approach of comparing apples and oranges amongst the multitude of diverse providers available. Rather, the best approach when selecting a service provider or choosing to perform work in-house or in-firm is to consider your ultimate objective and your needs in relation to the expert. There are, however, several factors that should always be considered when selecting and working with an expert. These factors are discussed in chapter four with regard to e-discovery experts and chapter five with regard to computer forensic experts.

CONCLUSION

The development of e-discovery law and technologies may be uncharted waters for you, but rest assured that there is no need to face e-discovery with trepidation. The general purpose of discovery is the same as it has always been—to exchange information fairly with your opponent to provide the information necessary to effectively advocate for your client, and visa versa. The advent of electronically stored information has merely caused the rulebook to evolve to necessarily accommodate its unique characteristics.

Courts expect attorneys to understand the burden, expense, and process associated with electronic discovery, and to have the ability to preserve, locate, and produce relevant ESI. This expectation necessitates an understanding of the governing law and applicable technologies, but does not necessitate becoming an e-discovery expert. This book can effectively serve as your guide as you navigate the waters of electronic discovery. There are also many experienced experts available who have the expertise to assist you through every step of the electronic discovery process. In the final analysis, take control of your discovery practice and captain your way to a successful litigation outcome by familiarizing yourself with and utilizing the information contained in this guidebook.