CHAPTER 1

Introduction

Chapter Contents

---

§ 1.01 Background

[1]—The Emergence of Modern Discovery Practices

In the latter half of the 20th century, civil litigation in American courts moved toward a new environment of broad discovery, which was championed by the federal courts and embodied in several major revisions to the Federal Rules of Civil Procedure. Civil litigation essentially moved from the "gamesmanship" mode of trial by ambush, with the norm being little or no discovery, to an environment in which "hide-the-ball" litigation tactics were no longer permissible.

During this same period, the volume of paper records maintained by American businesses expanded exponentially, based primarily on the development and rapid adoption of new technology such as mimeograph machines and photocopiers that made copying docu-

ments easy and economical. As this large volume of paper records continued to expand, businesses developed methods to gather and store these materials, such as off-site archival records facilities created by outsourcing vendors.

Not surprisingly, this growing volume of paper records considerably increased the burden imposed by the new "open discovery" environment for litigation. A breach of contract action might no longer focus solely on the terms of the paper original that was executed by the parties. Instead, discovery could require a search of old files for copies of the many drafts exchanged between the parties during the negotiation process, which might entail a search of files not only at the company headquarters, but also files maintained by off-site vendors or outside counsel. As the complexity of the litigation increased, the paper records search likewise increased, frequently in an exponential manner. Large teams would need to be assembled to identify, gather and review these voluminous records, created by numerous employees of the vast corporate enterprise, for responsiveness. The concept of "burdensomeness" as an objection to otherwise permissible discovery developed in parallel, and soon litigants relied on boilerplate objections of "undue burden" when responding to all types of discovery requests. All of this, of course, preceded the realm of electronic records and discovery, which has magnified the concept of "burdensomeness" several-fold.

[2]—Recognition of the Universe of Electronic Records

In the last decade of the 20th century, trial lawyers and courts began to grasp the fundamental changes in the nature of discovery following the digital revolution of e-mail, the World Wide Web, and the universal shift toward electronic data systems for managing financial and business information, whether it be a "mom and pop" family business or a vast global enterprise. During this period, some of the largest global corporations announced long-range plans to shift toward "paperless" business records systems, in which all information retained by the businesses would be in the form of electronically stored records. The data used for daily operations, such as purchase orders, sales reports, insurance claims, personnel records, and other routine "paperwork," would be inputted using electronic form templates employed throughout the company, based on extranets and other network systems, and feed directly into the company's main database systems. This would help avoid the need for recipients to retype information from paper forms into local records systems, or to maintain large internal mail distribution networks and paper archival systems in place.

Despite all these widely announced moves toward a paperless business environment, however, lawyers who focused on litigation often

seemed blissfully ignorant or unconcerned about this trend. As a result, the 1990s was an era when a great many practitioners appeared to be completely unaware of the potential scope of electronic discovery in their clients' litigation matters, and their duties with regard to preserving and producing electronic documents. Many litigators never bothered to search for electronic records when responding to ordinary discovery requests, and similarly never bothered specifically to request them from their opponents. E-mail in particular was rarely searched for or produced, unless an employee had printed the message and saved it in his or her personal files. Likewise, the vast majority of litigators produced electronic data such as financial statement information only in printed paper form, even when it was necessary to open an electronic spreadsheet stored on a computer in order to print the copy required.

Prior to the beginning of the new millennium, the concept of attempting to search for and retrieve stored electronic data on any broad scale could not be imagined by the typical trial lawyer or in-house counsel except in the rarest of instances. When a party was actually confronted with a specific request for electronic records by an e-savvy trial lawyer, the common refrain of "undue burden" reared its head once again in response. In most cases, this objection of "burdensomeness" was raised before any attorney had even taken the time to attempt to estimate the volume of electronic records at issue, or the difficulty that would be encountered in retrieving or reviewing them. More important, in all too many cases the trial lawyers raising these objections failed to consider whether the electronic records that were sought might actually be *helpful* in their own defense or the prosecution of their own claims.

During this same period in the 1990s, it was not unusual to see in-house counsel or IT department employees signing affidavits in support of objections to electronic discovery, attesting to the sheer impossibility of identifying or retrieving relevant documents, based on various claimed shortfalls in the party's electronic data systems. In many instances, however, these affidavits were based on woefully inadequate knowledge of the computer records systems at issue, or the party's own procedures and actual practices for maintaining back-up tapes or retrieving information when required by management in the ordinary course of business. At the same time, trial courts ranged widely in their experience and attitudes toward electronic discovery. Trial judges with little knowledge of computer systems frequently accepted claims of "undue burden" and limited discovery of electronic records. In other instances, the trial judge might order production of information stored in electronic formats, but only in printed paper form, rather than the original electronic form. This, of course, essentially shifted significant costs for managing and utilizing this

information to the requesting party (while simultaneously adding to the cost for the producing party, which typically did not complain).

[3]—Navigating the Shoals of Electronic Discovery Only by "Dead-Reckoning"

One major hurdle in the early years of electronic discovery was the lack of any authoritative rules or guidance from the judicial system on the rights and duties of parties with respect to electronic data. As the new millennium approached, even trial lawyers and in-house counsel who were savvy about electronic record systems and wanted to fulfill their discovery obligations with respect to electronic data found it difficult to discern the true scope of those obligations. The only universally accepted principle guiding electronic discovery was the need to be "reasonable" in both requests and responses or objections, just as with all other types of discovery, but there was no agreement about what that term means. And when it comes to electronic discovery, parties typically have radically different views as to what might be considered "reasonable" to search for and produce, particularly when the burden falls primarily (or entirely) on only one party.

For example, in the area of class action litigation over consumer goods and services, securities or antitrust disputes, the burden of responding to electronic discovery generally falls almost exclusively on the corporate defendants, because individual consumers or shareholders who serve as class representatives likely have few electronic records related to any issues in the case. This, not surprisingly, leads to demands by plaintiff attorneys who represent a class or putative class for vast electronic records searches that favor their side and impose tremendous cost and administrative burdens on the defendants. Indeed, an attorney's desire to press for electronic discovery often is motivated by a hope that his opponents will not have taken adequate steps to preserve or search for electronic records, which can put the opponents in jeopardy of having sanctions imposed (including default judgments or limitations on introducing evidence) that ultimately force a settlement based on procedural discovery errors rather than on the substantive merits of the case.

In contrast, in a commercial dispute between two large business entities with relatively equal potential burdens related to electronic discovery, counsel for the parties often exercise considerable restraint when demanding electronic records from their opponents. This simply reflects the recognition that their own client will likely disfavor having to undertake massive electronic records searches from its own systems.

This uncertainty about the scope of electronic discovery obligations in the 1990s was exacerbated by the drastic shortage of reported decisions providing guidance on the meaning of the term "reason-

able" in the context of electronic records. Most discovery disputes of any kind arise and are resolved in the trial court, with few such disputes ever reaching an appellate court for consideration. Discovery rulings in most trial courts typically are resolved by brief orders either granting or denying a discovery motion, even in federal courts whose written decisions are generally available today from electronic reporting services such as Lexis/Nexis or Westlaw. This left practitioners without written rulings describing the factual circumstances of particular electronic discovery disputes and the reasoning used in reaching the trial courts' end results. In other words, practitioners facing electronic discovery disputes had to navigate by the "seats of their pants," without any compass or sextant to help guide them.

Electronic discovery battles began to emerge as trial lawyers began to recognize the importance of data mining for electronic golden nuggets. Parties that aggressively sought electronic records refused to accept "no" for an answer from their opponents, and used all the procedural tools at their disposal to obtain orders requiring electronic records production or else sanctions for failures to produce. At the same time, the volume of electronic records and the systems in which they are stored multiplied endlessly. By 2000, e-mail had become a widespread form of communication throughout the world of business and government. Use of computer record systems for storing financial data and other business records became the norm, not the exception. New forms of electronic storage systems at low cost—such as personal digital assistants (PDAs), digital cameras, cellular phones with cameras and e-messaging systems, digital voice message systems, portable hard drives, and iPods and similar digital content recorders—swept the business and consumer market.

Since the initial publication of this treatise, the federal courts have adopted a number of amendments to the Federal Rules of Civil Procedure, effective in December 2006, that reflect an initial attempt to provide more guidance to parties on their obligations related to electronic discovery. These amended rules, which are discussed throughout the remaining chapters, start by imposing new terminology in this area, based on the concept of electronic discovery constituting the search for "electronically stored information" or "ESI." This term is broadly defined to encompass all types of electronic documents or data regardless of how stored. Nonetheless, the amended rules remain dependent on the concept of "reasonableness" as the guidepost, rather than providing a host of specific requirements stating what precisely must be produced or in what fashion.

For example, the amended federal rules differentiate between electronically stored information that is "reasonably accessible," such as information stored in online, active "databases," and information that is "not reasonably accessible," such as backup tapes that need to be

restored and loaded onto a server in order to even conduct an initial search for potentially responsive records. This lack of specificity in turn means that the scope of electronic discovery in federal courts remains uncertain in any particular case. Perhaps the most critical change is the new duty imposed by Rule 26(f)(3)(C) for the parties to address the topic of electronic discovery at the outset of the case and attempt to develop their own rules and guidelines to govern their activities related to requesting and responding to electronic discovery.

The amended federal rules also clearly impose an obligation on the parties to become familiar with their electronic records systems *in advance* of litigation so that they are in a position to discuss issues related to electronic discovery in an informed manner at the start of the case. Many large business entities that routinely face litigation have undertaken formal programs to identify and "map" their electronic records systems, ranging from large network database systems to individual personal computers or hand-held devices. This allows for better implementation of legal holds to retain potentially relevant documents at the beginning of a potential dispute and more adequately comply with businesses' document retention obligations. This type of planning also leads to identification of individuals within the company who can easily—and perhaps most accurately—describe the company's systems and be knowledgeable as to potential "accessible" and "non-accessible" electronic records collections, and the likely burden arising if searches of these collections are necessary. In addition, as part of this planning process, these companies are developing more sophisticated document retention plans that recognize the trend toward electronic records systems in preference to paper-based systems. Along with these new retention plans, these companies recognize the need to have in place more specific and detail-oriented legal hold procedures that can be easily implemented and provide the company with a better defense against accusations down the road of negligent or intentional destruction of electronically stored information.

Despite the increased attention focused on electronic discovery issues, it should be no surprise that what is "reasonable" in the context of electronic discovery still remains open to significant debate, as the later chapters of this treatise will explain in more detail. The fundamental questions at issue, however, remain the same:

> How broad a search for relevant electronic records is necessary?
>
> To what extent is a party required to attempt to retrieve and restore "deleted" documents that are not readily accessible in any existing, online records storage system?
>
> Who is required to be involved in conducting the search?

Can the requesting party be permitted to undertake its own independent search of the opponent's electronic record systems?

Who bears the cost of searching and retrieving electronic records or restoring electronic records that are "not reasonably accessible"?

What formats are required or permitted for the production of electronic records?

What standards do courts expect in-house counsel and trial lawyers to adhere to in dealing with electronic discovery?

What is the scope of the duty to supplement electronic records searches when the issues in dispute in the litigation remain ongoing?

[4]—The False Concept of "Deleted" Electronic Records

Practitioners have come to realize that true "deletion" of electronic records is a rather nebulous concept. In the world of paper records, physical deletion of a document could be achieved with certainty by shredding, burning or other means. But while everyone today is familiar with the "delete" key on his or her keyboard, achieving "deletion" of electronic records like e-mails comparable to destruction of old paper records is far more challenging. E-mail is a good example: although the individual user may "delete" a message, there is a great likelihood that a copy of that message resides on another network computer, such as the company's e-mail server, or even on computers owned by third parties. For example, copies of the e-mail may reside on servers used by outside vendors to manage e-mail communications, or on the personal computers of other recipients of the message. The latter may even routinely save such messages in "personal folders" that do not get cleansed by the routine auto-deletion processes employed by many network systems. In sum, actual "deletion" of all copies of an e-mail message is no easy task.

Whether an electronic record still exists may prove a difficult question to answer when facing a request for production of electronic records. Moreover, the danger of inadvertently deleting electronic records remains ever present, particularly in large organizations with electronic records backup procedures that have been developed by an IT department primarily for "disaster recovery" purposes and then overlooked by the in-house counsel or trial lawyers in the midst of a brewing or ongoing dispute. Most large businesses today use some form of backup system for key electronic records such as customer lists, financial data, and similar information. Over the years, the media used to store this backup data may have changed—from bulky and fragile magnetic tape to massive hard drives at data storage "farms"—but the importance of the data remains the same.

One popular method for electronic records backup that developed over time is the use of magnetic tape cassettes to store a "snap-shot" of the key record systems at month-end or some other regular interval, with reuse of the same tape cassette after a certain fixed retention period. Reuse of the cassette, of course, results in the destruction of all electronic records previously recorded on it. The simple reason for this reuse is that the business has never had any desire to capture all its electronic records and store them indefinitely. In the world of paper records, businesses routinely conduct periodic "file cleaning," if for no other reason than to provide space in the file drawers for the new records to be generated and collected during the coming year. The desire not to maintain old electronic records is no different. But there is one major difference: the *cost* of maintaining such records today is likely far less than the cost of maintaining a similar quantity of paper records, and the concept of physical limitations on storage capacity is no longer an issue. This factor complicates the document retention decision process for large companies that face ongoing litigation in the ordinary course of their business activities, and, accordingly, ongoing electronic discovery obligations to opposing parties. The old excuse of "tossing out the files" simply to ensure adequate file space for the new records to be stored in the coming year is not as readily available for electronic records.

The task of retrieving electronic records has spawned an entire new industry of electronic records management consultants and computer forensic examiners. These consultants are prepared to provide assistance in gathering and managing large volumes of electronic data, or restoring previously deleted files—often at hourly rates higher than the trial lawyers charge. In addition, the legal profession has developed an endless supply of continuing legal education seminars and conferences on electronic discovery. No reduction in these CLE offerings should be anticipated in the foreseeable future, given the nature of the problem and the ever growing awareness of the need thoroughly to understand electronic discovery practice.

[5]—Lack of Understanding of Electronic Records Generally, and Bad Habits in the Use of Electronic Communications Methods

One of the most difficult problems for employers involved in electronic discovery is the lack of understanding by the average employee of how electronic documents are stored, what they contain, and how significant they can be in any dispute. As noted earlier, it is very difficult truly to "delete" an electronic document such as an e-mail message. Many if not most people, however, appear to believe that simply hitting the "delete" key in their e-mail message application is

sufficient to make these messages disappear. This fundamental misunderstanding exacerbates the following two issues: the existence of metadata,[1] and bad habits in electronic-based communications.

Metadata are the additional information stored in electronic form that accompany many electronic documents such as a word processing document or an e-mail message. Metadata may contain such information as who has edited the document and when, what changes were made, other similar "tracking" information that accumulates as the document is worked on, and when the document has been printed. In contrast to a draft document that is handwritten on a piece of paper, and can be tossed into the "circular file" to be gotten rid of, the existence of metadata means that drafts of the electronically created document are not actually deleted. When an author circulates documents with metadata included, the recipient can frequently retrieve and examine all this information almost effortlessly. To avoid sending these data along with a file that is shared with others, the sender must use sophisticated document "scrubbing" software applications that can delete all this tag-along information, and remember to use it each time the document is shared. Without such electronic "scrubbing," the author ends up losing control over his or her ability to delete drafts and hide the editing process.

In the end, the most troubling issue with electronic discovery tends to be the bad habits of authors when drafting routine electronic messages such as e-mail. The growth and popularity of e-mail itself has led to new communications patterns and behavior at work and at home. In years past, most written business communications were prepared in relatively formal fashion, using "official" memo formats or internal communications forms. A written communication with an outside party would typically be done by letter, also in a relatively formal style. Documents drafted in a more formal style, of course, typically benefit from more thought and effort in the drafting process, as the author carefully reviews the draft and contemplates the meaning of the words being formally communicated either within or without the enterprise.

Formal communications formats unfortunately (for the litigator at least) have rapidly faded in direct proportion to the widespread adoption of "business casual" dress codes. E-mail is now the electronic communications equivalent of "business casual." As people and businesses face increasing pressure for cost-reductions and increased effi-

---

[1] The term "metadata" is here used to mean "definitional data that provides information about or documentation of other data managed within an application or environment." See http://www.hyperdictionary.com/dictionary/meta+data (last visited Aug. 10, 2005).

ciency, the "tedious" formality of business communications in the past has gone by the wayside. Only a few decades ago, a transaction such as the sale of a business would be documented by a contract that was prepared on a typewriter, using carbon paper to make the copies necessary to circulate to members of the business teams. A draft would then be dropped in the mail or sent across town by messenger, resulting in considerable delay in the negotiation process while simultaneously allowing the parties time to contemplate the transaction and carefully consider the ramifications of the terms being negotiated. All this changed with the advent of the photocopier and economical overnight delivery services, which increased the pace of negotiating transactions. Soon came the fax machine and now electronic messaging systems attaching electronic drafts of the contract. Speed is deemed to be of critical importance and value.

The emergence of personal digital assistants that can be used for the receipt and creation of e-mail is perhaps the leading contributor to the trend in informality and "quick answers" that may not be well thought out. Individuals use these devices to stay in constant communication with their business colleagues and clients. In doing so, they have to rely on small video screens and miniature keyboards that require "thumb typing" skills that engender the use of cryptic and abbreviated text messages, as well as hastily prepared comments that are done "on the fly" in automobiles, airplanes, restaurants, and other settings that in the past would not have been a place for preparing formal correspondence on important business or legal issues. The ability to forward messages or copy many additional recipients only exacerbates the problem because of the increased possibility of misdirected responses to unintended recipients, or multiple responses from many recipients who in turn prepare their responses hastily and without regard to their potential impact, and the need to explain them, at a trial many years later.

What this means is that people are sending messages and responding to messages that are drafted overwhelmingly in very informal style, and are dashing off these messages without always considering all the consequences of what they are saying. Moreover, the trend toward "business casual" has led users to express their innermost thoughts and opinions in a manner that in the past would have been reserved for a private conversation outside the hearing range of others or else a personal telephone call (without using the speakerphone option). This informality ultimately leads to recorded statements that most likely were never really intended to be repeated or reviewed by a stranger, but that can be forwarded effortlessly and surreptitiously to an unlimited audience at virtually no cost. This, in turn, leads to the proliferation of e-mail chains that ensure that there is no practical means of effectively deleting these messages, while simultaneously

resulting in a vast increase in the effort required to untangle and translate the story contained within these message strings for use at trial or otherwise.

One thing that has emerged from this trend are the oft-published examples of e-mail going to the wrong person in an embarrassing fashion, or messages that create significant liability issues based on poor word choices or unsuitable language. From this, many businesses are beginning to recognize the need to begin implementing training on "best practices" for document *creation*, and new policies on document retention and legal hold processes for electronic records. Overall, the only way to deal with this issue in the long term is to remain vigilant and provide constant reminders to employees of the need for attention to detail and restraint when using electronic messaging systems. One of the best ways to help illustrate the importance of this goal is to use examples of "blunders" by management or senior executive-level employees (either in-house or at another company) to emphasize that everyone can make mistakes, but it is best to catch them before hitting the "send" button.

[6]—The Current Electronic Discovery Landscape

Only a few years into the new millennium, the landscape of electronic discovery has changed dramatically:

- Courts have quickly begun to grasp the issues presented by electronic discovery and have responded with the development of more formal rules and published decisions.
- Trial lawyers have learned to use electronic discovery as a powerful weapon that can result in significant victories without ever having to get to the merits.
- In-house counsel have become savvy by investing the time necessary to understand their company's electronic records systems and learning how to track, retrieve, review and preserve, expeditiously and efficiently, relevant electronic documents.
- Outside counsel have learned that the duty to identify, preserve and produce relevant electronic records ultimately lies with them, which requires some modifications in the way that trial counsel has to deal with the client's in-house counsel and business management.
- A cottage industry of electronic consultants has emerged to provide a wide range of assistance to in-house and outside counsel dealing with electronic discovery issues.

§ 1.02 Electronic Discovery Issues

This book is intended to provide guidance for trial lawyers, in-house counsel, and courts that must deal with electronic discovery on a regular basis.

Chapter Two provides an overview of the rules governing electronic discovery under the Federal Rules of Civil Procedure. This is an evolving area that has undergone significant changes since the adoption of the amendments covering electronically stored information in December 2006. It is expected that there will be dramatic increases in the number of decisions by district courts in the near future as they become familiar with those amended rules and grow more confident in addressing disputes over electronic discovery. It is important to recognize that the amended rules, however, still do not distinguish between paper and electronic documents in many respects, despite considerable differences in the data captured in these two mediums. Instead, the amended Federal Rules leave the initial debate on how to address these differences to the parties as part of their overall pre-trial plan. Practitioners in state court matters need to be familiar with their own state court rules, which sometimes deal far more specifically with electronic discovery rights and duties.

Parties can benefit from careful pre-discovery planning and the use of discovery conferences based on rules such as Federal Rule of Civil Procedure 26(f) to raise common electronic discovery issues and attempt to reach agreement on the scope and timing of electronic searches and electronic document retention for the clients' ongoing businesses. It is far better to address these issues early in the case rather than ignore them until one party launches a surprise attack that sets the other party up for possible sanctions later in the case.

Chapter Two also deals with the use of protective orders to limit and define the scope of electronic discovery when significant burdens may be faced that outweigh the potential benefits of the requested production. And even if the client ultimately is required to undertake a major production of electronic records, counsel may succeed in shifting the costs of that effort to the opponent.

Chapter Three outlines basic strategies for dealing with electronic discovery in an ongoing case, from both offensive and defensive perspectives. Here, the type of matter at issue can make a big difference in the strategy employed. In the case of a single plaintiff asserting a claim against a large enterprise—as in a consumer class action, for example—the burden of electronic discovery is likely to be fairly one-sided, as the individual plaintiff will have few electronic documents of relevance, while the corporate defendant may have volumes of arguably relevant electronic records covering long periods of time. In contrast, ordinary commercial litigation between two business

enterprises changes the dynamics considerably, as both sides are likely to have many potentially relevant electronic documents. In the latter case, pursuing an aggressive approach to electronic discovery may lead to a retaliatory response that a client may not appreciate or be prepared for. For this reason, it is critically important to consult closely with in-house counsel before launching massive electronic discovery "attacks."

Chapter Three A deals with the more mundane aspects of electronic discovery, focusing on the four sequential steps that must be undertaken in this process with regard to any dispute that leads to litigation and a duty to preserve and produce electronically stored information. The first step is the determination of the potential scope of the data collection effort that must be undertaken. This is essentially identical to the type of scope determination required for traditional paper-based discovery, including: (1) determining the relevant subject matter for responsive data, based on potential claims and defenses; (2) identifying potential custodians of such data to interview as to the types of data that might be available for collection; (3) determining the time period at issue and the extent to which electronic records collections for that time period are reasonably accessible or not accessible; and (4) outlining the data storage systems to be included in the collection process based on the results of this overall analysis.

The second step in the discovery process discussed in Chapter Three A is the actual data collection effort, which involves several related tasks. The first covers the basic mechanics involved in making electronic copies of the records to be collected. The other topics discussed include the determination of appropriate steps to take to ensure data are not altered in that collection process, establishing an adequate chain of custody for evidentiary purposes if any of the electronic records ultimately need to be used at trial, and documenting all this activity to avoid the potential for sanctions down the road if questions arise on how the collection process was done.

The third element of the discovery process covered by Chapter Three A is sorting and analyzing all the raw data collected in some efficient and reasonable manner. The steps taken will vary based on the types of records collected. For example, do the electronic data contain meta-data to analyze and possibly "redact" before production? Are there potentially deleted files that may still be recoverable that should be searchered? This chapter covers this analytical and filtering process in detail, including an overview of forensic tools and methods to conduct these critical processes.

Last but not least, Chapter Three A addresses the potential need for the client to enlist the assistance of a computer forensic expert, either to help collect and review the client's own data, or else to review the opponent's electronic records. Computer forensics is a rapid growth

field with many purported "experts" who are often new to the scene, so careful screening of credentials and experience is important. Whether to engage an expert is something that needs to be addressed at the very outset of the discovery process, which is not ordinarily the case for other experts on the merits of the dispute. While computer forensic experts can be costly, their advice early on may ultimately save the client considerable expense—and provide insurance against potential sanctions as well.

Chapter Four addresses electronic document preservation both before and after litigation commences. One of the questions most frequently asked by clients is what steps must be taken to preserve electronic records when a dispute is threatened or litigation is initiated. Another frequent question is how to implement a document retention policy focusing on electronic documents and data that will withstand judicial scrutiny down the road, should an electronic discovery battle ensue. Increasingly, document retention policies—often disparaged as "document destruction" policies by opponents—must focus on electronic records, because more than 90% of the information retained by businesses today is stored in an electronic format. As noted earlier, under the new federal rules, the parties have a duty to be familiar with their own electronic records systems in order to be able intelligently to address the scope of their obligations for preserving and dealing with electronically stored information at the outset of the case.

For some industries, like securities broker/dealers, federal statutes and regulations already dictate stringent rules for retention of electronic records such as e-mail and voice mail messages. These industry-specific rules are beyond the scope of this treatise, and are generally within the realm of full-time corporate compliance departments. Failure to comply with these mandatory retention schemes, of course, may have important consequences in subsequent litigation. Because the pre-existing duty to preserve is clear, the failure to adhere to the standards may result in significant sanctions in civil litigation when the failure to produce is challenged.

Unfortunately, there remains no "silver bullet" for designing and implementing electronic document retention policies that need to balance reasonable needs to preserve records without imposing unreasonable burdens on the ongoing business enterprise. It is easy to predict that retention policies will continue to be litigated and amended or "tweaked" in response to continuing case law developments in this area, just as consumer product and service providers continually redraft arbitration clauses in standard terms and conditions in an attempt to address evolutionary case law affecting their enforceability.

Retention policies are also affected by the frequent inability of the business enterprise readily to restore electronic data even when properly preserved in some electronic format. Businesses routinely

encounter difficulty restoring archived electronic data because the data are stored in formats or media that are no longer readily accessible on the current computer system platforms of the enterprise. The business may need to engage forensic data consultants that maintain legacy systems and old versions of software applications precisely for this purpose. The business may also not have the database file record layout or glossary that is essential to understand what is contained within the data. This is a problem that is rarely, if ever, faced when dealing with paper records. Having old backup tapes with unintelligible data is the equivalent of finding a treasure-trove of paper documents that are written in a foreign language; to get to the golden nuggets that are needed, the practitioner may need to hire an electronic "translator."

Chapter Four also provides sample document retention policies and preservation orders.

Chapters Five and Six focus on the technical aspects of written discovery and depositions directed at conducting discovery of electronic records collections. These two chapters provide a roadmap for planning and engaging in these types of discovery. When reviewing these chapters, the advice outlined in Chapter Three for offensive and defensive discovery tactics should be kept in mind, particularly when the case involves a business versus business dispute. The more thorough the plan for aggressively seeking electronic records from the business opponent, the more likely it is that the opponent will turn these same weapons against the requesting party, so counsel needs to make sure that the client is fully apprised of what might be expected. Chapters Five and Six also contain sample requests for production of electronic documents, sample interrogatories, and a sample outline for deposing an electronic records custodian or information technology staff.

Chapter Seven is dedicated solely to the topic of electronic mail and messaging. This, of course, is by far the most challenging area for electronic discovery—and in the vast majority of cases, the most potentially dangerous as well. Given its importance, practitioners are encouraged to review this entire chapter to ensure a full understanding of the many thorny issues raised by e-mail records. The chapter first outlines the legal issues related to discovery of electronic messages, including situations involving deleted e-mail, which can be burdensome and costly to recover. Included in this overview is a summary of some of the federal statutes related to electronic mail, some of which establish privacy standards. Chapter Seven then discusses expectations of privacy concerning electronic messages. Courts and practitioners generally recognize that unrestricted rummaging by opposing counsel through electronic messages could have a serious impact on the reasonable privacy expectations of the messages' authors in many instances, while in others, there can be no such

expectation. The remainder of Chapter Seven delves into the technical and mechanical details of how electronic messaging systems work, and how to find and mine the fruits of electronic discovery in this medium. The chapter includes a sample e-mail use and retention policy.

Chapter Eight addresses special evidentiary issues that arise when dealing with electronic records. Just as with such physical objects as paper documents, electronic records must be authenticated before they will be admitted into evidence. But proving that the electronic record is in fact "authentic" and not modified in any material respect can be a much more daunting task than with many paper records or other physical objects. The challenge is analogous to the challenges first presented by the photocopy machine decades ago, and now the computer printer and far more accurate color photocopiers.

Chapter Nine provides insights into the role of experts in the realm of electronic discovery. Experts can be used in many ways, from designing and implementing electronic records retention plans to managing the search for records or authentication of what is found for use at trial. Electronic discovery is one of the fastest growing areas for the litigation consulting field. Litigation traditionally has relied on experts primarily for issues related to the merits of a claim, including liability—for example, using engineering experts to testify on design flaws, or medical experts to testify on causation and injury—or damages, where the economist is king. Over the past few decades, new areas of litigation expertise have emerged and matured, such as jury research consultants. Now, well-trained computer systems experts are needed to assist the practitioner in the procedural area of electronic discovery, to help find, restore, search, translate and reproduce electronic records and to provide the chain of custody necessary to get them admitted at trial. Failure to engage a competent computer forensic expert early in a major case could ultimately lead to harsh sanctions for the client if key records are not properly retained or identified and produced. Chapter Nine is intended to help the practitioner determine what particular expertise might be necessary or appropriate to help manage any electronic records challenge he or she is facing.