Making Everything Easier!™

e-Discovery FOR DUMMIES®

Learn to:

- Follow the correct steps in the e-discovery process
- Anticipate potential risks
- Develop an e-discovery strategy for your company
- Identify best practices in the event of litigation

Linda Volonino
Ian Redpath
e-discovery consultants

Get More and Do More at Dummies.com®

Start with **FREE** Cheat Sheets

Cheat Sheets include

- Checklists
- Charts
- Common Instructions
- And Other Good Stuff!

To access the Cheat Sheet created specifically for this book, go to
www.dummies.com/cheatsheet/ediscovery

Get Smart at Dummies.com

Dummies.com makes your life easier with 1,000s of answers on everything from removing wallpaper to using the latest version of Windows.

Check out our

- Videos
- Illustrated Articles
- Step-by-Step Instructions

Plus, each month you can win valuable prizes by entering our Dummies.com sweepstakes.*

Want a weekly dose of Dummies? Sign up for Newsletters on

- Digital Photography
- Microsoft Windows & Office
- Personal Finance & Investing
- Health & Wellness
- Computing, iPods & Cell Phones
- eBay
- Internet
- Food, Home & Garden

Find out "HOW" at Dummies.com

**Sweepstakes not currently available in all countries; visit Dummies.com for official rules.*

e-Discovery FOR DUMMIES®

by Linda Volonino and Ian Redpath

Wiley Publishing, Inc.

e-Discovery For Dummies®

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

Library of Congress Control Number: 2009937841

ISBN: 978-0-470-51012-4

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

About the Authors

Linda Volonino (PhD, MBA, CISSP, ACFE) entered the field of computer forensics and electronic evidence in 1998 with a PhD and MBA in information systems (IS). She's been a guest lecturer on computer forensics and e-discovery at the State University of New York at Buffalo School of Law, and to attorneys and state Supreme Court justices as part of Continuing Legal Education (CLE). She's a computer forensics investigator and e-discovery consultant with Robson Forensic, Inc. working for plaintiff and defense lawyers in civil and criminal cases. In addition to standard e-mail and e-document evidence, she's consulted on cases involving electronically stored information (ESI) from social media sites and handheld devices as part of e-discovery.

Linda's coauthored *Computer Forensics For Dummies* and four textbooks: two on information technology, one on information security, and one on computer forensics. She's published in academic, industry, and law journals on e-discovery and the need for electronic records management as part of prelitigation readiness. She's a senior editor of Information Systems Management and was Program Chair for the 2009 Conference on Digital Forensics, Security and Law. Linda can be reached via `lvolonino@aol.com`.

Ian J. Redpath holds a Bachelor's degree from Hillsdale College, a JD from the University of Detroit, and an LLM from the University of Wisconsin. He has 34 years experience in litigation and has been admitted to practice in the states of Michigan, Wisconsin, and New York as well as the Federal and Tax Courts. Ian is also a former prosecuting attorney. He has published numerous articles on contemporary issues and topics and coauthored several books.

Ian has taught American Jurisprudence at the University of Clermont-Ferrand School of Law in France and lectures regularly on American Law at the prestigious MGIMO in Russia. He has extensive national and international experience in developing, writing, and presenting continuing education programs.

Currently, Ian is the principal in the Redpath Law Offices with offices in Buffalo and New York City where he specializes in criminal and civil litigation. He can be reached at `IanRedpath@redpathlaw.com`.

Dedication

I would like to dedicate this book to my beautiful wife Liz, and children, Eric, Bridget, and Lauren who provide me with love, inspiration, and support.

– Ian Redpath

Authors' Acknowledgments

Our Project Editor Rebecca Senninger kept us moving forward and doing our best work. Thanks Rebecca! We're also most grateful to Amy Fandrei, Acquisitions Editor, for the expert guidance needed to write a techno-legal book that lawyers, managers, information technologists, and judges may use as a reference.

Special thanks to our hard-working copy editors Brian Walls, Virginia Sanders, and Heidi Unger and our technical editor Jake Frazier. We appreciate your feedback and suggestions for improving our chapters.

Publisher's Acknowledgments

We're proud of this book; please send us your comments at http://dummies.custhelp.com. For other comments, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

Some of the people who helped bring this book to market include the following:

Acquisitions and Editorial

Project Editor: Rebecca Senninger

Acquisitions Editor: Amy Fandrei

Copy Editor: Brian Walls

Technical Editor: Jake Frazier

Editorial Manager: Leah Cameron

Editorial Assistant: Amanda Graham

Sr. Editorial Assistant: Cherie Case

Cartoons: Rich Tennant (www.the5thwave.com)

Composition Services

Project Coordinator: Sheree Montgomery

Layout and Graphics: Joyce Haughey, Mark Pinto

Proofreaders: Laura Albert, ConText Editorial Services, Inc.

Indexer: Sherry Massey

Special Help: Virginia Sanders, Heidi Unger

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Acquisitions Director

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Table of Contents

Introduction

Electronic discovery gone wrong is kryptonite to a legal action, as many have learned since the amended Federal Rules of Civil Procedure (FRCP) took effect in December 2006. Now you may urgently want to learn about e-discovery (short for *electronic discovery*) but don't know who to call, or even better, what to read. *e-Discovery For Dummies* is an end-to-end reference and tutorial written for litigators and jurists, corporate counsel and paralegals, information technology (IT) and human resources (HR) managers, executives and record librarians, and anyone who might file a lawsuit or be the recipient of one. For those not engaged in e-discovery now, the time is fast approaching when having a commanding knowledge of it is going to be vital to your career.

Who Should Read This Book?

e-Discovery For Dummies is for everyone needing an understanding of the e-discovery rules of procedure and the protections they provide, and how to position your case to be covered by those protections. IT, HR, records managers, and others who might be responsible for e-litigation readiness or electronic records management should start reading this book as soon as possible.

CPAs who provide forensic information and damage calculations for clients need to be aware of e-discovery issues, particularly the liability implications of metadata contained in client files. Inadvertent disclosure of metadata in client files could remove legal protections. For example, if a client's metadata is disclosed accidentally, then it may enable opponents to use that metadata against the client's interests.

Insurance companies are enormously concerned and interested in e-discovery. Insurers are like the father of the bride — even though no one pays much attention to him at the event, he pays much of the bill. So insurance companies have one of the largest stakes in e-discovery.

If you know nothing about e-discovery or want to sharpen your litigation strategy, this book's for you.

About This Book

e-Discovery For Dummies is an introduction to the hottest legal issue. The e-discovery rules expand the definition of what's discoverable to include electronically stored information (ESI), require parties to discuss ESI during initial meet-and-confer conferences, may provide a safe harbor against sanctions for routine deletion of ESI, and may protect against a privilege waiver for inadvertent disclosure.

The rulings and opinions of various judges provide invaluable lessons that you and your lawyers can learn from this book, much cheaper than learning through experience. We cover the Advisory Guidelines to better prepare you to understand the process of obtaining, protecting, and presenting ESI. You learn how Federal Rule of Evidence 502, enacted in 2008, provides relief for inadvertent disclosure of items privileged under the attorney-client relationship or protected as work product.

Every company and agency needs to be litigation-ready and know how to proceed when requesting or responding to e-discovery agreements. Preparing for litigation implies that all of these new data repositories must be included in a data and records retention policy and program. Security executives involved in litigation could be called upon to describe their company's records retention policy and be knowledgeable of the systems used to manage their department's data. Lacking a credible program or failing to adhere to the policy is indefensible in court and might expose your company to legal risk.

It's an honest presentation of the issues and challenges, strengths and weaknesses of e-discovery.

What You're Not to Read

Depending on your background in law, criminal justice, investigative methods, or technology, you can skip the stuff you already know. If you're the victim, the accused, the plaintiff, or the defendant, feel free to skip sections that don't relate directly to your case or predicament.

Foolish Assumptions

We make a few conservative assumptions, even though we're serious about issues and advice we offer. We assume that:

- You need to understand e-discovery.
- You use and have a basic understanding of e-mail, the Internet, and digital devices.
- You have an interest in learning from the experience of others.
- You are considering expanding your career to include e-discovery.
- You realize that this book is not legal advice.

How This Book Is Organized

This book is organized into seven parts. They take you through the basics of e-discovery, ESI, rules, advisories, and litigation readiness. They cover the phases from preservation through production. Specialty issues, such as e-discovery in large cases and small cases and computer forensics, are covered. For a more detailed overview of topics, check out the following sections.

Part I: Examining e-Discovery and ESI Essentials

The book starts by introducing you to the e-discovery laws that have changed the responsibilities of legal and information technology (IT) professionals. You read why every lawsuit and most civil cases can and will involve e-discovery and the accessibility of ESI (as well as ESI that's not reasonably accessible).

You learn that most cases are settled as a result of e-discovery because that's when both sides learn the strengths and weaknesses of their position relative to that of their opposition.

Part II: Guidelines for e-Discovery and Professional Competence

This part gives you an in-depth understanding of the e-discovery amendments, The Sedona Conference advisory guidelines often used by the bench in settling disputes, and the expected standards of legal competence and conduct. Although the Federal Rules and advisories guide e-discovery, the competency of counsel turns them into a winning edge. We present the Electronic Discovery Reference Model (EDRM) as it relates to processes of preserving, collecting, processing, reviewing, and producing ESI.

Part III: Identifying, Preserving, and Collecting ESI

In this part, we cover the first phases of e-discovery, namely the identification, preservation, and collection of ESI. These are the steps to take when a lawsuit is filed. You learn what to do when faced with an e-discovery request and the countdown to the meet and confer with opposing counsel within 99 days.

We discuss the meet-and-confer conference in detail. Being prepared to negotiate during this conference can make the difference between a quick settlement and a prolonged battle. There are no re-negotiations or bailouts for bad agreements.

Part IV: Processing, Protecting, and Producing ESI

In the fourth part, we cover the next set of phases from processing of ESI through review, filtering, and the production of responsive, nonprivileged, redacted ESI. You read many examples of motions, mistakes, and monetary sanctions that could have been avoided.

All ESI issues might arise during these phases, including metadata, privilege, work product, keyword searches, and filtering by keyword, concept, and custodian. This part details the review process, which is the most expensive phase in e-discovery.

Part V: Getting Litigation Ready

In this fifth part, we examine the admissibility and relevance rule of electronic evidence, and forensics methods to recover and preserve it. Rules of evidence are subject to judgment, as are the federal rules of civil procedure. This part also covers advanced e-discovery strategies and issues, some of which are the use of experts, sanctions, depositions, and cost-shifting. We explain methods to authenticate evidence in civil trials. One indisputable duty is to keep the chain of custody intact because you can't repair tainted electronic evidence.

Part VI: Strategizing for e-Discovery Success

In the sixth part, you learn about archiving electronic records, which differs from data backups. We discuss electronic records management (ERM) that's necessary to be ready to respond to a request for ESI. The focus shifts from internal to external. We discuss e-discovery from the perspective of the judges and their powers to encourage parties to practice good faith and dissuade gamesmanship.

For large-scale, high-stakes, or unusual cases, you learn the value of partnering with vendors or litigation services companies to augment your expertise. For small cases, ESI may be the most convincing witness.

Part VII: The Part of Tens

Every *For Dummies* book has The Part of Tens, and we give you three of them. The first one covers the must-know rules. The second focuses on keeping you up-to-date. The third one focuses on the courts and career-advancing lessons.

Glossary

We include an e-discovery dictionary of legal and technical terms used throughout this book.

Icons Used in This Book

Useful clues represented by icons highlight especially significant issues in this book. The following paragraphs (with their representative icons) give you an idea of what to expect when you see these icons.

Time is money, and mistakes waste even more. Save yourself time, effort, and the pain of explaining to the court why you did or did not do something that you should or should not have done. These icons flag paragraphs that can be gold mines of information or land mines to sidestep.

Litigation that spans several years and involves many motions are not amenable to short summaries. The same is true of judges' opinions in cases where litigants or their lawyers made more than a fair share of mistakes. These icons provide an in-depth look at real-world cases and issues — both good and bad.

Sanctions ahead! We flag the land mines with this icon to draw your attention to what the rules mandate and what judges expect you to do correctly.

A heads-up and FYI icon on concepts to keep in mind.

Where to Go from Here

In this book, you find the basics of e-discovery rules, procedures, case law, and litigation readiness, but this is an exploding topic. You can use this book as a reference, how-to guide, and path to lifelong learning. Electronic discovery is not a passing phase. Electronic discovery case law is evolving. Litigants are sliding down the learning curve, which may significantly reduce time, costs, errors, and sanctions. When you know the basics and tactics, you have the foundation to expand your knowledge.

If you're looking for a handy reference to the e-discovery steps or the Federal Rules of Civil Procedure and Federal Rules of Evidence, check out the cheat sheet at `www.dummies.com/cheatsheet/ediscovery`.

Part I

Examining e-Discovery and ESI Essentials

The 5th Wave By Rich Tennant

"I'm trying to organize the IT guy's documents, and apparently his file system was informed heavily by the Da Vinci Code."

In this part . . .

This part presents e-discovery in digestible chunks so you understand the essentials of e-discovery at its simplest level. We explain e-discovery laws that have rewritten the responsibilities of legal and information technology (IT) professions in Chapter 1. Legal and IT — two groups most unlikely to speak a common language or operate at the same tempo — are most responsible for e-discovery success. Also in Chapter 1, you learn that all electronic content that we create, send, post, search, download, or store has a legal name: electronically stored information, or ESI. We cover why this ESI universe is subject to discovery and cite cases where failing to preserve and produce ESI cost litigants serious amounts of money and essentially gutted their cases.

In Chapter 2, you learn why working with ESI is messy even under the best circumstances. You're introduced to the relationship between the age of ESI and the ability to reach out and retrieve it from its storage media. ESI can be online, offline, gone, or somewhere in between. The ability to reach and retrieve ESI determines its accessibility, which in turn influences its discovery status from the perspective of judges (or *the bench*). You find out why it's best to resolve your ESI disputes with the opposing side rather than turn those disputes over to the bench. Also in Chapter 2, we foreshadow the fate of enterprises unprepared for e-discovery. You start to understand that investing in ESI retention and management tools to get into litigation-ready shape is much less risky than whining about why it's too burdensome to respond to an ESI request. Chapter 3 continues these lessons.

Prelitigation best practices get you into a strong defensive position, as you read in Chapter 3. You learn one of the most crucial lessons — that most cases are settled as a result of e-discovery because it's only then that both sides learn the strengths and weaknesses of the other's case. You don't go all in with no chance of winning, at least not more than once. When you do e-discovery right, you have a powerful offensive or defensive weapon.

"We used to say there's e-discovery as if it was a subset of all discovery. But now there's no other discovery."

—Judge Shira A. Scheindlin (2009),
e-discovery rock-star judge

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.

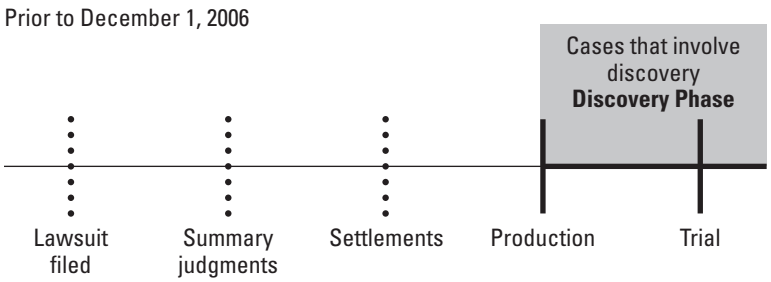

Figure 1-1: Discovery is avoidable if the case is resolved before that phase.

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.

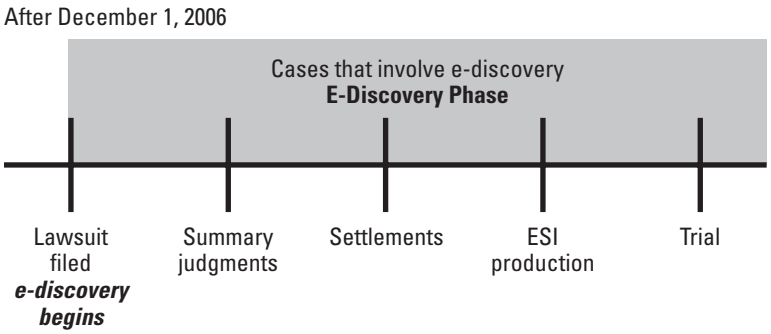

Figure 1-2: Electronic discovery moves to the front of the case.

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