Chapter 1

Knowing Why e-Discovery Is a Burning Issue

In This Chapter

- Diving into e-discovery
- Seeing electronic information in 3D
- Getting the layout of the litigation process
- Understanding the steps in the e-discovery process

Beginning in 1938, Federal Rules of Civil Procedure (FRCP) have governed the discovery of evidence in lawsuits and other civil cases. *Discovery* is the investigative phase of a legal case when opponents size up what evidence is, or might be, available. During discovery, the parties in a dispute — the *plaintiff* (party bringing suit) and the *defendant* (the party being sued) — have the right to request any information in any format relevant to the case from their opponent. Each party has to respond with either the information or a really good reason why the information cannot be presented.

Despite several updates, FRCP remained largely limited to paper until 2006. Evidence, on the other hand, had gone electronic and onto hard drives of computers and handheld devices. To synchronize the legal system to the realities of the digital age when almost everything is e-mailed or viewed on an Internet-enabled device, electronic discovery (e-discovery) amendments to the FRCP were enacted on December 1, 2006. Put simply, changes to the FRCP mean that almost all discovery now involves e-discovery.

In this chapter, you discover how e-discovery rules rocked the legal landscape by making *electrically stored information* (ESI) discoverable. You read why you must start thinking about e-discovery long before you're involved in a legal action. Electronic discovery is an inescapable obligation (like paying taxes); you must be able to produce all relevant ESI on demand. To produce data and documents, you have to save them in such a way that you can find, open, and read them. You and your lawyers can expect consequences when stuff goes missing. Armed with this information, you then get familiar with the basic stages in the e-discovery process.

Getting Thrust into the Biggest Change in the Litigation

In April 2006, the United States Supreme Court approved sweeping changes to the Federal Rules of Civil Procedure (FRCP). After getting Congress's approval, the amended FRCP became law on December 1, 2006. These amended rules are aimed at one issue — the discovery of *electronically stored information* (ESI). ESI used as evidence is electronic evidence, or e-evidence. Despite their differences, the terms *ESI* and *e-evidence* are often used interchangeably.

As you can guess from the title, the discovery of anything electronic is called *e-discovery*. With most or all decisive evidence being electronic, you need to understand both the legal and technological dimensions of e-discovery — and depending on your job, you may just be competent in one or the other. We talk about the legal side in Chapter 4, which details the new FRCP. Many U.S. state laws are based on federal laws so there's no escaping e-discovery rules. For a description of the federal rulemaking process, visit `uscourts.gov/rules/newrules3.html`.

You can download a copy of the 166-page FRCP describing its 86 rules from the U.S. Courts' Web site at `www.uscourts.gov/rules/CV2008.pdf`. If you're new to the rules, you might hold off reading them until you've read Chapter 4 in this book.

Why did e-discovery rules, in effect, steamroll the litigation landscape? The short answer is that lawyers and litigants were unprepared to comply with this type and volume of discovery and all its complexities. Two reasons account for most of this lack of preparedness.

- **Lawyers are not IT people.** The huge majority of lawyers never had a course in IT (information technology) or e-discovery in their law schools. Electronic evidence lives in many places and forms that are tough to find, collect, store, and interpret without technical skills.
- **Electronic discovery must be addressed when a lawsuit is filed.** When litigation initiates, so does the e-discovery clock. Comparing Figure 1-1 to Figure 1-2, you see how the discovery phase of litigation has changed. Prior to December 2006, discovery was an afterthought. Most litigation doesn't go to trial, so cases ended before discovery got started. Not anymore.

No matter the size of your case, you need to make sure your lawyer has a clear understanding of the technologies involved and knowledge of the e-discovery rules to meet and manage his e-discovery duties correctly. If your lawyer lacks the tech expertise and the experience to make e-discovery more efficient, you risk e-discovery going wrong; resulting in you getting sanctioned by the judge or maybe even losing your case.

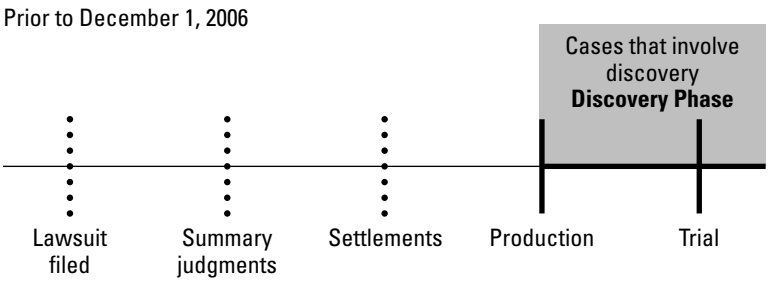

Figure 1-1: Discovery is avoidable if the case is resolved before that phase.

The FRCP applies to every type of litigation. Class action lawsuits, complex corporate fraud, and employment cases (for example, discrimination, wrongful termination, and harassment) involve e-discovery. Government investigations of fraud or improper conduct invariably dig into e-mail, instant messages, contact lists, and appointment calendars. In instances where a marriage is eroding, spouses might want to know and use what the other spouse is searching for on the Internet or texting.

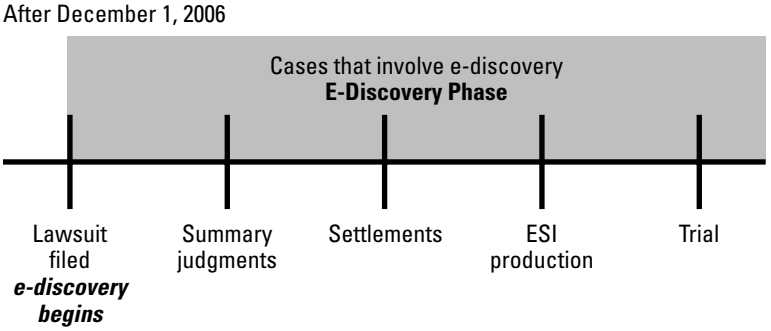

Figure 1-2: Electronic discovery moves to the front of the case.

New rules put electronic documents under a microscope

All computer systems, digital devices, and anything with a flash drive used by businesses, government agencies, health care and education institutions, and individuals that store electronic documents (word processing, spreadsheets, calendars, and presentations) are forms of ESI. Everything from terabyte-sized databases to text messages (even Twitter messages, or tweets) may be *discoverable* (subject to discovery) and, therefore, reviewable by others. Contact lists on an iPhone, legacy data on backup tapes, instant messages on a BlackBerry, posts on MySpace, and GPS and EZ-Pass records may be part of the ESI universe.

We use "may be" to temper our statements because privileged and confidential content *may* create exceptions to the rules. You find out about exceptions to the rules, and conditions that cancel (legally, *waive*) those exceptions, in Chapters 4 and 10.

Here's how you should go about finding ESI prior to a trial.

1. **Conduct an initial search.**

   Search data stores, often asking for help from data owners or IT experts, to identify documents, e-mails, spreadsheets, financial records, or other ESI that have been requested. Full-text searching is one of the basic tools used to find documents. Full-text and keyword searching are discussed in Chapter 9. You'll store all documents in a database.

2. **Perform a pre-production review.**

   Review all documents by hand, through a computer review, or most likely using both methods to verify their relevance and to exclude duplicate, privileged, confidential, and irrelevant content. Best practices and pitfalls of pre-production review are covered in Chapter 9.

3. **Perform a post-production review.**

   You hand over the ESI to your opposing party so they can review it. In some cases, the court may appoint a Special Master, or you and your opponent may agree to have a neutral expert review the ES, or you may hire your own expert. A S*pecial Master* is a neutral lawyer with technical expertise or an IT expert appointed by the court to manage and resolve e-discovery disputes in such areas as forms of production, keywords, and protocols.

During 2009, e-discovery costs amounted to 90 percent of a litigation budget with a majority of the costs associated with the review of ESI. You can take a big bite out of ESI costs by sticking to a disciplined approach to electronic records management in order to reduce the volume of ESI to review. For example, by requiring users to delete personal e-mail and disposing of electronic records that no longer need to be retained, there's a lot less ESI to collect, review, and produce.

New rules and case law expand professional responsibilities

Federal rules and case law pertaining to both e-discovery and e-evidence have added technological competence and ESI management to professional

responsibilities. *Case law* is the body of law or precedents created by judges' written opinions and decisions. Rules are interpreted in case law. That is, what the rules are interpreted to mean are determined by judges' opinions, which create case law.

For example, case law on how effectively your keyword search methodology has met its discovery obligations were created by the opinions of judges in three cases: *USA v. O'Keefe* (D.D.C. Feb. 18, 2008), *Equity Analytics v. Lundin* (D.D.C. Mar. 7, 2008), and *Victor Stanley, Inc. v. Creative Pipe, Inc.* (D. Md. May 29, 2008). The case law warns that a lawyer's failure to search an e-discovery database competently will lead to a bad outcome. Subsequent cases involving disputes over keyword or text searching often refer to those decisions.

You can find the text of significant e-discovery opinions using the federal court system's PACER (Public Access to Court Electronic Records) at `http://pacer.psc.uscourts.gov`. There's a small fee for accessing certain records.

Groundbreaking e-discovery case law stemmed from five opinions in *Zubulake v. U.B.S. Warburg*. *Zubulake* was an employment discrimination case in the Southern District of New York that resulted in opinions that are still referred to as the gold standard in e-discovery. You find out about the Zubulake opinions in Chapter 4.

FRCP requires you to quickly find ESI when required by the court. Waiting until you're facing an e-discovery request (actually, it's a *demand*) to start preparing for one can lead to severe sanctions.

Imagine waiting until a fire has started to install a sprinkler system, develop evacuation plans, or conduct fire drills. Inarguably, the new rules and case law have expanded the job descriptions of managers, lawyers, paralegals, litigation supporters, IT administrators, and data custodians.

Your attorneys and paralegals need to be IT proficient. Your attorneys need to know what ESI to request and to be able to defend their requests when vigorously challenged by the opposition. Attorneys also need to understand your IT infrastructure in order to comply with the request, prevent the destruction of evidentiary ESI (see the nearby sidebar about AMD and Intel), and keep a record of searches that you've conducted to validate the effectiveness of your searches. Your entire IT department must cooperate with your legal team. You must be able to identify, preserve, and collect ESI. With so much information potentially subject to an e-discovery order, your entire legal team — IT professionals and lawyers — must understand both IT and the law so you inadvertently or deliberately don't delete ESI that you're required to preserve.

Biggest e-discovery case catches Intel unprepared

In 2005, Advanced Micro Devices (AMD) brought a lawsuit against its archrival Intel for alleged anticompetitive practices in the chipmaker market. Both parties recognized that they faced the largest e-discovery ever. Estimates of production were roughly "a pile 137 miles high."

The Special Master appointed by the court to hear evidence from both AMD and Intel recommended that Intel be compelled to produce documents that it had declined to submit. In March 2007, Judge Joseph A. Farnan, Jr. gave Intel 30 days to recover more than 1,000 e-mails that it should have but did not preserve.

Intel faced several problems. Its e-mail system running on Microsoft Exchange servers automatically purged employee e-mail every 35 days and senior executives' e-mail every 60 days. Intel used nonindexed backup tapes designed for disaster recovery that were not suited for e-discovery. Trying to find all of the requested e-mail messages that contained specific keywords took a staggering amount of time because each backup tape had to be mounted to restore the contents in order to get them into shape to be searched and reviewed.

In a March 5, 2007 letter to Judge Farnan, Intel's lawyer advised the court and AMD of its extensive and expensive remediation efforts to find and recover lost e-mails. For e-mails sent by employees that hadn't been preserved as they should have, Intel planned to locate them from the e-mail in-boxes of employees who'd received them. The letter also stated:

"the overall scope of the e-mails and documents Intel will be producing is sweeping in breadth and magnitude — and will encompass the equivalent of tens of millions of pages of material from many hundreds of employees with overlapping involvement in communications, both internal and external."

The court scheduled the *AMD v. Intel* case for trial in February 2010.

Being unprepared is expensive. An unprepared manufacturing company spent $800,000 filtering its unmanaged e-mail system in response to an e-discovery request. Roughly 88 percent of their e-mails were irrelevant to the litigation and weren't produced.

Distinguishing Electronic Documents from Paper Documents

When you think of new technology (such as electronic documents) in terms of older technology (circa paper), you don't appreciate its distinctive qualities and capabilities. Legend has it that when electricity was invented and electrical lights replaced gas lamps in 1879, people would change their light bulbs quickly so electricity wouldn't leak out of the socket. Warning signs were posted that read "This room is equipped with Edison Electric Light. Do not attempt to light with match. Simply turn key on wall by the door." In fine

print at the bottom of the signs read "The use of electricity for lighting is in no way harmful to health, nor does it affect the soundness of sleep."

The key point is that a technological understanding of electronic documents, devices, and how they are managed is important — so that you don't take a match to them out of ignorance. A helpful approach is to start by comparing and contrasting characteristics of ESI and paper, which we do in the following sections.

Research firm Gartner found that nearly 90 percent of U.S. companies with revenue exceeding $1 billion are facing an average of 147 lawsuits at any given time, and that the average cost to defend a corporate lawsuit exceeds $1.5 million per case.

ESI has more volume

The amount of ESI created per person is measured in megabytes (MB) — roughly 800MB per year. One MB equals 1,048,576 (or 2^{20}) bytes, which would hold the content of a medium-sized novel. A Fortune 1000 pharmaceutical company with more than 70,000 employees archives 35 terabytes (TB) of new e-mail data every year. One TB is roughly 1.1 trillion bytes. The trivia question is, "How many pages of data equal one terabyte?" The answer is 75 million pages. Of the 60 billion e-mails sent worldwide on a daily basis, 25 billion are business-related.

Clearly, the volume of ESI is tough to fathom. Unlike paper, the volume of ESI multiplies because ESI *replicates itself*. When you send e-mail, a copy goes into your sent mail folder and another arrives in each of the receivers' inboxes, which might get stored on e-mail servers or archived. With paper documents, creating multiple copies requires more time and effort.

ESI is more complex

Electronic documents provide more recordkeeping information than a paper copy because metadata are embedded within it. *Metadata* is essentially the history of a document written with invisible ink. Every comment, edit, iteration of a document is hidden within that document, chronicling its life. There is also embedded data frequently stored with an ESI document, such as formulas in spreadsheets. Microsoft Office automatically embeds many different types of metadata in word processing, spreadsheet, and other applications. Examples of metadata are

- Title, subject, and author
- Location where the file is saved

- Dates and precise times when the document was created, accessed, modified, and printed
- Comments, revision number, total editing time, and the template used to create it

Metadata is discoverable when needed or relevant to a matter at hand. For example, you can use this information when there's a question of when a document was created or downloaded, whether it was modified, or backdated. Metadata may help authenticate a document, or establish facts material to a dispute, such as when a file was created or accessed, or when an e-mail message was sent.

Seeking out and viewing metadata embedded in a document is *mining* the document. Many e-discovery disputes are caused by, or because of, metadata. Those disputes are so significant they've led to case law.

Williams v. Sprint is a landmark case concerning metadata. It established the standard that the producing party should produce electronic documents with their metadata intact.

By mining a document, your attorney can view revisions made to the document, comments added by other users who reviewed the document, and whether it was drafted from a template. The disclosure of metadata can lead to the disclosure of client confidences and secrets, litigation strategy, editorial comments, legal issues raised by the client, and other confidential information. See Chapter 10 for explanations of these issues.

ESI is more fragile

Electronic documents are much easier to alter than paper documents without leaving a visible sign of the alteration. The sender of e-mail messages can spoof, or fake, the sender's identity — a spammer's tool of the trade. Data and files can be modified deliberately in numerous ways that may be detectable only with computer forensic techniques. We discuss recovering deleted data in Chapter 2. (For more computer forensics techniques, check out *Computer Forensics For Dummies,* by Linda Volonino and Reynaldo Anzaldua.)

Files can become corrupted. Hard drives crash. Users accidentally or deliberately can overwrite a file by saving a new file with the same filename as an existing one. Backup tapes get re-used, lost, stolen, or may break or get corrupted. Auto-delete policies may delete e-mails after a certain amount of time, even without an intentional action to delete them.

Figure 1-3 contrasts how paper and ESI are destroyed or altered and how they are preserved. Because ESI exists only on some storage media and that media may be overwritten, corrupted, or otherwise be unreadable,

you should take affirmative steps to preserve it. Absent deliberate action to preserve the ESI, the expectation is that it will be destroyed or altered. The courts understand this principle. So must you.

	Affirmative Steps	Passivity
Paper	Destroy, alter	Preserve
ESI	Preserve	Destroy, alter

Figure 1-3: Differences in how paper and ESI are destroyed and preserved.

ESI is harder to delete

Electronic documents are much more difficult to dispose of than paper documents even though they're fragile. The fragility/persistence paradox causes a lot of confusion. Jeff Rothenberg, a senior computer scientist at RAND, captured the paradox by pointing out humorously that "digital information lasts forever, or five years — whichever comes first." RAND (`www.rand.org`) is a nonprofit institution whose mission is to conduct research and analysis to help improve policy and decision-making.

For example, changing the data or formula in a cell of an Excel spreadsheet could be a *destructive change* (no traces of the change) if there are no other copies of that file or tracking changes is turned off. A destructive change or update is one that destroys the prior contents beyond recovery or detection. If you instead delete the Excel file from a hard drive and take the extra step of deleting it from your Recycle Bin, the entire file will remain intact in the same position on the drive unless it is overwritten. You read more about what happens when a file is deleted in Chapter 2. Computer forensics software could recover that file along with information about when it was deleted.

Deleting documents is futile if they were saved to a server, backed up, or e-mailed. Misunderstanding persistence may lead to the discovery of information that was never intended to be retained or that no one knew existed.

There's also the auto-recover or auto-save feature found in software programs that prevents data loss by automatically creating a backup copy of any currently open document every few minutes or other time interval. This so-called *replicant data* is stored on the hard drive as separate documents. Because they may not be deleted when the application program (such as Word) closes, they persist as copies of documents long since changed or deleted.

ESI is more software and hardware dependent

Data is unreadable or meaningless when separated from its original or native software environment. You need software to open and view a file correctly.

If you have five-and-a-quarter inch floppy disks and no computer with that drive, you cannot get at those files. If you don't have the correct software version, you can't open the file. Files stored on floppy disks, Zip drives, or other outdated media can't be accessed without hardware that can read them. If information has been transferred to backup tape, it may be difficult to restore the information because of technology upgrades or deterioration of the tape. When you change accounting software applications, for instance, you may not be able to access legacy (old) data years afterward.

Viewing the Litigation Process from 1,000 Feet

When you get involved in the litigation process, some milestones you can be involved with are shown in Figure 1-4. Notice the rather tight timeline and the two deadlines, which are specified by the amended FRCP. Total elapsed time from when the complaint is served (or lawsuit filed) until your lawyer submits your e-discovery plan to the court is only 120 days. The trial may be scheduled far into the future, which happened with *AMD v. Intel*. AMD filed the complaint in 2005; the trial is scheduled for 2010.

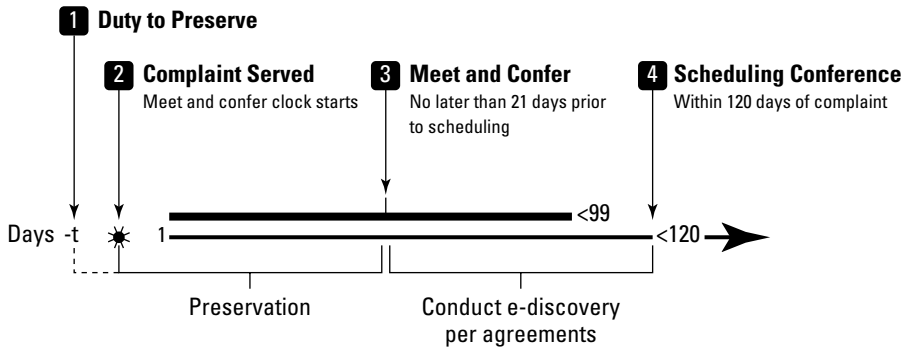

Figure 1-4: Overview of the litigation process.

Although the purpose of the new rules is to provide early structure, uniformity, and predictability to the litigation process, the reality is that right from Day 1 of a lawsuit, you must be ready to start evaluating with your IT team and legal counsel where you stand in terms of your ESI.

Here are the deadlines you need to observe:

- **Time minus zero:** Duty to preserve. You need to take affirmative action — active and timely measures — to prevent the destruction or alteration of what might be relevant e-evidence. This duty generally begins when you reasonably anticipate a legal action. That's a tough duty to comply with. Clairvoyance would be helpful because the scope of what needs to be preserved and when are not clear.

  Accept that it's difficult under the best of circumstances to know when your duty to preserve has triggered or what you need to preserve. Consult with your in-house counsel on when your duty to preserve ESI kicks in.

- **Day 1:** Complaint served. You're on solid ground here because there's no mistaking that a lawsuit is in play. This action starts a clock that counts off days.
- **By Day 99:** Meet-and-confer session. You must participate in a meet-and-confer session during which you cooperate with your opponent to negotiate an e-discovery plan. This type of cooperation is new and also a bit of a shock to the legal system that's used to being adversarial. The list of topics to negotiate includes the following:
  - Any issues relating to preserving discoverable ESI
  - Any issues relating to search, disclosure, or discovery of ESI
  - Format in which ESI should be produced
  - Scope of ESI holdings
  - Estimated costs in terms of difficulty, risk, time, and money of producing the ESI
- **By Day 120:** Scheduling conference. A scheduling conference is a hearing attended by all attorneys — yours and your opponents — and the judge to schedule certain dates and deadlines for the case. This event is generally the first time you come before the court.

By forcing these events early on in a case, by way of the FRCP amendments and case law, you really have no choice but to be ready to move forward with e-discovery at the start of a case.

Examining e-Discovery Processes

When you're involved in the e-discovery process, regardless of the type of case or investigation, you need to perform certain functions and meet requirements. Expect that none of the requirements is easy or cheap (in terms of time or money). On the plus side, performing them correctly saves time, effort, disruption, and stress. You face the following e-discovery functions.

Creating and retaining electronic records

Getting ready for e-discovery requires you being proactive. A standard used to evaluate proactive readiness is *reasonableness*. Your ability to demonstrate reasonableness starts with having established control over data, documents, and other electronic records. The base on which e-discovery is built is electronic records management (ERM). ERM is known by other names, such as records and information management, or RIM.

Here's how to set up an electronics rights management system:

1. **Develop an electronic record retention policy.**

   In light of litigation trends and declining storage costs, you can fall into the trap of believing that it's wise to save generously. Developing a keep-it-all retention policy is not the best approach because it focuses on the wrong factor — storage costs.

   You may think the FRCP requires you to save everything or save all e-mails. Regulated industries or certain types of companies, such as those in the financial, healthcare, and pharmaceutical sectors, have government regulations in place such as save all communications for seven years. But absent such regulation, the Supreme Court has indicated that you can set your own reasonable retention policy.

   Even if storage is cheap, management is costly. Good ERM is expensive because of the management, not the storage. As you read in Chapters 2 and 3, you need to keep your eye on the costs of reviewing electronic records to identify responsive ones. Define what is essential and needed as opposed to saving everything.

   Without an enforceable retention program and a secure, auditable archive and electronic records management solution, the costs associated with e-discovery are daunting, as you read in the *AMD v Intel* case.

2. **Implement the electronic records retention policy.**

   Even your best electronic records retention policy is of little use if employees don't implement it in a correct and uniform manner. Everyone who deals with records — employees, contract workers,

interns, and vendors — must receive sufficient and proper training on the policy. You need to document the training in detail.

3. **Monitor compliance with the policy.**

   Most likely, your retention program is partially automated and partially manual because end users need to categorize their records. To verify that retention requirements continue to be met, you have to monitor compliance.

4. **Destroy electronic records at the end of retention periods.**

   When electronic records no longer need to be retained, you need a secure way to destroy them.

5. **Change policies when you reasonably foresee litigation.**

   As soon as you reasonably expect to be involved in litigation, you must immediately set aside your ordinary electronic record retention program and implement a more demanding policy. This litigation-hold policy is critical, as you read in Part III. The litigation-hold policy must comply with the special requirements established at the meet-and-confer session and the scheduling conference.

No "model" electronic records retention program fits all. You should base your retention program on a case-by-case examination of your business, the legal and regulatory requirements of your industry and jurisdiction, and what use your company is likely to make of the documents, both for business and litigation purposes.

Identifying, preserving, and collecting data relevant to a legal matter

Assuming that electronic records are managed properly, the next step when facing litigation is to identify the relevant records, preserve them so they cannot be altered, and collect them for further review.

Methods used to identify relevant ESI may have been agreed to at the meet and confer or scheduling conference — although the duty to identify and preserve did start before this conference, when litigation was reasonably anticipated. If the meet and confer or scheduling conference has already happened, ask your lawyer whether an agreement is in place.

You have to preserve the ESI until it's needed. Preservation takes many forms, as discussed in Chapters 2 and 7. One of your difficulties at this stage is preserving data that is in use by the business. A lot of attention in case law has focused on data that is not reasonably accessible (see Chapters 2 and 3). Equally challenging is preserving live data because you cannot simply hand over a backup tape.

The standard for duty to preserve comes from the opinion of District Court Judge Shira A. Scheindlin, from the Southern District of New York, in *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y., Oct. 22, 2003). That case is referred to as *Zubulake IV* because it was the fourth in a series of what are called the *Zubulake decisions.*

Processing and filtering to remove the excess

As with every stage in the e-discovery process, there are strategies and best practices for the processing and filtering of ESI. After preserving and collecting the ESI, you'll confront the costly tasks of processing and reviewing the data for responding to the investigation, claim, or litigation.

Determining what to process is a balancing act of costs and risks. Gartner estimates the cost of reviewing 1GB for e-discovery is $18,750. Clearly, costs are reduced by reducing the volume to be filtered. Risks are increased by reducing the amount of ESI to process because relevant e-evidence might be excluded. Breaching e-discovery obligations can result in sanctions or worse even if processing and filtering were done in good faith. In Chapter 9, we explain this critical stage in detail.

Reviewing and analyzing for privilege

Confidential conversations and communications that are protected by law from being used as evidence or revealed to others are referred to as *privileged*. Examples of privilege are conversations or letters between a person and an attorney (*attorney-client privilege)*, therapist, physician, priest, minister, or spouse. Privilege is a major source of argument between opposing lawyers. Unless there's an exception, privileged ESI is not discoverable. There are an almost interminable number of exceptions to privilege.

You must review all ESI to identify what is and is not privileged. This stage may be the most expensive depending on the stakes of the case. ESI that you must review visually is much more costly than a coarser review using software for the same volume of ESI.

We talk more about privilege in Chapter 10.

Producing what's required

You start with the universe of ESI, filter out what's irrelevant, duplicated, or privileged, and then have the pool of ESI to produce. Before producing the ESI, you may need to do additional reviews.

If form of production was not specified by the requesting party at the meet-and-confer session, you might have some options. Producing ESI in native format is common because it's cheaper than having a forensics image created. With native production, if it existed as a `.docx` file, you produce it as a `.docx` file. Turn to Chapters 11 and 13 for more info about how to produce ESI.

Complications emerge when you have documents with attachments, for example, e-mail messages with attachments or project management files with attached resource files. Other complications are identified in Chapter 10.

FRCP Rule 34(b)(ii) allows you to produce ESI in a form or forms in which you ordinarily maintain it. Other reasonably usable forms may also be acceptable.

There are pros and cons concerning form of production. When balancing production risks and costs, keep in mind that the form of production most likely must include the metadata.

Clawing back what sneaked out

If ESI is produced that should not have been, a situation known as *inadvertent disclosure,* you can request its return via a clawback agreement. Revealing the content of your privileged communications or documents to your opponent is suboptimal because you can't take back what they've learned about you. Despite this downside, clawbacks are not unusual. When review or processing is not done thoroughly, you'll produce ESI that you shouldn't have. The consequences for not producing on schedule because the review is incomplete may be worse than the risks associated with clawback.

Clawback agreements may be discussed during the meet-and-confer session. Despite any agreements, numerous conditions apply to clawbacks. Courts might have to decide whether the producing party has met those clawback conditions.

We talk more about clawback agreements in Chapter 10.

Presenting at trial

Judges have little to no patience with lawyers who appear before them and don't understand their ESI or the ESI of the opposing side. The same applies to you if you're called upon to testify on behalf of your company's ESI retention policies, storage locations, or other e-discovery issues in court. No one can operate effectively in the courtroom without understanding e-evidence, where ESI is created and stored, how to collect and review it, how to recover it in a forensically sound manner, and how to have it admitted into evidence at trial. Chapter 5 discusses the professional competence and conduct of your lawyer.

You want to make sure that your lawyer and all your company's witnesses are armed with the knowledge to competently and confidently testify in court. Make time for these lessons. When your lawyers asks for information, be sure to prepare reports and diagrams that non-technical people (the judge or members of the jury) can understand.