Litigating with Electronically Stored Information

For a complete listing of titles in
the *Artech House Telecommunications Library,*
turn to the back of this book.

Litigating with Electronically Stored Information

Marian K. Riedy
Suman Beros
Kim Sperduto

ARTECH
HOUSE
BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

Cover design by Yekaterina Ratner

ISBN 13: 978-1-59693-220-3

685 Canton Street
Norwood, MA 02062

10 9 8 7 6 5 4 3 2 1

To the professional litigators battling in the trenches
every day with the new and abstruse legal issues
in the digitized world

Contents

Preface

We have attended many seminars and conferences on e-discovery and the amendments to the Federal Rules of Civil Procedure specifically concerning electronically stored information (ESI) over the last few years. The prevailing ethos at these gatherings has been negative. In effect, "you're not going to like it, but you've got to understand technology," and "you'd better be paying attention or you'll get socked with sanctions for spoliation of ESI." These statements may be true. But our attitude, and, we hope, the tenor of this book, is different. We view the accommodation of ESI in the practice of law as but another of the challenges to logic and legal reasoning that makes it all worthwhile. We have also tried to demonstrate in this book, through the interweaving of case law and rules, on one hand, and hard-core technology issues, on the other, that attorneys and information technologists really can talk to each other, with mutually beneficial results.

Litigating with Electronically Stored Information is also different in that it is not just about e-discovery or the 2006 amendments to the Federal Rules, although both these topics are covered in the book. Though we could not begin to cover comprehensively all the legal issues raised by ESI in the practice of law, we have included the principal subjects within the ambit of civil procedure and evidence that would arise for a litigator from the first meeting with a prospective client through trial. We have made best efforts to make the content reasonably accessible to attorneys new to the topics, but also useful for crafting sophisticated arguments for winning battles on the frontiers of the law.

We also touch on topics that we believe will be of interest to any attorney: ESI and security in the law firm, for example, and ethical issues of which to be aware in managing the firm's Web site. We have explored thorny issues that

have been created by the 2006 amendments—the strange interplay between the "good cause" showing of Rule 26(b)(2)(B) and cost shifting in discovery, for one—of which the bench should be aware. We have made recommendations for resolving open questions—for example, as to whether computer-generated records should be considered hearsay, or not—for students and academics to ponder. For IT professionals and business managers, *Litigating with Electronically Stored Information* provides a helpful framework for understanding their roles and responsibilities in regard to a pending or active litigation, and the potential legal consequences of choices made for creating, storing, and destroying ESI. We believe this book will be indispensable not only for professional litigators, but also for those executives responsible for managing litigation and the information technology issues such litigation presents.

Acknowledgments

We authors thank Natallia Maroz for her assistance in preparing the manuscript. We also thank Karen, Kate, and Julia for their support; Marsha Pearcy and Sophie Sperduto for their perpetual patience; and Gary Edwards for his unfailing good humor.

Part I
Introduction

1

Overview

A man is flying in a hot air balloon and realizes that he is lost. He reduces his altitude and spots a man down below. He lowers the balloon further and says,

"Excuse me, can you tell me where I am?"

The man below says, "Yes. You are in a hot air balloon, hovering 30 feet above this field."

"You must work in Information Technology," says the balloonist.

"I do," replies the man, "How did you know?"

"Well," says the balloonist, "everything you have told me is technically correct, but it's no use to anyone."

The man below says, "You must be a lawyer."

"I am," replies the balloonist, "but how did you know?"

"Well," says the man, "You don't know where you are, or where you're going, but you expect me to be able to help. You're in the same position you were before we met, but now, it's my fault" [1].

Introduction

Some lawyers shudder at the notion of thinking about native format versus TIFF, and just want IT to take care of it. Other attorneys accept the challenges of managing electronically stored information (ESI), understand SQL databases and native file viewers, and use sophisticated litigation support software in putting a case together.

Whatever one's view of the mechanics of processing ESI, no attorney can avoid the more important task of understanding the law applicable to litigating with ESI, as that law is developing, evolving, and maturing. *Litigating with Electronically Stored Information* explores this considerable challenge. This book

covers decisions on a broad range of topics, ranging from the assertion of personal jurisdiction premised on Internet-based activity to the admission of an e-mail message offered to prove the truth of the matter asserted. While numerous important state cases are analyzed, the discussion emphasizes federal court decisions. The 2006 amendments to the Federal Rules of Civil Procedure receive particular attention; while those amendments clarify certain issues with respect to litigating with ESI, they raise many more. The courts are just beginning to issue decisions interpreting the amended rules. *Litigating with Electronically Stored Information* evaluates the new decisional authority, as well as the preamendment case law, which has informed the new outcomes [2].

But of course, understanding the new rules is just the starting point. The more exciting challenge is to use that understanding to compose creative arguments for winning the disputes that inevitably arise litigating with ESI. *Litigating with Electronically Stored Information* accepts that challenge with gusto. The authors have employed their combined expertise in technology and litigation to propose just such arguments. Can an argument be made that ephemeral ESI—or data that is created but never stored in any medium for any length of time by the creator—is subject to the duty to preserve? We think so, under certain circumstances [3]. Is data that must be restored to be usable "not reasonably accessible" *per se* within the meaning of Fed. R. Civ. P. 26(b)(2)(B)? We don't think so [4]. Can a good argument be devised that once the "good cause" showing has been made for the discovery of ESI "not reasonably accessible," it would be unfair to shift the costs of producing that ESI to the requesting party? We think so [5].

For those attorneys who want checklists, forms, and samples, this is not the book for you. If, however, your litigation practice brings you face to face with analytical conundrums involving ESI, we believe your understanding of the issues involved—and therefore the quality of your practice—will be enhanced by reading *Litigating with Electronically Stored Information.*

Litigating with Electronically Stored Information is, eponymously, for litigators and trial attorneys. But we also include materials that are, or should be, of concern to any attorney, and to the client, including a chapter specifically devoted to developing an effective ESI management policy [6]. And although the principal focus of the book is the law of civil procedure, we believe the enormous importance of ESI to criminal law and procedure today warrants a look at that subject. With the kind permission of Christopher Slobogin, Stephen C. O'Connell Professor of Law, University of Florida Fredric G. Levin School of Law, an authority in the field, we have reprinted excerpts from his *Transaction Surveillance by the Government* [7].

We conclude this overview with a road map of all the chapters to come. But first, we provide some common definitions, observations, and advice.

What Is ESI?

The Federal Rules of Civil Procedure do not define ESI, and the Sedona Conference Glossary defines ESI simply as "electronically stored information" [8]. The Conference of Chief Justices, Working Group on Electronic Discovery, defines electronically stored information as follows [9]:

> Electronically-stored information is any information created, stored, or best utilized with computer technology of any type. It includes but is not limited to data; word-processing documents; spreadsheets; presentation documents; graphics; animations; images; e-mail and instant messages (including attachments); audio, video, and audiovisual recordings; voicemail stored on databases; networks; computers and computer systems; servers; archives; backup or disaster recovery systems; discs, CDs, diskettes, drives, tapes, cartridges and other storage media; printers; the Internet; personal digital assistants, handheld wireless devices; cellular telephones; pagers; fax machines; and voicemail systems.

We interpret ESI as including everything other than the traditional paper documents or microfilm: raw or processed data streams, output from measuring or testing devices, text stored as editable word processing documents or scanned images, and everything in between. Of course, ESI also includes those paper documents and microfilm that have been converted to electronic form.

The all-inclusiveness of the definition—plus the fact that ESI is so readily created, replicated, and transmitted—means the volume of ESI is staggering. Reports on the volume of e-mail per user vary, but by way of example, a white paper published by The Radicati Group, Inc., reports the worldwide e-mail traffic in 2005 as 135.6 billion e-mail messages per day. Another study calculated that a company with a workforce of 100,000 created 22 million new e-mail messages per week. The volume of e-mail continues to grow: any current estimate will soon be out of date.

E-mail is but the tip of the iceberg. Electronics and the electronic records they create seem to have penetrated almost every facet of our lives. Most cell phones typically show the last ten incoming and the last ten outgoing calls complete with the number and the time and date stamp. Of course, the rest of the record is in the phone company's computer. Each time a driver uses FastPass or a similar device to drive through a tollgate an electronic record is created. Most systems in newer cars are managed by electronics, which create ESI, including but not limited to GPS tracking data. So-called smart homes depend on electronics to manage more than just the traditional security systems, and electronic data is created thereby.

By virtue of its volume and ubiquity, ESI has changed more worlds than one, including the practice of law.

What's So Different About Litigating with ESI?

For one thing, the procedural rules are different: the Federal Rules of Civil Procedure, and analogous state rules, have formalized significant differences between litigating with ESI and with paper documents. The rules of evidence are different: a significant body of law holds that computer-generated statements are not hearsay even if offered to prove the truth of the matter asserted. The professional rules of ethics are different: protecting metadata from inadvertent disclosure was not an issue in the paper world. These differences are explored in *Litigating with Electronically Stored Information.*

But on a more fundamental level, it is ESI that is different [10]. The differences between ESI and paper can facilitate litigation—searching active files for key phrases can be done in seconds—or complicate matters. For example: Litigation counsel to a software development company asks the client to prepare for production the first and last 25 pages of its software product. The software consists of components written in different programming languages and scripts, and because the software is event-driven it does not even contain the traditional main module. The closest equivalent to the main is a relatively simple Web page that fits on less than two traditional 8½ × 11-inch pages—which can be expanded into more or fewer pages, depending on the choice of font. Certainly none of the developers thinks of any component of this software in terms of pages or documents.

This example, and our introductory anecdote, underscore the importance of effective communication between the attorney and IT in litigating with ESI, another of the items in the what's so different category. From understanding what potentially discoverable ESI exists and where it may reside—a topic we cover in Chapter 7—to authenticating ESI as evidence at trial, IT must be involved as never before. This task in and of itself is a challenge. IT professionals do not, in general, use the term ESI: it is too broad a concept to have practical, day-to-day meaning and use. In an organization of any substantial size, IT comprises persons with very different roles and specialties, as well as outside vendors. Many information technology professionals are attracted to that profession because of an affinity for *technology*, not *information,* and it is only the latter that is truly of interest to the litigator. But, somehow, the attorney and IT have to figure out, together, exactly where that balloon is.

The Road Map to Litigating with ESI

This book is divided into parts that roughly correspond to the chronological stages of a lawsuit. This structure was designed to let busy litigators identify as quickly as possible that portion of the book most relevant to the ESI litigation

issue on the desk today. Part I, "Introduction," includes Chapter 1, "Overview," and Chapter 2, "Jurisdiction and the Internet."

Part II, "Practicing with New Procedures," begins with "Overview of the 2006 Amendments," including the Federal Rules of Civil Procedure and Committee notes in Chapter 3. Chapter 4, "Scope and Form of Production—Rule 34," covers amended Rule 34 and provides practical tips on requesting a particular form for production. Chapter 5 tackles the controversial topic of "Accessible Versus Inaccessible Data" within the meaning of amended Rule 26. Part II concludes with an analysis in Chapter 6, "Shifting the Costs of Discovery," a topic intimately tied to the accessibility of the ESI in the first place.

Part III, "ESI Discovery," begins with Chapter 7, "Planning for Discovery," which includes a discussion of methodologies for targeting the right evidence in the large, complex, and ever-expanding universe of potentially discoverable ESI. Chapter 8, "Responding to Discovery," includes a discussion of the basic functionalities any litigation support software should provide in order to facilitate the process and an attorney's guide to computer forensics. Chapter 9, "Discovery from Third Parties," completes Part III.

Part IV, "ESI and the Attorney-Client Relationship," includes issues unique to ESI and the client's duty to preserve evidence in Chapter 10, "Duty to Preserve." Chapter 11, "Inadvertent Disclosure of Privileged Information or Work Product," evaluates an increasingly common misadventure in the digitized world. Chapter 12, "Ethical Issues in Litigating with ESI," includes a survey on the topic. Chapter 13, "ESI Management," provides a creative and universal approach applicable to the client's operations and to the law firm.

Part V, "ESI in the Courtroom," begins with Chapter 14, "Authentication," which sets out the law and discusses the mixed results possible for unwary counsel. Chapter 15, "Hearsay," continues the analysis of ESI as evidence including an important proposal for determining when "purely computer generated" documents or data should be admissible as not being hearsay at all (remember, hearsay is the statement of a person). Chapter 16, "Preservation Orders," evaluates the topic in the world of ESI. In addition to an analysis of the case law, we also assess orders actually used in selected cases. Chapter 17, "Sanctions," evaluates the always-popular topic and provides analysis and practice tips for those confronting intractable adversaries or incurable self-assuredness. Finally, Chapter 18, "Transaction Surveillance by the Government," is an excerpt from Christopher Slobogin's article of the same title.

We understand that *Litigating with Electronically Stored Information* is necessarily a preview of those areas of the law that will develop and evolve, much like the technology underlying these issues. The case law as it matures will be the result of the creative arguments made by the attorneys wrestling with the issues. It is in that spirit that we dedicate this book to those trial attorneys and professional litigators who battle in the trenches every day. It is undoubtedly through

your trials and errors that the law applicable to litigating with ESI will be illuminated and improved.

Endnotes

[1] This anecdote has been floating around in various electronic mailing lists and the Internet for quite some time.

[2] *See, e.g.,* Semroth v. City of Wichita, 2006 U.S. Dist. LEXIS 83363 (D. Kan. 2006), discussed in Chapter 6, *infra.*

[3] *See* Chapter 10, *infra.*

[4] *See* Chapter 5, *infra.*

[5] *See* Chapter 6, *infra.*

[6] *See* Chapter 13, *infra.*

[7] Reprinted with permission from Christopher Slobogin, *Transaction Surveillance by the Government,* 75 MISS. L. J. 139–166 (2005), copyright Mississippi Law Journal 2005. Acknowledgments to other authors from whom we have obtained permission to reprint materials are referenced herein as appropriate.

[8] "The Sedona Conference Glossary for E-Discovery & Digital Information Management," May 2005 Version, http://thesedonaconference.org/content/miscFiles/tsglossaryMay05.pdf. The Sedona Conference publishes information and guidelines on cutting edge legal issues that are highly regarded by the bench and the bar.

[9] Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information,* August 2006.

[10] The unique characteristics of ESI that are generally noted include greater volume, dispersal, searchability, persistence, changeable content, underlying metadata, and environmental dependence. *See, e.g.,* The Sedona Conference Working Group Series, "The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production," pp. 3–6, July 2005 Version, http://thesedonaconference.org/contnet/miscFiles/7_05TSP.pdf.

2

Jurisdiction and the Internet

In personam jurisdiction: power which a court has over the defendant himself.... A court which lacks personal jurisdiction is without power to enter a personal or in personam judgment [1].

Introduction

Your client is a consulting firm offering architectural, design, and engineering services to commercial real estate developers. The firm is incorporated in New York and has offices in New York and California. The firm's principals are licensed in various jurisdictions but none of them are licensed to practice in the state of Vermont. The firm's Web site advertises its "national consulting practice." A prospective client can view videos of the firm's work-in-progress, and, by entering an e-mail address, download partial architectural plans and blueprints related to the firm's work. The firm has never had an engagement in Vermont, and has no other contacts with Vermont other than the fact that Vermont residents can access the Web site.

A dispute arises between the firm and one of its client developers over a "stop work" order on a project located in Texas. The developer is also a New York corporation, but it has offices across the United States, including in the state of Vermont. You receive a letter from counsel for the developer stating that if the matter cannot be resolved short of litigation, they intend to file suit in Vermont. What do you advise the client about whether it is going to have to defend a suit in Vermont?

As stated by the Supreme Court, the rules governing personal jurisdiction are intended to give "a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit" [2]. But an organization cannot predict where it may be liable to suit, and structure its conduct accordingly, without an understanding of the rules.

Internet-based activity—using the Internet to buy, sell, advertise, correspond, or collect information—can under certain circumstances subject the user to the jurisdiction of the courts of the state in which data sent via the Internet is accessed [3]. This chapter explains these certain circumstances. The resulting assessment of potential exposure to litigation in states where the organization has no office, employees, or other agents may be a factor to be considered in operational decisions. In addition, by having a grasp of the risks of litigation in foreign states, the organization can make whatever advance preparations for insuring against that risk it deems necessary.

Because citing Internet activity as a basis for the assertion of personal jurisdiction is a relatively recent strategy, the legal framework for assessing whether a court may exercise jurisdiction within the limits set by the due process clause of the Constitution and relevant state statutes is not well settled. No case has yet reached the Supreme Court. Moreover, the personal jurisdiction analysis is very fact specific. A court's decision in one case is rarely controlling in another because the facts in the two cases will inevitably differ. Accordingly, it is difficult to generalize about whether and when the use of the Internet will subject the user to suit. But some approximations can be made, and distinctions can be drawn among differing categories of Internet activity.

What follows, then, is a summary of the basic legal concepts defining in personam jurisdiction and those that are evolving in regard to Internet usage. The main focus, however, will be on the facts of the cases. The objective is to provide a rough matrix for assessing whether an organization's Internet-based operations are providing a basis for the assertion of personal jurisdiction in states other than those in which it physically operates [4].

Basic Legal Principles of Personal Jurisdiction

"Before a person or property may be subjected to the court's jurisdiction, the person or property must have the adequate territorial connection with the state and certain prescribed steps must be taken to subject that person or property to the court's authority" [5]. That "adequate territorial connection" is otherwise known as the proper jurisdictional basis. The "prescribed steps" that must be taken refer to service of process: delivering a summons and complaint to the

company's registered agent, for example. This chapter concerns only the former topic, or jurisdictional basis.

The due process clause limits the exercise of judicial jurisdiction. Otherwise stated, the due process clause, as construed by the courts, defines what is a proper jurisdictional basis. A court that exercises jurisdiction over the defendant in the absence of a proper jurisdictional basis violates the defendant's right not to be deprived of property without due process, and its judgment is therefore void.

A person who is domiciled in the forum, and a business organized under the laws of or having its principal place of business in a forum, are generally subject to the jurisdiction of the courts of that forum state. A nonresident, such as a business that accesses a state only through an Internet connection, may also be subject to jurisdiction in that foreign forum, as it is called.

The jurisdiction of state courts over nonresidents is defined by statute, and those statutory definitions of jurisdiction are upheld by the courts so long as they do not deny due process. In many states, the so-called long-arm statute that authorizes the assertion of jurisdiction over nonresident parties is coextensive in reach to the due process clause, either by the explicit terms of the statute or as construed by the courts [6]. In those states, the statutory and constitutional inquiries into the validity of exercising jurisdiction merge into one. In other states the exercise of personal jurisdiction must comply with the specific bases set forth in the long-arm statute, as well as due process requirements [7].

In general, the federal courts must also comply with the provisions of the long-arm statutes of the states within which they are located, [8] and this is true even if the cause of action is federal, and not state [9]. One exception to this rule is when a federal statute specifically confers personal jurisdiction over certain parties.

Due Process and Jurisdiction over Nonresident Parties

The starting point for analyzing the constitutional validity of exercising personal jurisdiction is the Supreme Court's opinion in *International Shoe Co. v. Washington* [10]. This case established the minimum contacts standard against which any assertion of jurisdiction must ultimately be measured. In particular, "due process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice'"[11].

The minimum contacts standard has been much refined. Cases decided by the Supreme Court after *International Shoe* that are of particular import to Internet-based contacts include *McGee v. International Life Ins. Co.* [12], holding

that a single transaction may be sufficient to support the exercise of jurisdiction if that one transaction has a "substantial" connection with the forum state. In *Hanson v. Denckla* [13], the Court held that the necessary minimum contacts do not exist unless "there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws" [14]. Fairness to the nonresident party requires that it be a foreseeable consequence of its conduct that it might be haled into the court of the forum state [15].

Foreseeability alone is not, however, sufficient. In *World-Wide Volkswagen Corp. v. Woodson* [16], the plaintiffs, New York residents, purchased a car in New York, were injured while driving that car through Oklahoma, and brought suit in an Oklahoma state court. The manufacturer did not sell its vehicles in Oklahoma and had made no efforts to establish business relationships in Oklahoma. Plaintiffs argued that because the manufacturer sold its products worldwide, it was foreseeable that a case could arise in any jurisdiction, including Oklahoma. The Court rejected that argument because Volkswagen itself had not purposefully directed any conduct towards residents of Oklahoma. Its only contact with Oklahoma was the fortuitous fact that the plaintiffs had driven their car into that state.

The necessary element of purposeful activity, or intention, was again explained in *Calder v. Jones* [17], a libel action. In *Calder*, the Court held that a California court had jurisdiction over Florida reporters who had written an allegedly libelous article for *The National Enquirer* about a California actress because the writers expressly aimed at California: the writers knew that California was the focal point of the story and that the brunt of the harm would be borne in California where the actress lived and worked and in which *The Enquirer* had its largest circulation. *Calder* is often called the effects test for determining whether jurisdiction can be asserted over a nonresident defendant acting outside the state who causes harm to a resident of another forum.

What constitutes sufficient contacts varies depending on whether the court is asserting general jurisdiction or specific jurisdiction. Specific jurisdiction may arise when a nonresident defendant purposefully avails itself of a jurisdiction and the plaintiff's alleged injuries arise out of those activities. If the court has general jurisdiction, it may render judgment on any cause of action. General jurisdiction exists if the plaintiff's injuries do not arise out of the nonresident's activities, but the defendant has maintained "substantial" or "continuous and systematic" contacts with the forum. Whether dealing with general or specific jurisdiction, the touchstone remains some purposeful conduct so that a party is not haled into a court solely as a result of "random" or "fortuitous events," or "attenuated" contacts [18].

Once it is shown that a party has minimum contacts with the forum state, it remains necessary to consider whether the balance of competing interests and

the nature and quality of the defendant's purposeful contacts render it fair to subject the defendant to jurisdiction in that state [19]. As Justice Brennan put it in *Burger King Corp. v. Rudzewicz* [20], "the concept of fair play and substantial justice may defeat the reasonableness of jurisdiction even if the defendant has purposefully engaged in forum activities." The fairness analysis includes four factors: the burden on the defendant; the forum state's interest in adjudicating the dispute; the plaintiff's interest in obtaining convenient and effective relief; and the interstate judicial system's interest in obtaining the most efficient resolution of controversies. *See Asahi Metal Indus. Co. v. Superior Court of California*, 480 U.S. 102, 121 (1987) (Stevens, J., concurring).

Jurisdiction and Internet Contacts

Today, virtually every business and organization operates a Web site. Accordingly, this category of Internet activity can almost always be cited as a contact with the forum state when personal jurisdiction is disputed by a nonresident party. The bulk of the reported decisions on jurisdiction and the Internet therefore concern the operation of a Web site, which is also, then, the main focus of what follows. The remainder of the chapter sets forth the basic outlines of how jurisdiction can be based on other types of Internet activities: posting information on Internet bulletin boards, sending e-mail, accessing remote servers, and purchasing goods on a Web site.

Operating a Web Site

A Web site establishes a continuous contact of sorts with every state in which the residents have Internet access. Some early decisions on jurisdiction and the Internet, focusing on that fact of constancy of access, found the mere operation of a Web site to suffice as a basis for personal jurisdiction. For example, in *Inset Systems, Inc. v. Instruction Set* [21], a Connecticut corporation sued a Massachusetts corporation in Connecticut, alleging trademark infringement. The defendant's contact with Connecticut consisted of a Web site accessible to approximately 10,000 Connecticut residents, and maintaining a toll-free number. The defendant contested the court's jurisdiction, relying on cases involving television and radio holding that national advertising not targeted to a particular forum would not support the exercise of jurisdiction. The court distinguished those cases on the grounds that the Web site was continuously available to any Internet user, and it held that jurisdiction was proper.

But that development was short lived. As stated by the United States Court of Appeals for the Fourth Circuit [22]: "If we were to conclude as a general principle that a person's act of placing information on the Internet subjects

that person to personal jurisdiction in each State in which that information is accessed, then the defense of personal jurisdiction, in the sense that a State has geographically limited judicial power, would no longer exist. The person placing information on the Internet would be subject to personal jurisdiction in every State."

Nonetheless, a Web site is a contact with the forum where it is accessed. Assessing the significance of that contact for jurisdictional purposes requires applying the due process principles with "some adaptation of those principles because the Internet is omnipresent …" [23].

Both state and federal courts generally apply one or more of two tests to assess whether a Web site constitutes the requisite minimum contacts for the assertion of special jurisdiction over a nonresident operator of a Web site: the *Zippo* sliding scale test measuring the interactivity of the site and, in cases where the operator is alleged to have committed an intentional tort (e.g., defamation), the effects test set forth in *Calder v. Jones*. Both tests measure the purposefulness of the Internet activity, using different metrics. The nature of what Internet activity suffices to constitute the substantial and continuous contacts necessary to exercise general jurisdiction is more of an open question, as discussed below.

In *Zippo Manufacturing Company v. Zippo Dot Com, Inc.* [24], Zippo Manufacturing, maker of Zippo lighters, brought suit in Pennsylvania against Dot Com, a California corporation with its principal place of business in California, alleging, *inter alia*, trademark dilution and infringement. Dot Com moved to dismiss for lack of personal jurisdiction.

Dot Com operated an Internet news service from the registered domain names zippo.com, zippo.net, and zipponews.com. Its contact with Pennsylvania was almost entirely through its Web site. Dot Com had some 140,000 subscribers worldwide, including 3,000 who were Pennsylvania residents. Those residents had subscribed for Dot Com's services through the Web site, and accessed Dot Com's news messages by entering their assigned password on the Web site. Dot Com advertised its services on its Web site, which advertisements were accessible by Pennsylvania Internet users. Dot Com had also entered into agreements with seven Internet access providers in Pennsylvania.

The court framed its analysis with the following observations [25]:

> … the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite

> end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. (Citations omitted.)

The court in *Zippo* went on to conclude that Dot Com was at one end of the spectrum: it was doing business, albeit that business was conducted electronically, with Pennsylvania residents, having "sold passwords to approximately 7,000 subscribers in Pennsylvania and entered into seven contracts with Internet access providers to furnish its services to their customers in Pennsylvania" [26]. It rejected Dot Com's argument that those contacts were fortuitous because its Pennsylvania subscribers happened to find its Web site. Because Dot Com "repeatedly and consciously chose to process Pennsylvania residents' applications," and "freely chose" to do so, its contacts were "purposeful availment" and not fortuitous or coincidental. "If Dot Com had not wanted to be amenable to jurisdiction in Pennsylvania, the solution would have been simple—it could have chosen not to sell its services to Pennsylvania residents" [27].

The effects test applied to information published on a Web site is a fairly straightforward replication of the principles set forth in *Calder v. Jones* regarding a print medium. That is, to establish jurisdiction it must be shown that (1) the defendant committed an intentional tort; (2) the plaintiff felt the brunt of the harm in the forum; and (3) the defendant expressly aimed his tortious conduct at the forum, such that the forum can be said to be the focal point of the tortious activity [28].

What the result of applying the Zippo sliding scale or the effects test will be in a particular case is not comfortably predictable [29]. The concept of level of interactivity is imprecise. What information on a Web site is sufficient to show that the operator expressly aimed at a forum cannot readily be quantified in advance. But at least an organization can predict what facts the courts will consider in evaluating a Web site for the significance and sufficiency of its contacts with a forum.

The following is a sampling of the facts of specific cases in which personal jurisdiction was contested [30], representing the range of most passive to most interactive sites, and least to greatest effects in the forum state. These cases are grouped by whether the sites were primarily transactional, membership-based, or informational, to assist an organization in quickly assessing the rules in regard to its Web site: the analytical framework is the same for all types.

Transactional

- In *Poly-America v. Shrink Wrap International, Inc.* [31], a cybersquatting dispute, the plaintiff brought suit in Texas against a competitor, a Michigan corporation, whose only contact with the forum was its Web site. The site had a link for sending e-mail, but did not include any forms for ordering products. The plaintiff had produced no evidence that the defendant had made any sales on its site. This passive Web site, the court held, did not support the exercise of personal jurisdiction.
- In *Butler v. Beer Across America* [32], plaintiff brought suit in Alabama against three Illinois corporations based on a state statute authorizing civil actions against a person who sells liquor to a minor. The plaintiff's minor son had placed an order, paid for with a credit card, for twelve bottles of beer on Beer Across America's Web site. The bottles had duly been delivered to his home in Alabama. In regard to the Web site, the court found it to have a "limited degree of interactivity" because the site was similar to an "electronic version of a postal reply card" and did not provide for the regular exchange of information. Accordingly, the site was insufficient to satisfy the minimum contacts requirement. Finding no other significant contacts with the forum (e.g., defendants' total volume of sales to Alabama was "minor" and it did not target Alabama in marketing or sales) the court declined to exercise jurisdiction.
- In *Visage Spa v. Salon Visage, Inc.* [33], a patent infringement case brought in Michigan, the court found that it did not have personal jurisdiction over the defendant whose Web site only passively displayed information and did not offer goods for sale. But as to the other defendant, whose site offered to sell gift certificates and other products, the court held that it did have personal jurisdiction because the site was sufficiently interactive, even though the evidence showed that only a single gift certificate had been sold to a Michigan resident. "If Defendant Spa was not intending for residents of Michigan to purchase gift certificates from its Web site, then it would have limited its sales to states other than Michigan, or simply refused to sell to anyone located in Michigan." The court found that the effects test was also passed because the defendant had allegedly committed an intentional tort—posting an infringing mark on its Web site—and had notice that another claimed the mark. Further, the brunt of the harm occurred in Michigan, where plaintiff was located.
- In *Snowney v. Harrah's Entertainment, Inc.* [34], plaintiff filed a class action in California alleging fraud and deceptive business practices

arising from the imposition of an energy surcharge on a hotel bill. The defendants, Nevada corporations, operated a Web site that quoted room rates and permitted visitors to make hotel reservations on the site. The site also touted its proximity to California and provided directions from California to the hotels. The court found that the site was interactive and, at a "minimum," in the "middle ground" of the Zippo sliding scale. Further, by specifically targeting California residents, defendants had "purposely availed" themselves of doing business in California, such that the court could exercise special jurisdiction over the nonresident defendants. The court noted that, even if the Web site were not alone enough to confer jurisdiction, defendants had other contacts with California, including billboard and print advertising in the state.

- In *Hsin Ten Enter. USA, Inc. v. Clark Enter.* [35], a New York corporation sued a Kansas corporation in New York for patent infringement arising from defendant's marketing and sales of certain exercise equipment. The court found that the defendant's "highly interactive" Web site, on which customers could purchase equipment, download an order form, and talk to an online representative, in combination with other contacts with the forum (e.g., participation at trade shows in New York) satisfied the "transacts business" section of the long-arm statute, N.Y. C.P.L.R. § 302(a)(1), as well as due process requirements.
- In *Gator.com Corp. v. L.L. Bean, Inc.* [36], a declaratory judgment suit brought by a California corporation against a Maine corporation, a panel of the Ninth Circuit held that L.L. Bean's "virtual store" sales in California constituted such "substantial and continuous" business as to support the exercise of general jurisdiction. Using the sliding scale analysis, the court found L.L. Bean's Web site to be "highly interactive" and its "millions of dollars in sales, driving by an extensive, ongoing, and sophisticated sales effort involving very large numbers of direct email solicitations" clearly constituted doing business in the state. The decision was vacated for rehearing en banc, but the appeal was ultimately dismissed as moot.
- In *Lakin v. Prudential Securities, Inc.* [37], plaintiff brought a negligence and breach of fiduciary duty action in Missouri against Prudential, a Georgia corporation. Prudential operated a Web site which the court found to be "under the middle category" of the Zippo scale. Missouri visitors to the site could establish and access online accounts, apply for home-equity loans and lines of credit, and exchange e-mail with customer service representatives. The court found this degree of interactivity "not sufficient" for the exercise of general jurisdiction (which would be necessary given that the claim did not relate to

Prudential's contacts with Missouri). However, it remanded to allow the plaintiff to conduct discovery to determine whether the quantity of Prudential's contacts through its Web site would be sufficient to exercise general jurisdiction. Specifically, the court noted that the issue would depend on the number of times Missouri customers accessed the Web site; the number of Missouri customers that requested information about services; the number of Missouri residents that applied for loans online; the number of times a representative responded to Missouri residents; and the number and amount of home-equity loans that resulted from online applications.

Membership

- In *Rescuecom Corporation v. Hyams* [38], a New York corporation brought suit in New York against a resident of Texas for violation of a franchise agreement. Defendant operated a Web site that allegedly warned prospective franchisees about plaintiff's franchise operation and provided links to competitors. On the Web site, visitors could register, receive a log-in name and password, and thereafter post messages to each other. At least two registered members were New York residents. Plaintiff argued that this Web site constituted the transaction of business within the meaning of New York's long-arm statute. The court disagreed. Finding that the site was in the "middle ground" of interactivity, it noted that with respect to such sites courts distinguish between those with significant commercial elements, which typically are found to constitute the transaction of business, and those lacking significant commercial elements, which typically are not. Because defendant's Web site offered nothing for sale and did not generate income in any other manner, its operation did not satisfy the requirements of the statute.

- In *Waka v. DCKickball* [39], plaintiff brought suit in Virginia against a District of Columbia nonprofit corporation for copyright infringement and defamation. The defendant operated a Web site on which it solicited kickball teams to register to play in D.C., for payment of a registration fee. The site also solicited e-mail addresses. The evidence also showed that a number of Virginia residents had accepted the defendant's offer to play in D.C. The court found the site sufficiently "interactive" and of a commercial nature to satisfy the "minimum contacts" requirement. It also found that the defendant's Web site satisfied Virginia's long-arm statute authorizing jurisdiction over a party that

"regularly does or solicits business" in Virginia because the Web site could be accessed by a Virginia resident 24 hours per day.

- In *Gather, Inc. v. Gatheroo* [40], plaintiff filed a trademark infringement action in Massachusetts against two Minnesota entities. On defendants' Web site, http://gatheroo.com, visitors were invited to register and become members. Members received an e-mail with a hyperlink to Web sites containing links to groups or members from their home states. Seven registrants were from Massachusetts. The site also solicited advertisers, which solicitations were "available" to Massachusetts residents; the business was in an early stage and had not yet generated any advertising revenues. The court found the site sufficiently showed "purposeful availment" to assert specific jurisdiction based on the facts that Gatheroo accepted members from Massachusetts, communicated directly with Massachusetts users, provided information specifically about Massachusetts to Massachusetts users, and solicited advertisers from users, including those in Massachusetts. The court rejected defendants' argument that the number of users was too few to establish jurisdiction.

Informational

- In *The Cadle Company v. Schlichtmann* [41], the plaintiff brought a defamation action in Ohio against a resident of Massachusetts who operated a Web site informing others of what he believed were plaintiff's unlawful activities in Massachusetts. The site also contained contact information for persons interested in learning about efforts to stop plaintiff's allegedly illegal practices in Massachusetts. The court of appeals found the site to be "semi-interactive." Proceeding to the next step of the Zippo analysis for such sites, the "level of interactivity and commercial nature of the exchange of information" that occurs on the site, the court found no evidence that any interaction or exchange of information occurred with any Ohio resident, so that the site did not support the exercise of personal jurisdiction based on the "nature of the Web site." The court also looked to the effects test, but because the site referred only to plaintiff's activities in Massachusetts, and did not target Ohio readers, the court concluded that the operator of the site had not purposefully availed himself in Ohio via the Web site.
- In *Carefirst of Maryland, Inc. v. Carefirst Pregnancy Centers* [42], plaintiff brought a trademark infringement action in Maryland against CPC, an Illinois nonprofit. CPC was a prolife organization providing assistance to Chicago-area women. Its Web site provided information to

pregnant women about nutrition and prenatal care, offered pregnancy testing, and solicited donations. CPC had received $1,542 in donations from Maryland residents, but only one—made by the lawyer for the plaintiff—was made through the Web site. The court found the site to be "semi-interactive" on the Zippo scale because it allowed users to exchange information with the host. But because the level of interactivity with Maryland residents was minimal—the evidence showed only the one donation—and the overall content of the site was "strongly local" to the Chicago area, the court found that CPC had not directed sufficient electronic activity into Maryland to support jurisdiction.

- In *Northwest Healthcare Alliance Inc. v. Healthgrades.com* [43], a home health-care provider brought a defamation action in Washington against a Delaware company with its principal place of business in Colorado. The defendant published ratings of home health-care providers on its Web site, and had rated plaintiff unfavorably. The court found that the site satisfied the effects test because the operator was "well aware that its ratings of Washington home health providers would be of value primarily to Washington consumers," the rating concerned the Washington activities of a Washington resident, and the brunt of the harm allegedly suffered occurred in Washington, where plaintiff operated. Accordingly, the assertion of personal jurisdiction would be appropriate.

Other Internet Activities

Posting information on a Web site is largely analogous to printing or broadcasting information, and is subjected to much the same analysis for jurisdictional purposes. However, because of the unique omnipresence of such material, the relative interactivity of the site on which it is posted may be considered, as well. For example, in *Revell v. Lidov* [44], plaintiff brought a defamation action in Texas against Columbia University and the author of an allegedly defamatory article, a Massachusetts resident. The article was posted on an Internet bulletin board maintained by Columbia's School of Journalism. The subject of the article was the bombing of Pan Am Flight 103. In the article Lidov alleged that senior members of the Reagan Administration conspired to cover up the fact that the administration had advance warning of the terrorists' intent to bomb the plane but did nothing to stop it. Revell was specifically named as a member of the alleged conspiracy. The court found the bulletin board itself to be insufficiently interactive to create specific jurisdiction. Turning then to the Calder effects test, the court observed that Lidov had stated in an affidavit that he did not know Revell was a resident of Texas. Because "[k]nowledge of the particular

forum in which a potential plaintiff will bear the brunt of the harm forms an essential part of the Calder test," and there was nothing in the posted article directed specifically at Texas, the court in Texas did not have personal jurisdiction over the defendant [45].

A similar result was reached in *Pettus v. Combs* [46], a defamation action arising from a message posted on eBay. The suit was brought in Texas against a resident of New York. Though the message posted on eBay was directed to the plaintiff, the defendant did not know the plaintiff was a Texas resident at the time of the posting, and nothing about the subject matter of the message was directed to Texas. Accordingly, the court concluded, the defendant was not subject to personal jurisdiction in Texas.

If, however, the author of content posted on an Internet bulletin board knows where the subject of the posted material is located, and the brunt of the harm allegedly resulting from the contents of the post is felt in the same forum, the author may be subject to personal jurisdiction in that forum.

For e-mail, the rules established for its communication analogs—letters, and wire and facsimile transmissions—largely suffice. Thus, sending a single e-mail into a forum, like sending one letter, may sustain the exercise of specific jurisdiction if that contact has a substantial connection with the forum [47]. More commonly, jurisdiction could not properly be asserted based on one or a few e-mail contacts with a forum, just as it could not be based on a few telephone calls [48].

But if the requisite purposeful availment is present, the fact that the mailer contacted only a few residents of the forum does not defeat jurisdiction. For example, in *First Act, Inc. v Brook Mays Music Company* [49], plaintiff filed a defamation action in Massachusetts against a Texas corporation. Both the defendant and plaintiff manufactured and sold musical instruments. The defendant had sent e-mail to 8,000 persons across the country addressing the quality of the plaintiff's instruments. Sixty of these persons were Massachusetts residents. The court found that the assertion of specific jurisdiction was proper and complied with the Calder test because the defendant sent the e-mail to persons on a list that it maintained and controlled. Thus, defendant knew, or should have known, who would receive the e-mail, including residents of Massachusetts, and had, therefore, purposefully directed its conduct toward the forum.

Accessing servers from outside the forum state may subject a nonresident party to the jurisdiction of the forum in which these servers are located:

- In *Traveljungle v. American Airlines, Inc.* [50], Traveljungle, a company registered in the United Kingdom with principal places of business in Germany and Bulgaria, operated a Web site that gathered travel information in response to requests from site visitors. American contended that Traveljungle used "screen-scraping software" to extract fares and

other information from American's Web site, which conduct, it alleged, was tortious, breach of contract, and in violation of Texas state statutes. American argued that this "contact" with its servers, which were located in Texas, supported the exercise of jurisdiction in Texas, in which the suit was brought. Traveljungle argued that its contacts with Texas were insufficient—because it only occasionally "viewed" American's site—and fortuitous because it had no knowledge that the servers were located in Texas. But the court found that by "deliberately directing its activity toward AA.com, Traveljungle should have been aware of the possibility that it would be haled into any forum where AA.com's servers were located" [51].

- In *Intercon, Inc. v. Bell Atlantic Internet Solutions, Inc.* [52], defendant, a Delaware corporation and provider of e-mail service, mistakenly routed its customers' e-mail messages to the wrong domain name for a period of time, thereby using plaintiff's mail server during that time. Plaintiff's staff noticed a slow-down on its server and contacted defendant several times before defendant took steps to halt the problem. Plaintiff sued for damages in Oklahoma, where its server was located. The court found that defendant had "purposefully directed its conduct toward Oklahoma" from the time it was advised of the problem by plaintiff, such that the assertion of jurisdiction was appropriate.
- In *Earthlink, Inc. v. Pope* [53], Earthlink brought an action in Georgia against a number of parties alleging, *inter alia*, federal civil RICO violations, conversion, and trespass. Plaintiff alleged that defendants used fictitious names and credit cards to purchase Earthlink accounts, which were then used to send illegal spam e-mail. The nonresident defendants argued that the court did not have jurisdiction because the plaintiff had not shown that a substantial number of the unsolicited e-mail was sent to Georgia and that their only other connection to Georgia was the initial dial-up to purchase the accounts. The court found that defendants' "substantial other activity within Earthlink's Georgia network," including connections to and from the Earthlink network to make the spam e-mail appear to originate from Earthlink, constituted sufficient "electronic contact" to support the assertion of jurisdiction.
- In *Flowserve Corporation v. Midwest Pipe Repair* [54], plaintiff brought an action in Texas against a former employee and his current employer alleging misappropriation of trade secrets and conversion. The employee allegedly misappropriated the confidential information from outside Texas using the Internet to access plaintiff's server located in Texas. Applying the Calder effects test, the court found that defendant was subject to jurisdiction in Texas because he committed tortious acts

outside the state, directed at the forum state, which acts had foreseeable effects on the plaintiff in the forum state.

The courts are split on whether an online auction sale subjects the seller to jurisdiction in the forum where the buyer is located. The traditional rule is that by contracting to provide goods and services to a resident of a forum the seller subjects itself to the jurisdiction of the buyer's forum. Applying that rule to online auction sales, some courts have found the exercise of jurisdiction to be appropriate. In *Tindall v. One 1973 Ford Mustang,* for example, nonresident defendants sold a car on eBay to a Michigan resident, and the court found that the dispute arising from that sale could properly be heard in Michigan. The sale amounted to the transaction of business in the state, giving the Michigan court personal jurisdiction [55].

But the majority of courts have concluded "that the Internet and particularly an eBay transaction may alter the jurisdictional analysis…" [56]. Unlike phone calls or written correspondence directed into a forum for the purpose of consummating a deal, an Internet-based contract may be random in regard to the location of the parties. The court so found in *Boschetto v. Hansing* [57], declining to exercise jurisdiction in California over Wisconsin defendants in a breach of contract action arising from the sale of a car on eBay. The court followed the "overwhelming majority of courts" that have held that an eBay seller does not purposefully avail himself of the privilege of doing business in a forum state absent some additional conduct directed at the forum state. The court in *Boschetto* further noted that "too easy a test" of personal jurisdiction would put too great a burden on Internet commerce.

However, a party regularly doing business over the Internet—purchasing or selling—with residents of a particular forum would likely have subjected itself to the jurisdiction of that forum. See also the "Operating a Web Site" section of this chapter.

Conclusion

The Internet has obviously changed the rules for doing business. It has opened even the smallest storefront to shoppers around the world, and allows for the continuous and convenient interchange of an unparalleled amount of information. New technologies do not, however, change the fundamental principles of jurisdiction. While persons "should not be permitted to take advantage of modern technology via the Internet or other electronic means to escape traditional notions of jurisdiction" [58], persons using the Internet to conduct business are also protected by the precepts of fairness governing the exercise of personal jurisdiction. At bottom, only if it is fair and a foreseeable consequence of an

organization's Internet activities that it be haled into the court of a particular state will the rules require it to defend the consequences of those activities in that state.

Applying these principles to our opening hypothetical, the most likely answer to the client's question is no, unless the site's interactive features had been used by some significant number of Vermont residents.

Endnotes

[1] Black's Law Dictionary, 544 (6th ed. 1991), (Centennial Edition, Abridged).

[2] World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

[3] This chapter examines jurisdictional principles regarding only civil matters.

[4] This chapter does not cover international law insofar as it may affect the assertion of jurisdiction over an alien corporation in U.S. courts or whether and to what extent a U.S. corporation may be subject to suit in another country. For various topics in this extensive arena s*ee, e.g.*, Gavin R. Skene, *International Law and Technology,* Article*: The Extraterritorial Operation of Australian E-Commerce Legislation*, 13 TUL. J. INT'L & COMP. L. 219 (2005); Brian Fitzgerald, *Case Note: Dow Jones & Co., Inc. v. Gutnick: Negotiating "American Legal Hegemony"* in the Transnational World of Cyberspace, 27 MELB. U. L. Rev. 590 (2003); Gregory J. Wrenn, Article: *Cyberspace Is Real, Natural Borders Are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace,* 38 STAN. J. INT'L L. 97 (2002); Tapio Puurunen, Article: *The Legislative Jurisdiction of States Over Transactions in International Electronic Commerce,* 18 J. MARSHALL J. COMPUTER & INFO. L. 689 (2000).

[5] Moore, J. W., *Federal Practice*, § 108.01[1] (3rd ed. 2003).

[6] *E.g.,* Bancroft & Masters, Inc. v. Augusta Nat'l Inc.*,* 223 F.3d 1082, 1086 (9th Cir. 2000); Shoppers Food Warehouse v. Moreno, 746 A.2d 320, 329 (D.C. 2000).

[7] Moore, J. W., *Federal Practice* § 108.60[3][a] (3rd ed. 2003).

[8] *See* Fed. R. Civ. P. 4(k)(1)(A).

[9] *E.g.,* Graphic Controls Corporation v. Utah Medical Products, 149 F.3d 1382, 1385–1386 (Fed. Cir. 1998).

[10] 326 U.S. 310 (1945).

[11] *Id.* at 316 (citations omitted).

[12] 355 U.S. 220, 223 (1957).

[13] 357 U.S. 235 (1958).

[14] *Id.* at 253.

[15] *See* Shaffer v. Heitner, 433 U.S. 186 (1977).

[16] 444 U.S. 286 (1980).

[17] 465 U.S. 783 (1984).

[18] Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985).

[19] *Id.* at 476.

[20] 471 U.S. 462, 477–78 (1985).

[21] 937 F. Supp. 161 (D. Conn. 1996).

[22] ALS Scan, Inc. v. Digital Service Consultants, Inc., 293 F.3d 707, 712 (4th Cir. 2002).

[23] *Id.*

[24] 952 F. Supp. 1119 (W.D. Pa. 1997).

[25] *Id.* at 1124.

[26] *Id.* at 1125–26.

[27] *Id.* at 1126–27.

[28] *See, e.g.,* IMO Indus., Inc. v. Kiekert AG, 155 F.3d 254, 265-66 (3d. Cir. 1988).

[29] Some jurisdictions apply the Zippo sliding scale and the principles of Calder as separate tests. *See* Northwest Healthcare Alliance, Inc. v. Healthgrades.com., Inc., 50 Fed. Appx. 339, 340 (9th Cir.), *cert. denied*, 2003 U.S. LEXIS 3267 (2003). The Fourth Circuit has adopted and adapted the Zippo sliding scale so that it is effectively congruent with the effects test, s*ee* ALS Scan, Inc. v. Digital Services Consultants, Inc.*,* 293 F.3d at 714, and there are variations in between. The distinction may become important. As one court noted, it would be a "difficult question" to decide whether a Web site that failed the Zippo test could still give rise to jurisdiction under the *Calder* test. *See* Revell v. Lidov, 317 F.3d 467, 472, n. 30 (5th Cir. 2002).

[30] The following are decisions on the defendant's motion to dismiss for lack of personal jurisdiction. To defeat such a motion the opposing party need only make a *prima facie* showing that the defendant is subject to the jurisdiction of the court. *E.g.,* Carefirst of Maryland, Inc. v. Carefirst Pregnancy Centers, 334 F.3d 390 (4th Cir. 2003). The court's decision on a motion to dismiss is often dispositive, but the issue could again be raised in a motion for summary judgment should sufficient additional facts be adduced to justify revisiting the issue.

[31] 2004 U.S. Dist. LEXIS 7875 (N.D. Tex. 2004).

[32] 83 F. Supp. 2d 1261 (N.D. Alab. 2000).

[33] 2006 U.S. Dist. LEXIS 51824 (E.D. Mich. 2006).

[34] 35 Cal. 4th 1054 (2005).

[35] 138 F. Supp. 2d 449 (S.D. N.Y. 2000).

[36] 341 F.3d 1072 (9th Cir. 2002), *vacated, rehearing on banc granted*, 366 F.3d 789 (9th Cir. 2003), *appeal dis'd as moot*, 398 F.3d 1125 (9th Cir. 2005).

[37] 348 F.3d 704 (8th Cir. 2003).

[38] 2006 U.S. Dist. LEXIS 45282 (N.D. N.Y. 2006).

[39] 2006 U.S. Dist. LEXIS 34501 (E.D. Va. 2006).

[40] 2006 U.S. Dist. LEXIS 52849 (D. Mass. 2006)

[41] 123 Fed. Appx. 675 (6th Cir. 2005).

[42] 334 F.3d 390 (4th Cir. 2003).

[43] 50 Fed. Appx. 339 (9th Cir.), *cert. denied*, 2003 U.S. LEXIS 3267 (2003).

[44] 317 F.3d 467 (5th Cir. 2002).

[45] The court also dismissed the complaint against Columbia, without specifically distinguishing between the results of the effects test as applied to the person posting the article and the operator of the Web site on which the article was posted.

[46] 2006 U.S. Dist. LEXIS 39279 (W.D. Tex. 2006).

[47] *See* Internet Doorway, Inc. v. Parks, 138 F.Supp. 2d 773, 779 (S.D. Miss. 2001).

[48] *See, e.g.,* Rice v. Karsch, 154 Fed. Appx. 454, 463 (6th Cir. 2005).

[49] 311 F. Supp. 2d 258 (D.Mass. 2004).

[50] 2006 Tex. App. LEXIS 10634 (2006).

[51] *Id.* at *24, 25.

[52] 205 F. 3d 1244 (10th Cir. 2000).

[53] 2006 U.S. Dist. LEXIS 66596 (N.D. Ga. 2006).

[54] 2006 U.S. Dist. LEXIS 4315 (N.D. Tex. 2006).

[55] 2006 U.S. Dist. LEXIS 29621 (E.D. Mich. 2006), *See also* Malcolm v. Esposito, 63 Va. Cir. 440 (Fairfax 2003), also involving the sale of one car on eBay. But the court in *Malcolm* also noted several factors in addition to the fact that the nonresident had entered into a contract in Virginia supporting its assertion of jurisdiction: defendants made multiple sales on eBay, advertised that they had national and international clients, and sent a winning bidder e-mail to plaintiff.

[56] Boschetto v. Hansing, 2006 U.S. Dist. LEXIS 50807 (N.D. Cal. 2006).

[57] *Id.*

[58] Peridyne Tech. Solutions LLC v. Matheson Fast Freight, Inc., 117 F. Supp. 2d 1366, 1371 (N.D. Ga. 2000) (citations omitted).

Part II
Practicing with New Procedures

3

Overview of the 2006 Amendments

This chapter sets forth the text of the 2006 amendments to the Federal Rules of Civil Procedure and the Committee Notes on these amendments. Each of the amendments is explored in detail in subsequent chapters; this is intended to be a convenient reference to all the amendments.

Rule 16. Pretrial Conferences; Scheduling; Management

. . .

(b) Scheduling and Planning. Except in categories of actions exempted by district court rule as inappropriate, the district judge, or a magistrate judge when authorized by district court rule, shall, after receiving the report from the parties under Rule 26(f) or after consulting with the attorneys for the parties and any unrepresented parties by a scheduling conference, telephone, mail, or other suitable means, enter a scheduling order that limits the time

1. To join other parties and to amend the pleadings;
2. To file motions;
3. To complete discovery.

   The scheduling order may also include

4. Modifications of the times for disclosures under Rules 26(a) and 26(e)(1) and of the extent of discovery to be permitted;

5. Provisions for disclosure or discovery of electronically stored information;
6. Any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production;
7. The date or dates for conferences before trial, a final pretrial conference, and trial;
8. Any other matters appropriate in the circumstances of the case.

The order shall issue as soon as practicable but in any event within 90 days after the appearance of a defendant and within 120 days after the complaint has been served on a defendant. A schedule shall not be modified except upon a showing of good cause and by leave of the district judge or, when authorized by local rule, by a magistrate judge.

. . .

Notes of Advisory Committee on 2006 Amendments

The amendment to Rule 16(b) is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur. Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information if such discovery is contemplated in the action. Form 35 is amended to call for a report to the court about the results of this discussion. In many instances, the court's involvement early in the litigation will help avoid difficulties that might otherwise arise.

Rule 16(b) is also amended to include among the topics that may be addressed in the scheduling order any agreements that the parties reach to facilitate discovery by minimizing the risk of waiver of privilege or work-product protection. Rule 26(f) is amended to add to the discovery plan the parties' proposal for the court to enter a case management or other order adopting such an agreement. The parties may agree to various arrangements. For example, they may agree to initial provision of requested materials without waiver of privilege or protection to enable the party seeking production to designate the materials desired or protection for actual production, with the privilege review of only those materials to follow. Alternatively, they may agree that if privileged or protected information is inadvertently produced, the producing

party may by timely notice assert the privilege or protection and obtain return of the materials without waiver. Other arrangements are possible. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.

An order that includes the parties' agreement may be helpful in avoiding delay and excessive cost in discovery. *See Manual for Complex Litigation* (4th) § 11.446. Rule 16(b)(6) recognizes the propriety of including such agreements in the court's order. The rule does not provide the court with authority to enter such a case management or other order without party agreement, or limit the court's authority to act on motion.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

. . .

(a) Required Disclosures; Methods to Discover Additional Matter.

(1) Initial disclosures. Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:

(A) The name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) A copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment.

. . .

Notes of Advisory Committee on 2006 Amendments. Note to Subdivision (a)

Rule 26(a)(1)(B) is amended to parallel Rule 34(a) by recognizing that a party must disclose electronically stored information as well as

documents that it may use to support its claims or defenses. The term "electronically stored information" has the same broad meaning in Rule 26(a)(1) as in Rule 34(a). This amendment is consistent with the 1993 addition of Rule 26(a)(1)(B). The term "data compilations" is deleted as unnecessary because it is a subset of both documents and electronically stored information.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

. . .

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

. . .

(2) Limitations.

(A) By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

(B) A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(C) The frequency or extent of the use of discovery methods otherwise permitted under these rules.

. . .

Note to Subdivision (b)(2)

The amendment to Rule 26(b)(2) is designed to address issues raised by difficulties in locating, retrieving, and providing discovery of some electronically stored information. Electronic storage systems often make it easier to locate and retrieve information. These advantages are properly taken into account in determining the reasonable scope of discovery in a particular case. But some sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible.

It is not possible to define in a rule the different types of technological features that may affect the burdens and costs of accessing electronically stored information. Information systems are designed to provide ready access to information used in regular ongoing activities. They also may be designed so as to provide ready access to information that is not regularly used. But a system may retain information on sources that are accessible only by incurring substantial burdens or costs. Subparagraph (B) is added to regulate discovery from such sources.

Under this rule, a responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery. The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.

A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.

The volume of—and the ability to search—much electronically stored information means that in many cases the responding party will be able to produce information from reasonably accessible sources that will fully satisfy the parties' discovery needs. In many circumstances the requesting party should obtain and evaluate the information from such sources before insisting that the responding party search and produce

information contained on sources that are not reasonably accessible. If the requesting party continues to seek discovery of information from sources identified as not reasonably accessible, the parties should discuss the burdens and costs of accessing and retrieving the information, the needs that may establish good cause for requiring all or part of the requested discovery even if the information sought is not reasonably accessible, and conditions on obtaining and producing the information that may be appropriate.

If the parties cannot agree whether, or on what terms, sources identified as not reasonably accessible should be searched and discoverable information produced, the issue may be raised either by a motion to compel discovery or by a motion for a protective order. The parties must confer before bringing either motion. If the parties do not resolve the issue and the court must decide, the responding party must show that the identified sources of information are not reasonably accessible because of undue burden or cost. The requesting party may need discovery to test this assertion. Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party's information systems.

Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery. The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

The responding party has the burden as to one aspect of the inquiry—whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and

produce whatever responsive information may be found. The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information. In some cases, the court will be able to determine whether the identified sources are not reasonably accessible and whether the requesting party has shown good cause for some or all of the discovery, consistent with the limitations of Rule 26(b)(2)(C), through a single proceeding or presentation. The good-cause determination, however, may be complicated because the court and parties may know little about what information the sources identified as not reasonably accessible might contain, whether it is relevant, or how valuable it may be to the litigation. In such cases, the parties may need some focused discovery, which may include sampling of the sources, to learn more about what burdens and costs are involved in accessing the information, what the information consists of, and how valuable it is for the litigation in light of information that can be obtained by exhausting other opportunities for discovery.

The good-cause inquiry and consideration of the Rule 26(b)(2)(C) limitations are coupled with the authority to set conditions for discovery. The conditions may take the form of limits on the amount, type, or sources of information required to be accessed and produced. The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. A requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause. But the producing party's burdens in reviewing the information for relevance and privilege may weigh against permitting the requested discovery.

The limitations of Rule 26(b)(2)(C) continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

. . .

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

. . .

(5) Claims of Privilege or Protection of Trial Preparation Materials.

(A) Information withheld. When a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection.

(B) Information produced. If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

. . .

Note to Subdivision (b)(5)

The Committee has repeatedly been advised that the risk of privilege waiver, and the work necessary to avoid it, add to the costs and delay of discovery. When the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed. Rule 26(b)(5)(A) provides a procedure for a party that has withheld information on the basis of privilege or protection as trial-preparation material to make the claim so that the requesting party can decide whether to contest the claim and the court can resolve the

dispute. Rule 26(b)(5)(B) is added to provide a procedure for a party to assert a claim of privilege or trial-preparation material protection after information is produced in discovery in the action and, if the claim is contested, permit any party that received the information to present the matter to the court for resolution.

Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production. The courts have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information. Rule 26(b)(5)(B) provides a procedure for presenting and addressing these issues. Rule 26(b)(5)(B) works in tandem with Rule 26(f), which is amended to direct the parties to discuss privilege issues in preparing their discovery plan, and which, with amended Rule 16(b), allows the parties to ask the court to include in an order any agreements the parties reach regarding issues of privilege or trial-preparation material protection. Agreements reached under Rule 26(f)(4) and orders including such agreements entered under Rule 16(b)(6) may be considered when a court determines whether a waiver has occurred. Such agreements and orders ordinarily control if they adopt procedures different from those in Rule 26(b)(5)(B).

A party asserting a claim of privilege or protection after production must give notice to the receiving party. That notice should be in writing unless the circumstances preclude it. Such circumstances could include the assertion of the claim during a deposition. The notice should be as specific as possible in identifying the information and stating the basis for the claim. Because the receiving party must decide whether to challenge the claim and may sequester the information and submit it to the court for a ruling on whether the claimed privilege or protection applies and whether it has been waived, the notice should be sufficiently detailed so as to enable the receiving party and the court to understand the basis for the claim and to determine whether waiver has occurred. Courts will continue to examine whether a claim of privilege or protection was made at a reasonable time when delay is part of the waiver determination under the governing law.

After receiving notice, each party that received the information must promptly return, sequester, or destroy the information and any copies it has. The option of sequestering or destroying the information is included in part because the receiving party may have incorporated the information in protected trial-preparation materials. No receiving party may use or disclose the information pending resolution of the privilege claim. The receiving party may present to the court the questions whether the information is privileged or protected as

trial-preparation material, and whether the privilege or protection has been waived. If it does so, it must provide the court with the grounds for the privilege or protection specified in the producing party's notice, and serve all parties. In presenting the question, the party may use the content of the information only to the extent permitted by the applicable law of privilege, protection for trial-preparation material, and professional responsibility.

If a party disclosed the information to nonparties before receiving notice of a claim of privilege or protection as trial-preparation material, it must take reasonable steps to retrieve the information and to return it, sequester it until the claim is resolved, or destroy it.

Whether the information is returned or not, the producing party must preserve the information pending the court's ruling on whether the claim of privilege or of protection is properly asserted and whether it was waived. As with claims made under Rule 26(b)(5)(A), there may be no ruling if the other parties do not contest the claim.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

. . .

(f) Conference of Parties; Planning for Discovery. Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:

1. What changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement as to when disclosures under Rule 26(a)(1) were made or will be made;
2. The subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused upon particular issues;

3. Any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;
4. Any issues relating to claims of privilege or of protection as trial-preparation material, including—if the parties agree on a procedure to assert such claims after production—whether to ask the court to include their agreement in an order;
5. What changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed;
6. Any other orders that should be entered by the court under Rule 26(c) or under Rule 16(b) and (c).

. . .

Note to Subdivision (f)

Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information during their discovery-planning conference. The rule focuses on "issues relating to disclosure or discovery of electronically stored information," the discussion is not required in cases not involving electronic discovery, and the amendment imposes no additional requirements in those cases. When the parties do anticipate disclosure or discovery of electronically stored information, discussion at the outset may avoid later difficulties or ease their resolution.

When a case involves discovery of electronically stored information, the issues to be addressed during the Rule 26(f) conference depend on the nature and extent of the contemplated discovery and of the parties' information systems. It may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful.

The particular issues regarding electronically stored information that deserve attention during the discovery planning stage depend on the specifics of the given case. *See Manual for Complex Litigation* (4th) § 40.25(2) (listing topics for discussion in a proposed order regarding meet-and-confer sessions). For example, the parties may specify the topics for such discovery and the time period for which discovery will

be sought. They may identify the various sources of such information within a party's control that should be searched for electronically stored information. They may discuss whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information. *See* Rule 26(b)(2)(B). Rule 26(f)(3) explicitly directs the parties to discuss the form or forms in which electronically stored information might be produced. The parties may be able to reach agreement on the forms of production, making discovery more efficient. Rule 34(b) is amended to permit a requesting party to specify the form or forms in which it wants electronically stored information produced. If the requesting party does not specify a form, Rule 34(b) directs the responding party to state the forms it intends to use in the production. Early discussion of the forms of production may facilitate the application of Rule 34(b) by allowing the parties to determine what forms of production will meet both parties' needs. Early identification of disputes over the forms of production may help avoid the expense and delay of searches or productions using inappropriate forms.

Rule 26(f) is also amended to direct the parties to discuss any issues regarding preservation of discoverable information during their conference as they develop a discovery plan. This provision applies to all sorts of discoverable information, but can be particularly important with regard to electronically stored information. The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes.

The parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities. Cf. *Manual for Complex Litigation* (4th) § 11.422 ("A blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations.") The parties should take account of these considerations in their discussions, with the goal of agreeing on reasonable preservation steps.

The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex

parte preservation orders should issue only in exceptional circumstances.

Rule 26(f) is also amended to provide that the parties should discuss any issues relating to assertions of privilege or of protection as trial-preparation materials, including whether the parties can facilitate discovery by agreeing on procedures for asserting claims of privilege or protection after production and whether to ask the court to enter an order that includes any agreement the parties reach. The Committee has repeatedly been advised about the discovery difficulties that can result from efforts to guard against waiver of privilege and work-product protection. Frequently parties find it necessary to spend large amounts of time reviewing materials requested through discovery to avoid waiving privilege. These efforts are necessary because materials subject to a claim of privilege or protection are often difficult to identify. A failure to withhold even one such item may result in an argument that there has been a waiver of privilege as to all other privileged materials on that subject matter. Efforts to avoid the risk of waiver can impose substantial costs on the party producing the material and the time required for the privilege review can substantially delay access for the party seeking discovery.

These problems often become more acute when discovery of electronically stored information is sought. The volume of such data, and the informality that attends use of e-mail and some other types of electronically stored information, may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming. Other aspects of electronically stored information pose particular difficulties for privilege review. For example, production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image. Whether this information should be produced may be among the topics discussed in the Rule 26(f) conference. If it is, it may need to be reviewed to ensure that no privileged information is included, further complicating the task of privilege review.

Parties may attempt to minimize these costs and delays by agreeing to protocols that minimize the risk of waiver. They may agree that the responding party will provide certain requested materials for initial

examination without waiving any privilege or protection—sometimes known as a "quick peek." The requesting party then designates the documents it wishes to have actually produced. This designation is the Rule 34 request. The responding party then responds in the usual course, screening only those documents actually requested for formal production and asserting privilege claims as provided in Rule 26(b)(5)(A). On other occasions, parties enter agreements—sometimes called "clawback agreements"—that production without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances. Other voluntary arrangements may be appropriate depending on the circumstances of each litigation. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.

Although these agreements may not be appropriate for all cases, in certain cases they can facilitate prompt and economical discovery by reducing delay before the discovering party obtains access to documents, and by reducing the cost and burden of review by the producing party. A case management or other order including such agreements may further facilitate the discovery process. Form 35 is amended to include a report to the court about any agreement regarding protections against inadvertent forfeiture or waiver of privilege or protection that the parties have reached, and Rule 16(b) is amended to recognize that the court may include such an agreement in a case management or other order. If the parties agree to entry of such an order, their proposal should be included in the report to the court.

Rule 26(b)(5)(B) is added to establish a parallel procedure to assert privilege or protection as trial-preparation material after production, leaving the question of waiver to later determination by the court.

Rule 33. Interrogatories to Parties

. . .

(d) Option to Produce Business Records. Where the answer to an interrogatory may be derived or ascertained from the business records, including electronically stored information, of the party upon whom the interrogatory has been served or from an examination, audit or inspection of such business records, including a compilation, abstract or summary thereof, and the burden of deriving or ascertaining the answer

is substantially the same for the party serving the interrogatory as for the party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit or inspect such records and to make copies, compilations, abstracts, or summaries. A specification shall be in sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained.

. . .

Notes of Advisory Committee on 2006 Amendments

Rule 33(d) is amended to parallel Rule 34(a) by recognizing the importance of electronically stored information. The term "electronically stored information" has the same broad meaning in Rule 33(d) as in Rule 34(a). Much business information is stored only in electronic form; the Rule 33(d) option should be available with respect to such records as well.

Special difficulties may arise in using electronically stored information, either due to its form or because it is dependent on a particular computer system. Rule 33(d) allows a responding party to substitute access to documents or electronically stored information for an answer only if the burden of deriving the answer will be substantially the same for either party. Rule 33(d) states that a party electing to respond to an interrogatory by providing electronically stored information must ensure that the interrogating party can locate and identify it "as readily as can the party served," and that the responding party must give the interrogating party a "reasonable opportunity to examine, audit, or inspect" the information. Depending on the circumstances, satisfying these provisions with regard to electronically stored information may require the responding party to provide some combination of technical support, information on application software, or other assistance. The key question is whether such support enables the interrogating party to derive or ascertain the answer from the electronically stored information as readily as the responding party. A party that wishes to invoke Rule 33(d) by specifying electronically stored information may be required to provide direct access to its electronic information system, but only if that is necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory. In that situation, the responding party's need to protect sensitive interests

of confidentiality or privacy may mean that it must derive or ascertain and provide the answer itself rather than invoke Rule 33(d).

Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry upon Land for Inspection and Other Purposes

(a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained—translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

(b) Procedure. The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced. Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d).

The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the

remaining parts. If objection is made to the requested form or forms for producing electronically stored information—or if no form was specified in the request—the responding party must state the form or forms it intends to use. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

Unless the parties otherwise agree, or the court otherwise orders,

(i) A party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request;

(ii) If a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained, or in a form or forms that are reasonably usable;

(iii) A party need not produce the same electronically stored information in more than one form.

Notes of Advisory Committee on 2006 Amendments. Note to Subdivision (a)

As originally adopted, Rule 34 focused on discovery of "documents" and "things." In 1970, Rule 34(a) was amended to include discovery of data compilations, anticipating that the use of computerized information would increase. Since then, the growth in electronically stored information and in the variety of systems for creating and storing such information has been dramatic. Lawyers and judges interpreted the term "documents" to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a "document." Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. At the same time, a Rule 34

request for production of "documents" should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and documents.

Discoverable information often exists in both paper and electronic form, and the same or similar information might exist in both. The items listed in Rule 34(a) show different ways in which information may be recorded or stored. Images, for example, might be hard-copy documents or electronically stored information. The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically stored information—information "stored in any medium," to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.

References elsewhere in the rules to "electronically stored information" should be understood to invoke this expansive approach. A companion change is made to Rule 33(d), making it explicit that parties choosing to respond to an interrogatory by permitting access to responsive records may do so by providing access to electronically stored information. More generally, the term used in Rule 34(a)(1) appears in a number of other amendments, such as those to Rules 26(a)(1), 26(b)(2), 26(b)(5)(B), 26(f), 34(b), 37(f), and 45. In each of these rules, electronically stored information has the same broad meaning it has under Rule 34(a)(1). References to "documents" appear in discovery rules that are not amended, including Rules 30(f), 36(a), and 37(c)(2). These references should be interpreted to include electronically stored information as circumstances warrant.

The term "electronically stored information" is broad, but whether material that falls within this term should be produced, and in what form, are separate questions that must be addressed under Rules 26(b), 26(c), and 34(b).

The Rule 34(a) requirement that, if necessary, a party producing electronically stored information translate it into reasonably usable form does not address the issue of translating from one human language to another. *See In re Puerto Rico Elect. Power Auth.,* 687 F.2d 501, 504-150 (1st Cir. 1989).

Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly permits it. As with any other form of discovery, issues of burden and intrusiveness raised by requests to test or sample can be addressed under Rules 26(b)(2) and 26(c). Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Rule 34(a)(1) is further amended to make clear that tangible things must—like documents and land sought to be examined—be designated in the request.

Note to Subdivision (b)

Rule 34(b) provides that a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the discovery request. The production of electronically stored information should be subject to comparable requirements to protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party. Rule 34(b) is amended to ensure similar protection for electronically stored information.

The amendment to Rule 34(b) permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The form of production is more important to the exchange of electronically stored information than of hard-copy materials, although a party might specify hard copy as the requested form. Specification of the desired form or forms may facilitate the orderly, efficient, and cost-effective discovery of electronically stored information. The rule recognizes that different forms of production may be appropriate for different types of electronically stored information. Using current technology, for example, a party might be called upon to produce word processing documents, e-mail messages, electronic spreadsheets, different image or sound files, and material from

databases. Requiring that such diverse types of electronically stored information all be produced in the same form could prove impossible, and even if possible could increase the cost and burdens of producing and using the information. The rule therefore provides that the requesting party may ask for different forms of production for different types of electronically stored information.

The rule does not require that the requesting party choose a form or forms of production. The requesting party may not have a preference. In some cases, the requesting party may not know what form the producing party uses to maintain its electronically stored information, although Rule 26(f)(3) is amended to call for discussion of the form of production in the parties' prediscovery conference.

The responding party also is involved in determining the form of production. In the written response to the production request that Rule 34 requires, the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies. Stating the intended form before the production occurs may permit the parties to identify and seek to resolve disputes before the expense and work of the production occurs. A party that responds to a discovery request by simply producing electronically stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form. Additional time might be required to permit a responding party to assess the appropriate form or forms of production.

If the requesting party is not satisfied with the form stated by the responding party, or if the responding party has objected to the form specified by the requesting party, the parties must meet and confer under Rule 37(a)(2)(B) in an effort to resolve the matter before the requesting party can file a motion to compel. If they cannot agree and the court resolves the dispute, the court is not limited to the forms initially chosen by the requesting party, stated by the responding party, or specified in this rule for situations in which there is no court order or party agreement.

If the form of production is not specified by party agreement or court order, the responding party must produce electronically stored information either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. Rule 34(a) requires that, if necessary, a responding party "translate" information it

produces into a "reasonably usable" form. Under some circumstances, the responding party may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information. The rule does not require a party to produce electronically stored information in the form in which it is ordinarily maintained, as long as it is produced in a reasonably usable form. But the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.

Some electronically stored information may be ordinarily maintained in a form that is not reasonably usable by any party. One example is "legacy" data that can be used only by superseded systems. The questions whether a producing party should be required to convert such information to a more usable form, or should be required to produce it at all, should be addressed under Rule 26(b)(2)(B).

Whether or not the requesting party specified the form of production, Rule 34(b) provides that the same electronically stored information ordinarily need be produced in only one form.

Rule 37. Failure to Make Disclosures or Cooperate in Discovery; Sanctions

. . .

(f) Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

. . .

Notes of Advisory Committee on 2006 Amendments. Note to Subdivision (f)

Subdivision (f) is new. It focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that

attends ordinary use. Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part. Under Rule 37(f), absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.

Rule 37(f) applies only to information lost due to the "routine operation of an electronic information system"—the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs. The "routine operation" of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.

Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good-faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.

The protection provided by Rule 37(f) applies only to sanctions "under these rules." It does not affect other sources of authority to impose sanctions or rules of professional responsibility.

This rule restricts the imposition of "sanctions." It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes or alternatives for some or all of the lost information.

Rule 45. Subpoena

(a) Form; Issuance.

(1) Every subpoena shall

. . .

(C) Command each person to whom it is directed to attend and give testimony or to produce and permit inspection, copying, testing, or sampling of designated books, documents, electronically stored information, or tangible things in the possession, custody or control of that person, or to permit inspection of premises, at a time and place therein specified; and

. . .

A command to produce evidence or to permit inspection, copying, testing, or sampling may be joined with a command to appear at trial or hearing or at deposition, or may be issued separately. A subpoena may specify the form or forms in which electronically stored information is to be produced.

. . .

(c) Protection of Persons Subject to Subpoenas.

. . .

(2) (A) A person commanded to produce and permit inspection, copying, testing, or sampling of designated electronically stored

information, books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(B) Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection, copying, testing, or sampling may, within 14 days after service of the subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to producing any or all of the designated materials or inspection of the premises-or to producing electronically stored information in the form or forms requested.

. . .

(d) Duties in Responding to Subpoena.

. . .

(1) (A) [...]

(B) If a subpoena does not specify the form or forms for producing electronically stored information, a person responding to a subpoena must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable.

(C) The person responding to a subpoena need not produce the same electronically stored information in more than one form.

(D) A person responding to a subpoena need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or to quash, the person from whom discovery is sought must show that the information sought is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for such discovery.

(2) (A) [...]

(B) If information is produced in response to a subpoena that is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not disclose the information until

the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The person who produced the information must preserve the information until the claim is resolved.

. . .

Notes of Advisory Committee on 2006 Amendments

Rule 45 is amended to conform the provisions for subpoenas to changes in other discovery rules, largely related to discovery of electronically stored information. Rule 34 is amended to provide in greater detail for the production of electronically stored information. Rule 45(a)(1)(C) is amended to recognize that electronically stored information, as defined in Rule 34(a), can also be sought by subpoena. Like Rule 34(b), Rule 45(a)(1) is amended to provide that the subpoena can designate a form or forms for production of electronic data. Rule 45(c)(2) is amended, like Rule 34(b), to authorize the person served with a subpoena to object to the requested form or forms. In addition, as under Rule 34(b), Rule 45(d)(1)(B) is amended to provide that if the subpoena does not specify the form or forms for electronically stored information, the person served with the subpoena must produce electronically stored information in a form or forms in which it is usually maintained or in a form or forms that are reasonably usable. Rule 45(d)(1)(C) is added to provide that the person producing electronically stored information should not have to produce the same information in more than one form unless so ordered by the court for good cause.

As with discovery of electronically stored information from parties, complying with a subpoena for such information may impose burdens on the responding person. Rule 45(c) provides protection against undue impositions on nonparties. For example, Rule 45(c)(1) directs that a party serving a subpoena "shall take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena," and Rule 45(c)(2)(B) permits the person served with the subpoena to object to it and directs that an order requiring compliance "shall protect a person who is neither a party nor a party's officer from significant expense resulting from" compliance. Rule 45(d)(1)(D) is added to provide that the responding person need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible, unless the court orders such discovery for good cause, considering the limitations of Rule 26(b)(2)(C), on terms

that protect a nonparty against significant expense. A parallel provision is added to Rule 26(b)(2).

Rule 45(a)(1)(B) is also amended, as is Rule 34(a), to provide that a subpoena is available to permit testing and sampling as well as inspection and copying. As in Rule 34, this change recognizes that on occasion the opportunity to perform testing or sampling may be important, both for documents and for electronically stored information. Because testing or sampling may present particular issues of burden or intrusion for the person served with the subpoena, however, the protective provisions of Rule 45(c) should be enforced with vigilance when such demands are made. Inspection or testing of certain types of electronically stored information or of a person's electronic information system may raise issues of confidentiality or privacy. The addition of sampling and testing to Rule 45(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a person's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Rule 45(d)(2) is amended, as is Rule 26(b)(5), to add a procedure for assertion of privilege or of protection as trial-preparation materials after production. The receiving party may submit the information to the court for resolution of the privilege claim, as under Rule 26(b)(5)(B).

Other minor amendments are made to conform the rule to the changes described above.

Form 35. Report of Parties' Planning Meeting

. . .

3. Discovery Plan. The parties jointly propose to the court the following discovery plan: [Use separate paragraphs or subparagraphs as necessary if parties disagree.]

Discovery will be needed on the following subjects: (brief description of subjects on which discovery will be needed);

Disclosure or discovery of electronically stored information should be handled as follows: (brief description of parties' proposals);

The parties have agreed to an order regarding claims of privilege or protection as trial-preparation material asserted after

production, as follows: (brief description of provisions of proposed order);

All discovery commenced in time to be completed by (date). [Discovery on (issue for early discovery) to be completed by (date).]

Endnote

[1] As proposed for approval by the Committee, the amendments were not in numerical order. We have chosen the latter as more helpful to the practitioner becoming familiar with the new rules.

4

Scope and Form of Production—Rule 34

Introduction

> *In a products liability action the plaintiff class requested certain "raw" clinical test results. Defendant produced a dozen CDs onto which thousands of spreadsheets had been copied. Plaintiff objected that the data was completely indecipherable because it was in no apparent order and could not be organized by any reasonable sorting technique, such as date-ordering (the individual entries being undated), and moved to compel production in a "reasonably useable" form. Defendant defended the production on the grounds that the data had been produced as it was "ordinarily maintained." Who wins?*

Fed. R. Civ. P. 34 addresses an issue that seldom arose in the discovery of paper documents. A party's ESI will be maintained in different forms, and over the life cycle of ESI its form is likely to change. In what form is that ESI to be produced in discovery? Rule 34 "provides a structure and procedure for the parties to identify the form or forms of production that are most useful or appropriate for the litigation; provides guidance to the responding party if no request, order, or agreement specifies the form or forms of production; and provides guidance to the court if there is a dispute" [1].

This chapter explores Fed. R. Civ. P. 34 in detail, and notes issues that may arise in interpreting and applying the amended Rule. We examine preamendment decisions that may guide the courts in interpreting Rule 34 and analyze postamendment decisions. The chapter concludes with suggestions to the requesting party on specifying the form or forms in which ESI is to be produced.

Rule 34 Request

Rule 34 provides, in pertinent part:

> (a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things … or (2) to permit entry upon designated land or property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

The request "shall specify a reasonable time, place, and manner of making the inspection" and "may specify the form or forms in which electronically stored information is to be produced" [2].

The responding party must produce, allow inspection, or state objections [3]. Each of these options, with a focus on ESI, is explored next.

Responses

Production—Default Options

If the request does not specify the form or forms in which ESI is to be produced (or if objection is made to the requested form, as discussed later), the responding party must state the form or forms it intends to use. The default options for the form in which ESI may be produced, in lieu of a specific request, are that the responding party "must" produce the information "in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably useable" [4]. A responding party need not produce the same ESI in more than one form [5].

In general terms, Rule 34(b) is intended "to protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party" [6]. To prevent production of paper documents in a manner that creates "unnecessary obstacles," the Rule requires that such documents be produced "as they are kept in the usual course of business," or the responding party "shall organize and label them to correspond with the categories in the requests" [7]. Though the specific requirements for the production of ESI are

phrased differently than for paper documents, the requirements are intended to be comparable and attain the same objective [8].

In this regard, one issue that arises is whether the phrase "ordinarily maintained" is intended to mean something different from "kept in the usual course of business," an issue the Committee Note does not specifically address. A business would ordinarily backup e-mail and "maintain" that e-mail in some medium: on tape or with an online data storage service, for example. The authors and recipients of that same e-mail keep the correspondence on desktops and laptops for some period of time—in client folders, for example—to refer to or work with. If request is made in discovery for certain employees' e-mail, the responding party could argue that the backup version is how the e-mail is "ordinarily maintained," even though the cost of producing that e-mail might be much higher, and justify a request for cost shifting. The requesting party would presumably prefer the active data, at least if it is likely to be complete.

It seems this issue should be resolved by reference to the Committee Note which explains that "ordinarily maintained" is intended to be the "functional analogue" of "kept in the usual course of business" [9]. That is, a party choosing this option should produce in the form the ESI is ordinarily maintained *for the use of the business*, rather than as it is maintained for backup or storage.

Producing ESI exactly as it is ordinarily maintained does not necessarily comply with the Rule. Instead, Rule 34(a) provides that documents and ESI may have to be "translated, if necessary" into reasonably usable form. Thus, "[u]nder Rule 34(a) and (b), the form or forms in which the responding party ordinarily maintains its information can be the default choice of the responding party, but if necessary that party might have to translate the information to make it 'reasonably usable'" [10].

Under what circumstances must the responding party "translate" ESI from the form in which it is ordinarily maintained, and what type of translation is required? On one extreme, ESI that is not reasonably accessible would presumptively not require translation. As the Committee Note explains:

> Some electronically stored information may be ordinarily maintained in a form that is not reasonably usable by any party. One example is "legacy" data that can be used only by superseded systems. The questions whether a producing party should be required to convert such information to a more usable form, or should be required to produce it at all, should be addressed under Rule 26(b)(2)(B).

On the other end of the spectrum, ESI produced in a form that is searchable by the responding party is presumably reasonably usable [11]. However, a responding party is not required to translate ESI from the form in which it is ordinarily maintained into an electronically searchable form. The Committee

specifically rejected electronically searchable as the alternative to the form in which ESI is ordinarily maintained as one of the default options. Instead, it chose "reasonably usable" to be consistent with Rule 34(a). Therefore, although the production of ESI as it is ordinarily maintained and in searchable form is acceptable, it is not required.

Preamendment decisions interpreting Rule 34(a) suggest factors that might be considered in determining whether translation should be required of the producing party when ESI is ordinarily maintained in some form between inaccessible and readily searchable. One of these factors is the relative burden on the parties of actually performing the translation [12]. Another is the extent to which the data can only be translated accurately by the responding party [13]. If translation is required in order to determine whether the data is actually responsive, it may be considered necessary as otherwise the production is merely a "data dump" [14]. The fact that the ESI is being produced in the form in which it is ordinarily maintained ought to weigh against requiring translation of that ESI [15], else the distinction between the two default options is meaningless. An interesting scenario will undoubtedly arise when a party produces ESI in the manner in which it is "ordinarily maintained" and that production is completely disorganized. Under the cases construing the old Rule 34, one did not satisfy one's production obligation by producing a haystack and inviting the requesting party to find the needle [16]. Or, the better argument would be that ESI that is completely disorganized is not reasonably usable and must be translated by means of some form of organization or indexing, even if it is ordinarily maintained in that disorganized fashion [17]. Finally, whether and to what extent a producing party will be required to translate ESI into reasonably usable form will be assessed by the proportionality test set forth in Fed. R. Civ. P. 26(b)(2)(C) [18].

As for the second option—to produce ESI in a reasonably usable form—the Committee Note explains the following: "the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly downgrades this feature" [19].

Finally, what does "reasonably usable" mean? The responding party "may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information" [20]. The responding party may be required to allow the requesting party access to proprietary hardware or software, though a protective order may be necessary to protect that interest [21].

Inspect, Test, and Sample

Before Rule 34 was amended, a party could seek permission to inspect documents (Rule 34(a)(1)) and inspect, test, or sample property or any designated object or operation thereon (Rule 34(a)(2)). The rule was generally interpreted as allowing for the inspection or testing of any "relevant matter" and not considered an extraordinary means of discovery [22], so long as the normal operations of the responding party would not be unduly interrupted by the inspection [23]. To protect confidential or proprietary information from unwarranted exposure, the court imposed restrictions or limitations on the scope of the inspection [24], or entered a protective order prohibiting unauthorized use or disclosure of any information obtained in the inspection [25].

Typically a party seeks to inspect a computer or computer system in order to obtain a mirror image of the computer's hard drive. The federal courts generally assumed that the provisions of preamended Rule 34 concerning inspection, copying, and testing of tangible objects authorized a court to order inspection of a computer and copying of ESI stored on the computer's hard drive [26], and the amendments to the Rule make that authority explicit. It is not so clear what showing is required of the requesting party to justify such an order.

The requesting party obtained permission to inspect and copy computer hard drives in *Balboa Threadworks, Inc. v. Stucky* [27] simply by showing that the computers contained relevant information. *Balboa* was a copyright/Lanham Act claim involving allegedly copied embroidery designs. Copying the hard drives was directly relevant to the claims that defendants downloaded the copyrighted embroidery patterns. The *Balboa* court explicitly linked its acceptance of the mirror-imaging request (defined as a "bit for bit, sector for sector" forensic duplicate) with the explicit nature of the copyright claim. Because it was "reasonable to conclude that some relevant evidence … may be found on any of the Defendants' computers" [28], the order to allow inspection was granted [29].

No such showing of the existence of relevant information was required in *Visa Int'l Serv. Assoc. v. JSL Corp.* [30]. In this case, Visa sought an order compelling the inspection of a personal notebook hard drive [31]. The defendant objected that an inspection would be "harassment" and that the backup files of the hard drive had been searched. The court noted that there was "no evidence" that data existed that had not been produced from the backup files. However, the court concluded, so long as Visa paid for the inspection, it would grant the motion [32].

More commonly, the courts rely on some indication that relevant information is being deleted, or is at risk for being deleted, before ordering that a requesting party's computers be made available for inspection and copying. But the decisions vary in defining what degree of risk must be shown.

Evidence that, in general, ESI is at risk for deletion satisfied the court in *Antioch Co. v. Scrapbook Borders, Inc.* [33]. *Antioch* was also a copyright/unfair competition claim involving scrapbook designs and accessories. When a former employee started a competing entity and sold similar designs, the former employer sued. It then sought an order compelling the defendants to produce computer equipment for inspection, copying, and imaging. In support of its motion, plaintiff produced an affidavit from a computer forensics expert explaining that data retained on a computer hard drive is constantly being overwritten by new data through the normal use of the computer equipment [34]. The court noted that it was "well accepted" that deleted data was discoverable, and concluding from the affidavit "that the Defendants may have relevant information, on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the Plaintiff's claims," the court granted the motion to compel [35].

In *Simon Property Group, L.P. v. MySimon, Inc.* [36], a trademark infringement claim, the plaintiff requested inspection of the defendant's computers and computer servers. The defendant objected and plaintiff moved to compel. The court considered the motion in light of the central principle that deleted computer records are discoverable under Fed. R. Civ. P. 34 [37]. Without specifically holding that such a showing was required, the court granted the motion because the plaintiff had shown "troubling discrepancies" in the defendant's document production [38].

In *Powers v. Thomas M. Cooley Law Sch.* [39], defendant sought an order compelling the plaintiff to make a computer available for mirror imaging, and in denying the motion the court set a high standard for review of a motion to compel inspection and copying of a computer hard drive [40]:

> The discovery process is designed to be extrajudicial, and relies upon the responding party to search his records to produce the requested data. In the absence of a strong showing that the responding party has somehow defaulted in this obligation, the court should not resort to extreme, expensive, or extraordinary means to guarantee compliance.

Finding that the defendant had failed to show any "discovery misconduct" by the plaintiff, and failed to identify any category of relevant discovery material that might be uncovered in the imaging, the court held that it was "unwilling to expand the expense and burden of this case by ordering examination of the computers maintained by either party."

In support of the standard articulated for reviewing a motion to compel inspection, the court in *Powers* quoted the Committee Note to amended Rule 34(a) [41], which provides in pertinent part:

> Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

The court interpreted the Note as "suggesting that direct inspection of an opponent's computer should be the exception and not the rule."

But the Note also provides:

> Rule 34(a)(1) is … amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly permits it.

And at least one commentator has suggested that this language "reinforces the intent to allow direct access to inspect computers" [42]. It could also be argued that the provisions of Rule 34(b), allowing the requesting party to specify the form in which ESI is to be produced, weigh on the side of allowing inspection of the responding party's computer. That is, if a party requests ESI in native form—and no objection is made or the court grants a motion to compel production in the form specified—mirror imaging is one means of obtaining the ESI in native form.

Ameriwood Industries, Inc. v. Liberman [43] is a postamendment decision on a request to obtain mirror imaging in discovery. In this case, plaintiff brought breach of fiduciary duty and other causes of action against former employees and their recently formed company, alleging that the defendants had improperly used plaintiff's computers and misappropriated confidential information. In document requests, plaintiff requested the hard drives of defendants' computers or mirror images. Defendants objected and plaintiff moved to compel.

In opposition to the motion defendants argued that responsive information had already been produced, so that mirror imaging was not necessary and, in the alternative, that the data requested in the mirror image was not reasonably accessible. Based on the evidence submitted by defendants as to the significant cost of copying the hard drives, recovering deleted information, and translating the recovered data into reviewable format, the court agreed that the requested information was "not reasonably accessible" within the meaning of Fed. R. Civ.

P. 26(b)(2)(B) [44]. But the court also found that plaintiff had shown "good cause" for discovery, primarily because of the evidence of a "discrepancy" in defendants' prior production (plaintiff submitted an e-mail sent by one of the defendants to one of plaintiff's customers that had not been produced by defendants) and the fact that the alleged wrong had been committed by using the computers at issue [45]. Therefore, the court granted the motion [46], imposing a three-step imaging, recovery, and disclosure procedure to protect against the disclosure of confidential information and irrelevant information and prevent undue burden on the responding party [47].

Another way to inspect ESI would be through a limited remote access to the computing environment of the other party. Although this approach intuitively may appear too intrusive, it affords both parties a significant level of control while leveraging the efficiencies of modern computing and networking. Using a virtual private network (VPN), commonly used to connect remote workers to their corporate computing infrastructure, a party could be given a limited access to specific data on the responding party's computing infrastructure. In addition to limiting access only to specific applications, folders, subfolders, or files, the responding party would be able to keep track of the requesting party's access and even generate an audit trail. Depending on the case and the parties' situation, this may be an appropriate approach for inspection of specific ESI, for data sampling, or for transmittal of requested data production.

Object to Specified Form or Production

The response to a Rule 34(a) request for production of ESI may be an objection to the requested form or forms of production [48]. If objection is made, and the requesting party files a motion to compel production in the form specified, under what circumstances should that motion be granted? Certain parameters are clear. A party would not be compelled to produce ESI stored in an inaccessible source in a "reasonably usable" form unless good cause is shown [49]. One could argue that a request for one of the default forms should be granted: implicit in the fact that the rule allows for production in one of the default forms absent specification of form by the requesting party is the notion that either of these may be "useful or appropriate" for the litigation [50]. On the other hand, the facts may show that producing ESI as it is ordinarily maintained, for example, is unduly burdensome because of difficulties in marking for identification and authentication, conducting privilege review, and so forth [51]. In other words, the general limitations of Rule 26(b)(2)(C) continue to be relevant considerations in this regard.

Requesting a Form or Forms

For many reasons native form is the optimal choice: production can be quick and efficient because data in native form can be downloaded directly from the medium in which it is stored [52]; marking for identification and authentication can be accomplished in one step, avoiding duplication and possible "chain of custody" issues; and data in native form is usually fully searchable. Native form is also desirable if any functionality that is intrinsic to the application that produced that data is going to be used in evaluation of such ESI. For example, if understanding formulas in an Excel spreadsheet is relevant such spreadsheets should be sought in native form. Or, if understanding how the party uses certain application is relevant, the native data might be needed. For example, in Microsoft Outlook, the user can control the view of e-mail messages including grouping messages by conversation or hiding read messages. Understanding such different views and therefore understanding the party's way of using such application may only be possible by examining native data through the application that created such data.

Mirror imaging is one means of capturing data in native form. If, however, only certain types of ESI or ESI from one specific application is required, requesting only a copy of that data—in its native form—may be more appropriate than requesting a mirror image of the disk. The mirror image of the disk will include much more than the relevant ESI, and will be costlier to produce and review, costs which may be borne by the requesting party. However, in order to capture deleted or inactive data, the so-called residual data that is still stored on the drive even though not accessible to the user or to the file system, the mirror image of the entire disc must be sought.

Unless the requesting party has the proper hardware and software to store and access ESI in native form, and appropriate procedures in place to avoid authentication or chain of custody concerns, another form must be chosen [53]. PDF and TIFF files have some advantages over paper: less storage space is required, and the documents can be transmitted electronically. PDF in text format is preferable to TIFF because it is searchable; TIFF is not. Nontext PDF and TIFF files can be annotated or indexed to facilitate review and retrieval, and as between PDF and TIFF files, the former are generally easier to annotate and index. The choice of form is, ultimately, a function of office resources and the scope of the anticipated production.

Endnotes

[1] Advisory Committee Introduction to *Interrogatories and Requests for Production Involving Electronically Stored Information: Rules 33 and 34,* http://www.uscourts.gov/rules/Reports/ST09-2005.pdf., p. 64.

[2] Fed R. Civ. P. 34(b).

[3] Moore, J. W., et al., *Federal Practice,* § 34.13[2][a](3rd ed. 1999).

[4] Fed R. Civ. P. 34(b)(ii).

[5] Fed R. Civ. P. 34(b)(iii).

[6] Advisory Committee Note, Rule 34, Subdivision (b), at Chapter 3, p. 43.

[7] Fed R. Civ. P. 34(b)(i).

[8] *See* n. 6, *supra*.

[9] Advisory Committee Introduction, n. 1, *supra*, p. 64.

[10] *Id.*

[11] *See* Zakre v. Norddeutsche Landesbank Girozentrale, 2004 U.S. Dist. LEXIS 6026 (S.D. N.Y. 2004) (e-mail produced on compact discs was close to the form in which it was ordinarily maintained and, in any event, was text-searchable). It should be noted, however, that ESI readily searchable by the responding party's system may not be readily searchable, or searchable at all, on the requesting party's system.

[12] *See* Powerhouse Marks, LLC v. Chi Hsin Impex., Inc., 2006 U.S. Dist. LEXIS 2767 at *9 (E.D. Mich. 2006); Chemtex, LLC v. St. Anthony Enterprises, Inc., 2004 U.S. Dist. LEXIS 6031 at *2 (S.D.N.Y. 2004).

[13] *See* Powerhouse Marks, LLC v. Chi Shin Impex, Inc*., supra*.

[14] Advisory Committee Introduction, n. 1, *supra*, p. 65.

[15] The mere assertion by a party that ESI is ordinarily maintained in a particular form may not be sufficient if the form of production is objected to by the requesting party. *See* Bergersen Co. v. Shelter Mut. Ins. Co., 2006 U.S. Dist. LEXIS 17452 (D.Kan. 2006).

[16] *See* Standard Dyeing & Finishing Co. v. Arma Textile Printers Corp., 1987 U.S. Dist. LEXIS 868, at *2 (S.D.N.Y. 1987), citing 8 C. Wright, A. Miller, A. Miller & F. Elliot, Federal Practice and Procedure P 2213 (Supp. 1986).

[17] If this argument prevails in the courts, the plaintiff in our opening hypothetical has the winning argument.

[18] Of course, if the requesting party is willing to pay the cost of translating data into a form reasonably usable, that fact weighs in favor of requiring production in that form. *See* National Union Elec. Co. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980).

[19] Advisory Committee Note, Rule 34, Subsection (b), at Chapter 3, p. 43.

[20] *Id.*

[21] David K. Isom, Article: *Electronic Discovery Primer for Judges*, 2005 FED. CTS. L. REV. 1 (2005).

[22] *See* Cuno, Inc. v. Pall Corp., 116 F.R.D. 279, 281 (E.D.N.Y. 1987) (granting motion to compel inspection of defendant's entire manufacturing facility in patent infringement action); National Dairy Products Corp. v. L.D. Schreiber & Co., 61 F.R.D. 581 (E.D. Wis. 1973) (permitting inspection and testing of operations allegedly infringing patent).

[23] *See* N.O. v. Callahan, 110 F.R.D. 637, 640 (D. Mass. 1986).

[24] *See* Petz v. Ethan Allen, Inc., 113 F.R.D. 494 (D.Conn. 1985) (limiting inspection of personnel files in an employment discrimination case to parties and their attorneys).

[25] *See* Cuno, Inc. v. Pall Corp., *supra;* National Dairy Products Corp. v. L.D. Schreiber & Co., *supra.*

[26] *See, e.g.,* Simon Property Group, L.P. v. MySimon, Inc., 194 F.R.D. 639, 640–41 (S.D. Ind. 2000).

[27] 2006 U.S. Dist. LEXIS 29265 (D. Kan. 2006).

[28] *Id.* at *12.

[29] The court imposed protocols for the inspection to prevent the disclosure of irrelevant and privileged information, discussed *infra.*

[30] 2006 U.S. Dist. LEXIS 77451 (D. Nev. 2006).

[31] It is not clear from the opinion, but the notebook was apparently used by an employee or agent of the defendant.

[32] 2006 U.S. Dist. LEXIS 77451, at *12. The court also imposed conditions on the inspection to protect against the disclosure of privileged information, discussed *infra.*

[33] 210 F.R.D. 645 (D. Minn. 2002).

[34] *Id.* at 651.

[35] *Id.* at 651–52.

[36] 194 F.R.D. 639 (D. Ind. 2000).

[37] *Id.* at 640. The court also considered its power to prevent undue burden or expense and limit discovery as set forth in Fed. R. Civ. P. 26(b)(2)(iii) and 26(c) and imposed the protocols on the inspection. In regard to these protocols, *see* n. 46, *infra.*

[38] *Id.* at 641.

[39] 2006 U.S. Dist. LEXIS 67706 (W. D. Mich. 2006).

[40] *Id.* at *10.

[41] The court also relied on In re Ford Motor Co., 345 F.3d 1315 (11th Cir. 2003), in which the Eleventh Circuit granted mandamus to prevent implementation of a district court order allowing plaintiffs to inspect certain databases on Ford's computers. The circuit court found several reasons to disapprove of the district court's order, including the fact that the district court had made no findings that Ford had failed to comply properly with

discovery requests, and also that the district court had imposed no restrictions on the inspection to prevent the disclosure of irrelevant or privileged information.

[42] David K. Isom, Article: *Electronic Discovery Primer for Judges*, 2005 FED. CTS. L. REV. 1 (2005).

[43] 2006 U.S. Dist. LEXIS 93380 (E.D. Mo. 2006).

[44] *Id.* at *11, 12.

[45] *Id.* at *13, 14.

[46] The court noted: "In performing the good cause inquiry, the court is also permitted to set conditions on discovery, including but not limited to payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. *See* Fed. R. Civ. P. 26(b)(2)." *Id.* at *15. Plaintiff did not object to paying, and was ordered to pay the costs of the mirror-imaging process. In regard to this cost-shifting issue, see Chapter 6.

[47] When a court orders that computers be made available for mirror imaging, the order is ordinarily accompanied by restrictions or protocols on that inspection for these purposes. The protocols imposed by the court in Simon Property Group, LP v. MySimon, Inc., *supra*, are commonly used as a model. *See, e.g.,* Ameriwood at *16.

[48] Fed. R. Civ. P. 34(b).

[49] *See* Fed. R. Civ. P. 26(b)(2)(B).

[50] *See* Advisory Committee introduction, n. 1, *supra*, p. 64, setting this forth as one of the general objectives of the amendments to the Rule.

[51] *But see* Hagenbuch v. 3B6 Sistemi Elettronici Industriali, S.R.L., 2006 U.S. Dist. LEXIS 10838 (N.D.Ill. 2006). In this case, the plaintiff requested information in electronic format, but the defendant converted the requested information to TIFF for production. The court agreed with the plaintiff that the production in TIFF format was not sufficient because potentially relevant ESI, including metadata, was not captured in the TIFF format. The court rejected defendant's argument that the benefits of being able to use Bates numbers on the TIFF documents justified its failure to produce the designated electronic medium because alternative means of marking and identifying could be devised by the parties.

[52] Of course, the parties would have to reach an agreement regarding nonwaiver of privilege prior to a direct transfer of data.

[53] With the advent of commodity on-demand computing, such as Amazon's Simple Storage Service (S3) and Elastic Compute Cloud (EC2) services, requesting ESI in native form should be increasingly feasible.

5

Accessible Versus Inaccessible Data

Introduction

Experienced litigators are virtually unanimous that a controversial aspect of the 2006 amendments will be the distinction drawn in Rule 26(b)(2)(B) between accessible and inaccessible data [1]. Under the new rule, a party from whom discovery is sought need not review or produce electronically stored information that is "not reasonably accessible," even if it is otherwise discoverable. Pursuant to the new rule, the responding party may unilaterally designate certain ESI as "inaccessible," thereby preventing—or at the very least delaying—its production. Critics understandably argue such unilateral authority constitutes an invitation for mischief.

There is little doubt that it will take the federal courts some time to develop a body of case law that defines which electronic materials are reasonably accessible and which are not. In the meantime, prudent practitioners must comprehend and master the burden of discovering inaccessible materials.

Two-Tier Analysis

The new Rule 26(b)(2)(B) establishes a two-tier procedure for evaluating access to inaccessible materials. Under the new rule, even if the responding party knows or has reason to believe that it has relevant information, it need not locate, review, or produce that information if it is not reasonably accessible. Instead, the responding party must only "identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing" (tier one) unless "good cause" is shown (tier two) [2].

Under the first tier, after a designation of inaccessibility, the requesting party bears the burden of challenging the producing party's claim that the information is not reasonably accessible. The requesting party can even request discovery on the accessibility issue. The court might then "require the responding party to conduct a sampling of information contained in the sources identified as not reasonably accessible; allow some form of inspection of such sources, or tak[e] depositions of witnesses knowledgeable about the responding party's information systems" [3]. Once that challenge has passed the *prima facie* threshold, the burden then shifts to the responding party to demonstrate that the information is not reasonably accessible [4].

Under the second tier, if the court agrees that the requested information is not reasonably accessible, the requesting party must show good cause for discovery. "Good cause" refers to the proportionality test of the existing rule [5], but is apparently not identical. The Advisory Committee Note lists seven factors for the courts to consider in determining whether good cause has been demonstrated [6]:

1. The specificity of the discovery request;
2. The quantity of information available from other and more easily accessed sources;
3. The failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
4. The likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
5. The predictions as to the importance and usefulness of the further information;
6. The importance of the issues at stake in the litigation;
7. The parties' resources.

The Advisory Committee also advises that the requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause [7]. Whether or not the requesting party volunteers to pay part of the costs for access, the court maintains its authority pursuant to Rule 26(b)(2)(C) to impose conditions on discovery, including "payment by the requesting party of part or all of the 'reasonable costs' of obtaining the information" [8].

The court's finding on accessibility has significant practical consequences for the parties. Despite this significance, new Rule 26(b)(2) does not define "reasonably accessible." ESI only becomes "inaccessible" "because of undue burden or cost" associated with producing it. Again, the Advisory Committee lists

examples of data that would be substantially burdensome or costly for the producing party to retrieve [9]:

> … backup tapes intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on successor systems; data that was deleted but remains in fragmented form, requiring a modern version of forensics to restore and retrieve; and databases that were designed to create certain information in certain ways and that cannot readily create very different kinds or forms of information.

These examples may be helpful, but they certainly will rarely be case determinative. They are also likely to lose relevance quickly given rapid technological change in the field of data formatting and storage.

Winning the Accessibility Fight

The first observation the experienced litigator will make in evaluating an accessibility/inaccessibility motion is that "undue burden or cost" in the words of Rule 26(b)(2)(B), does not simply mean burdensome or costly, it must be something more—some *undue* burden or cost. Put differently, there must be some distinction between the "undue burden and cost" of the new Rule 26(b)(2)(B) and the "unduly burdensome" standard of the old proportionality test under Rule 26(b)(2)(C) or there would have been no purpose in adopting the new ESI test. One would reason that since inaccessible data need not even be searched for responsive documents, the (b)(2)(B) undue burden or cost test must be a more rigorous showing than that required under the old proportionality standard.

This distinction manifests itself in very practical ways. For example, those cases that hold cost shifting (see Chapter 6, "Shifting the Costs of Discovery") inappropriate for certain types of ESI would seem to support the notion that all such ESI is readily accessible [10]. In contrast, that body of case law supporting cost shifting for certain types of ESI is not necessarily relevant to the tier-one undue burden or expense enquiry. The finding, for example, that a plaintiff should share costs under the proportionality test of (b)(2)(C) is not equivalent to the tier-one enquiry that production is unnecessary because of undue burden or expense. Sorting out the distinctions between these enquiries—and the results such enquiries produce—will take years of litigation.

Zubulake v. UBS Warburg LLC, (Zubulake I) [11], in which Judge Sheindlin established a two-tier cost-shifting test analogous to the two-tier test in Rule 26(b)(2)(B), is instructive. *Zubulake I* divides data into accessible and inaccessible formats. Judge Sheindlin reasoned "information deemed 'accessible'

is stored in a readily usable format. Although the time it takes to actually access the data ranges from milliseconds to days, the data does not need to be restored or otherwise manipulated to be usable. Inaccessible data, on the other hand, is not readily usable" [12]. If data is accessible, "it would be wholly inappropriate to even consider cost-shifting" [13]. For inaccessible data, a seven-factor "proportionality" test determines whether and to what extent the costs of production should be shifted to the requesting party [14].

Using the *Zubulake I* formulation, the issue of accessibility/inaccessibility appears to turn on the media in which the ESI is stored [15]. The court specified five categories of data. Three were considered accessible: active online data; near-line data (data on removable storage media that can readily be inserted into read/write devices such as optical discs, CDs, and DVDs), and offline storage archives. Two categories were considered inaccessible because the data was not readily usable as stored: backup tapes and erased, fragmented, or damaged data. The court ordered the defendant to produce all responsive e-mail in accessible format; in a subsequent decision the judge ordered plaintiff to bear a part of the costs of retrieving and processing responsive e-mails in inaccessible format [16]. *Zubulake I* can be cited for the proposition that active, online data, near-line data, and offline storage archives constitute accessible data within the meaning of new Rule 26(b)(2)(B).

Certain types of backup files, data that requires restoration, legacy data, and databases may constitute more problematic categories of data. Data in these categories must be carefully assessed to determine whether it is not reasonably accessible [17].

Backup Files. Both the Advisory Committee and Judge Sheindlin identified backup tapes as inaccessible data. But such a categorical classification is probably overstated. First, the committee limited its view of backups to those "intended for disaster recovery purposes that are not indexed, organized, or susceptible to electronic searching" [18]. But indexing is a matter of degree. If backup tapes were completely unorganized they would be virtually useless to the owner and not worth maintaining even for emergencies. Targeted discovery should request the means or methods by which the responding party organized the backup to make it useful. Most backup software also automatically creates a simple table of contents or index. Even if the data is inaccessible, such an index would not be, and it may yield information that would justify pursuing the tapes themselves.

Since *Zubulake I,* technological advances have eliminated some of the difficulties of accessing information stored as backup. As described by Judge Scheindlin [19]:

> The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks. As a result, [t]he data on a backup tape are not

> organized for retrieval of individual documents or files [because] … the organization of the data mirrors the computer's structure.

Increasingly, businesses are utilizing backup and recovery services delivered over the Internet, or opting for disc-based backup, rather than tape drives. Both of these overcome the sequential-access issue identified in *Zubulake I*—and litigants should be chary of accepting categorical classifications of all backups as inaccessible.

Restored Data. Judge Sheindlin also concluded that ESI on backup tapes was inaccessible in part because it had been compressed for storage and must be "restored" to be readable [20]. Similarly, the Advisory Committee introduction notes that a responding party might have difficulty reviewing or producing data that requires restoration or translation.

Restoration is not, however, necessarily burdensome or costly. The WinZip utility compresses and organizes multiple compressed files into a single zip file. The individual files are restored with one click. This is not to suggest that it is worth arguing that the data stored on conventional magnetic backup tapes is readily usable or accessible. The objection that data must be restored, however, should not simply be taken at face value. Thus, the restoration argument in support of inaccessibility needs to be parsed and assessed in each particular case rather than submitted to as categorically correct. As just one example, decompressing ESI typically only requires someone to babysit the computer to restart a failed or aborted decompression program. Such decompression should hardly be categorized as being unduly burdensome.

Legacy Data. The Advisory Committee advises that legacy data—data created by or stored in system architecture the company no longer uses—is not reasonably accessible if it is "unintelligible" on the company's existing system. Data that is saved for legal purposes, for example, may only be accessible through the purchase of new software. But because data that is truly irretrievable is useless to the business, certain legacy data must be accessible by some means. For example, the business may have a limited license agreement for the application that created the legacy data, even if the business no longer uses that application to capture new data. If so, that data could still be considered reasonably accessible.

Databases. Even before the 2006 amendments, many litigants argued that producing databases was burdensome because they must be decoded or disassembled before the requesting party could use them. According to the Advisory Committee, databases that "cannot readily create very different kinds or forms of information" from the kind or form for which they were designed are a problem in discovery [21]. Again, that assumption may apply in most circumstances, but it is not one that the savvy litigant should indulge. For example, if the responding party claims that the particular form of information sought from a database is not the form for which the database was designed, the requesting

party should determine under what circumstances the company had previously utilized the form sought. If there is evidence of historical use, the ESI may be considered reasonably accessible. Alternatively, the requesting party may reexamine its request to determine if it can reformulate its discovery request or otherwise make use of the data in the form in which it is stored.

Endnotes

[1] This chapter is reprinted, in part, from Marian K. Riedy and Suman Beros, *Win the Accessible Battle for E-Data*, with permission of TRIAL (December 2006), Copyright American Association for Justice 2006.

[2] Advisory Committee Note, Rule 26(b)(2), Chapter 3, p. 32. How exactly a party is to identify such sources is another issue. That is, would "in backup tapes" be sufficient, or must the identification be more precise to fit the requirements of the Rule?

[3] *Id.*, Chapter 3, p. 34.

[4] *Id.*

[5] Advisory Committee Introduction to *Discovery into Electronically Stored Information that Is Not Reasonably Accessible:* Rule 26(b)(2), http://www.uscourts.gov/rules/Reports/ST09-2005.pdf, p. 41.

[6] Advisory Committee Note, Chapter 3, p. 34. The seven-part list in the advisory committee note is similar, though not identical, to the seven-part test for cost-shifting set forth in Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322-23 (S.D.N.Y. 2003) (Zubulake I). Regarding the relationship between the good cause test and the cost-shifting tests used by the courts preamendment, *see* Chapter 6.

[7] Advisory Committee Note, Chapter 3, p. 35.

[8] *Id.*

[9] Advisory Committee Introduction, n. 5, *supra*, p. 40.

[10] *See* Eggleston v. Wal-Mart Stores, E., LP, 2006 U.S. Dist. LEXIS 12849 (E.D. Va. 2006); In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437 (D. N.J. 2002).

[11] 217 F.R.D. 309 (S.D. N.Y. 2003).

[12] *Id.* at 320.

[13] *Id.*

[14] *Id.* at 322–23. Other influential cost-shifting tests do not incorporate this two-step approach. *See* Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D. N.Y. 2002); McPeek v. Ashcroft, 202 F.R.D. 31 (D. D.C. 2001).

[15] *Zubulake I* at 318.

[16] Cost-shifting was ordered in Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D. N.Y. 2003) (Zubulake III).

[17] The good-cause analysis is examined more fully in Chapter 6.

[18] Advisory Committee Introduction, n. 5, *supra*, p. 40.

[19] 217 F.R.D. at 318 (quoting, respectively, Internetnews.com, *Tape Drive* (rev. June 21, 2002), http://inews.webopedia.com/TERM/t/tape_drive.html (last accessed Sept. 25, 2006); Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, 2000 FED. CTS. L. REV. 2, 5, http://www.fclr.org/2000fedctslrev2.htm (last accessed Sept. 25, 2006).

[20] *Id.* at 319–20.

[21] Advisory Committee Introduction, n. 5, *supra*, p. 40.

6

Shifting the Costs of Discovery

Introduction

> *In an employment discrimination case, the plaintiff requested performance evaluations of identified coworkers for a specified period of time. In response, defendant stated that the information requested was maintained as ESI. It further objected to production on the grounds that the ESI was not reasonably accessible because defendant no longer had license to the application with which the evaluations had been created. Plaintiff moved to compel. In the hearing on the motion, the court found that plaintiff had met the "good cause" showing of Fed. R. Civ. P. 26(b)(2)(B). Defendant then argued that plaintiff should bear the cost of production. Plaintiff contended that having shown good cause, cost shifting would not be appropriate. Who wins?*

Under the federal discovery rules, the presumption is that the responding party must bear the expense of complying with discovery requests [1]. However, as a practical matter, what a party may discover may depend upon its willingness to pay all or part of the costs of discovery. "[D]iscovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter" [2]. In the previous chapter we explored the general limitations on the scope of discovery of ESI set forth in Fed. R. Civ. P. 26(b)(2)(B). In this chapter, we focus on the imposition of costs on the requesting party as a condition to discovery of ESI.

Shifting the costs of production is of course not unique to the discovery of ESI. Preamendment Fed. R. Civ. P. 26(b) and 26(c) authorized the courts to protect a party from "undue burden or expense" by conditioning discovery on the requesting party's payment of the costs of discovery [3]. But the issue has

assumed even greater prominence in discovering ESI, and received enhanced and focused attention by the courts.

Prior to the 2006 amendments, the courts expanded upon the proportionality test of what is now Rule 26(b)(2)(C), and developed various tests specific to the discovery of ESI for determining when and under what conditions cost shifting would be appropriate. The already complex cost-shifting analysis has been further complicated by the amendments, particularly by the distinct treatment accorded ESI not reasonably accessible.

This chapter sets forth the principal cost-shifting tests developed by the courts prior to the rule amendments and discusses how the preamendment tests fit within the amended rules. We next analyze postamendment cost-shifting decisions, and conclude with a note on technology developments that may affect the cost-shifting issue.

Cost Shifting Tests Preamendment

Even before the 2006 amendments, the courts "devised creative solutions for balancing the broad scope of discovery prescribed in Rule 26(b)(1) with the cost-consciousness of Rule 26(b)(2)" [4] when ESI was sought in discovery. Representatives of these creative solutions are described next.

Seminal Cases

Three particularly influential tests developed preamendment were the marginal utility test devised by Magistrate Judge Facciola in *McPeek v. Ashcroft* [5], the eight-part test adopted by Magistrate Judge James Francis in *Rowe Entm't, Inc. v. William Morris Agency, Inc.* [6], and Judge Shira Scheindlin's seven-part test set forth in *Zubulake v. UBS Warburg LLC (Zubulake I)* [7].

In *McPeek v. Ashcroft*, a sexual-harassment claim, the plaintiff sought information contained in backup tapes maintained by the defendant, which objected that the likelihood of obtaining relevant information from the tapes did not justify the costs. The court rejected the notion that a responding party should always have to pay for and produce data from backup tapes because that would create a disincentive for the requesting party to demand anything less than all the tapes. The opposite extreme—requiring the requesting party to pay the costs of all tapes restored—would not be fair if there would likely be relevant information on the backup tapes. The optimal result would be to allocate costs based on the benefit of production (discovery of relevant information) relative to the cost of realizing that benefit. "The more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the government agency search at

its own expense. The less likely it is, the more unjust it would be to make the agency search at its own expense. The difference is 'at the margin'" [8].

Applying this test to the dispute before it, the court "decided to take small steps and perform, as it were, a test run." Specifically, the court ordered the defendant to perform a backup restoration of e-mail from a time period that was especially likely to yield evidence of alleged retaliation against the plaintiff. The court did not, at this stage, order restoration of data other than e-mail. The court directed the defendant to document the time and money expended in this test run search and to file a sworn certification summarizing that information. At that point, the parties were to present their respective cases as to whether "the results and the expense do or do not justify any further search" [9].

In *Rowe Entm't, Inc. v. William Morris Agency*, a discrimination and unfair competition claim by black concert promoters, the plaintiffs sought to discover e-mail, most of which was stored on backup tapes. Defendant sought a protective order on the grounds that the production would be unduly burdensome because of the cost of restoring the tapes. The court found that the plaintiffs had successfully demonstrated that the discovery sought was relevant, so that a blanket order precluding discovery would not be justified. The question was whether production would constitute an undue burden or expense such that shifting all or part of the costs of production would be appropriate.

To assess whether the burden was undue, the court adopted a balancing test based on the following eight factors: (1) the specificity of the requests; (2) the likelihood of a successful search; (3) availability from other sources; (4) purposes of retention [10]; (5) benefit to the parties [11]; (6) total costs of production; (7) ability to control costs; and (8) the parties' resources [12].

In the case before it, the *Rowe* court determined that six of the eight factors favored the shifting of costs to the plaintiffs, one of the factors favored leaving those costs with the defendant, and one factor was neutral. Accordingly, the court readily determined that the costs of obtaining discovery of e-mail in the case should shift to the plaintiffs. Like all complex, multipart legal tests, the application of the *Rowe* standard to any particular case will depend heavily on the facts and whether the court chooses to weigh some factors more than others.

In *Zubulake I* [13], an employment-discrimination case, plaintiff sought all documents concerning any communication about her by or between UBS employees, including e-mail. The court held that Zubulake was entitled to discovery of the requested e-mails so long as they were relevant, "which they clearly are." Defendant argued that the production of the e-mail would subject it to undue burden and expense and requested that the costs of production be shifted to the plaintiff [14].

The court held that cost-shifting "would be wholly inappropriate" if the data at issue were "accessible" because the production of accessible data is, by definition, not unduly burdensome [15]. In the court's view, whether data is

accessible or inaccessible turns largely on the media in which it is stored. Examples of accessible data include active, online data; near-line data; and offline storage/ archives. UBS was ordered to produce all responsive e-mail on its optical discs or on its active servers at its own expense [16].

In regard to inaccessible data—backup tapes and erased, damaged, or fragmented data—cost shifting would be considered.

The court in *Zubulake* noted that "the most influential response to the problem of cost-shifting" to date was the eight-factor balancing test set forth in *Rowe Entertainment*. But the court declined to employ that test on the grounds that it generally favored cost shifting as the result of being incomplete and giving equal weight to all factors.

Thus, the court devised the following seven-factor test, to be weighed in descending order of importance:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and incentive to do so;
6. The importance of the issues at stake in the litigation;
7. The relative benefits to the parties of obtaining the information [17].

The court summarized these as comprising a marginal utility test (1 and 2), cost issues (3, 4, and 5), the "rarely applicable" but potentially dominating sixth factor, and the usually least important seventh factor (one would assume that the discovery would benefit the requesting party). "But in the unusual case where production will also provide a tangible or strategic benefit to the responding party, that fact may weigh against shifting costs" [18].

The court ordered defendant to produce responsive e-mail from five backup tapes selected by the plaintiff (as well as all responsive e-mail in accessible format), after review of which the court would conduct this cost-shifting test.

The Hybrid Offspring

Most courts have adopted some combination of or variation on these early seminal cost-shifting tests. For example, in *Hagemeyer N.Am., Inc. v. Gateway Data*

Scis Corp. [19], plaintiff moved to compel the production of backup tapes that might contain relevant e-mail. The court, noting that the Seventh Circuit had not yet adopted a cost-shifting test, held that it would apply, in tiered fashion, the sampling test of *McPeek v. Ashcroft* and the seven-factor test of *Zubulake I.*

In *Wiginton v. CB Richard Ellis, Inc.* [20], the court devised a variation of the *Zubulake I* test. In this class action alleging a nationwide practice of sexual harassment, plaintiffs sought discovery of pornographic material they claimed was distributed via e-mail. Defendant initially produced a sample of e-mail backup tapes from eleven of its offices, from which plaintiffs' expert extracted the data and, pursuant to a court order defining the appropriate search terms, found responsive documents. The exact number—and therefore the results of this sampling procedure—was disputed. But by either party's calculation, responsive documents resided on the backup tapes, and the court proceeded to determine whether the cost of producing the remainder of the information requested would be an undue burden justifying cost shifting, or not.

The court modified the *Zubulake* test "by adding a factor that considers the importance of the requested discovery in resolving the issues of the litigation." Hence, the factors considered were the:

1. Likelihood of discovering critical information (marginal utility factor);
2. Availability of the information from other sources;
3. Amount in controversy as compared to the total cost of production;
4. Parties' resources, as compared to the total cost of production;
5. Relative ability of each party to control costs and its incentive to do so;
6. Importance of the issues at stake in the litigation;
7. Importance of the requested discovery in resolving the issues at stake in the litigation;
8. Relative benefits to the parties of obtaining the information [21].

Other courts limit the number of factors to be considered in deciding whether to shift costs. For example, in *Multitechnology Services, L.P. v. Verizon* [22], the defendant moved for a protective order regarding plaintiff's request for information concerning Verizon's past and present customers, available in electronic format in its computer databases and archives. Verizon objected that responding to the request would be unduly burdensome, costing some $60,000.

Plaintiff urged the court to apply the *Zubulake I* test that, it argued, would show that cost shifting was not warranted. The court, noting that *Zubulake I* was not binding authority, did not analyze all of the seven factors in the *Zubulake I* balancing test. It did consider the availability of the information

from other sources and the cost of production compared to the total amount in controversy. But most significant to the *Verizon* court were considerations of relative benefit and ability to control costs: "The court finds that requiring the parties to evenly shoulder the expense is the most effective resolution because it balances the benefit of the discovery to MTS and provides Verizon with incentive to manage the costs it incurs …" [23].

Cost Shifting and the Amendments to Rule 26(b)(2)

Preamendment, the courts were divided on the question of whether the cost-shifting analysis should be different for accessible versus inaccessible ESI. The court in *Zubulake I* held that cost shifting should be considered "wholly inappropriate" when a party is requesting accessible data. In contrast, the court in *OpenTV v. Liberate Technologies* [24] agreed with that principle, but ordered cost shifting in the discovery of a source code database that Judge Scheindlin would presumably have deemed accessible. As discussed above, *Verizon* applied yet another conceptual approach, rejecting the accessible/inaccessible distinction, and ordering the plaintiff to pay part of the costs of obtaining information from databases and archives [25]. No distinction was made between accessible and inaccessible data in applying the marginal utility test [26].

Rule 26(b)(2)(B) seems to have answered this question. If the rules are different for the discovery of ESI, in general, then presumably the cost-shifting rules are different, as well. But what are the new cost-shifting rules to be?

Reasonably Accessible ESI

The preamendment cost-shifting tests were based on and derived from the proportionality test of Fed. R. Civ. P. 26(b)(2), now codified in Rule 26(b)(2)(C). The Committee Note provides that "[t]he limitations of Rule 26(b)(2)(C) continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources" [27]. But the clear implication of the different treatment accorded accessible and inaccessible ESI is that cost shifting is, in general, less appropriate when it is accessible ESI that is at issue, and perhaps even "wholly inappropriate" [28].

Not Reasonably Accessible ESI

Assuming the requesting party has shown good cause to discover ESI not reasonably accessible, under what circumstances should all or part of the costs be borne by the requesting party? The Committee Note to Rule 26(b) states that a

party's willingness to bear or share in the costs may be weighed in the good cause inquiry. But the question still remains: *when* should reference be made to cost shifting when conducting the good-cause analysis?

The answer cannot easily be found by reference to the preamendment, multifactor cost-shifting tests because these have been incorporated into the good-cause analysis itself. That is, the seven considerations to be balanced in determining whether good cause has been shown are nearly identical to the cost-shifting test of *Zubulake I* and similar to that set forth in *Rowe Entertainment*.

What additional factors, then, should be considered in deciding whether to shift costs [29]? The total cost of production—not included in the good-cause analysis—would be one such factor. But the cost of production would presumably already have been considered in determining whether the ESI sought in discovery was not reasonably accessible because of undue burden or cost.

One solution would be to shift all or part of the costs if the good-cause analysis is equivocal. Otherwise stated, if the factors balance fairly evenly, requiring the requesting party to pay would tip the balance conclusively towards requiring production. The problem with this approach is that it is too easy. That is, the multifactor good-cause test is complex, and fully assessing what the result should be is a complicated process. With all due respect to the courts, if cost shifting too easily solves the problem, cost shifting may be ordered too often to truly comport with the presumption that the responding party pays, and may create yet another systemic advantage for the deep-pocketed litigant.

Moreover, it should be noted that the factors that tip the balance *toward* a finding that good cause has been shown weigh *against* cost shifting in the preamendment cost-shifting tests. As argued in Chapter 5, if, in regard to ESI sought in a discovery request, cost shifting would not have been appropriate under the "unduly burdensome" standard of those tests, that ESI should not be considered not reasonably accessible because of undue burden or cost because the latter should be a more stringent or exacting test.

The better argument seems to be, then, that if the good-cause showing has been made, based on the seven factors set forth in the Committee Note, costs should not be shifted because in effect the requesting party has disproven the responding party's initial showing that the ESI sought is not reasonably accessible [30]. It is, however, reasonable to predict that the courts will shift all or part of the costs of discovering ESI that is not reasonably accessible when considerations of fairness and efficiency counsel that result [31]. Only time will tell how the courts will resolve cost shifting in this new, two-tiered analytical environment [32].

Postamendment Decisions

In *Semroth v. City of Wichita* [33], a sexual harassment and discrimination case, plaintiffs in discovery requested e-mail from backup tapes, and after negotiating with the defendant asked specifically for copies of e-mail from 117 different supervising officers stored on the backup tape of a specific day. The defendant moved for an order compelling plaintiffs to pay the cost of restoring the tape: the cost of restoration would be approximately $2,624.95 [34].

Plaintiffs first argued that the low cost of compliance in this case would make any cost shifting unnecessary. The court disagreed with that "bright-line argument": " … the data sought is on an [sic] medium which can be classified as 'inaccessible,' i.e., back-up tapes, which must be restored before they can be searched for relevant data. This suggests that the process of producing such data could constitute an undue burden on Defendant" [35]. "However," the court noted, "the Amendment to Rule 26(b)(2)(B) makes clear that any inaccessibility must be 'because of undue burden or cost.' This brings into play Plaintiffs' argument that the costs in this case are not so significant as to cause an undue burden on the City" [36].

The court resolved this apparent dilemma by analyzing the cost-shifting issue based upon the factors identified in *Zubulake I* and the seven factors set forth in the Committee Note to Rule 26(b)(2), the similarities of which, the court noted, were "readily apparent" [37]. But though the potential benefits of discovery, the relative resources of the parties, and the other factors were considered, at bottom the court found that the cost of restoring and searching the single e-mail backup tape was not such as to render that tape "not reasonably accessible because of undue burden or cost." Accordingly, cost shifting was not warranted [38]. The court did, however, limit the number of keywords to be used and the number of mailboxes to be searched once the data was restored.

In *Ameriwood Industries, Inc. v. Liberman* [39], plaintiff brought breach of fiduciary duty and other causes of action against former employees and their recently formed company, alleging that the defendants had improperly used plaintiff's computers and misappropriated confidential information. In document requests plaintiff requested the hard drives of defendants' computers or mirror images thereof. Defendants objected and plaintiff moved to compel.

In opposition to the motion, defendants argued that responsive information had already been produced, so that mirror imaging was not necessary and, in the alternative, that the data requested in the mirror image was not reasonably accessible. Based on the evidence submitted by defendants as to the significant cost of copying the hard drives, recovering deleted information, and translating the recovered data into reviewable format, the court agreed that the requested information was "not reasonably accessible" within the meaning of Fed. R. Civ. P. 26(b)(2)(B) [40]. But the court also found that plaintiff had shown "good

cause" for discovery, primarily because of the evidence of a "discrepancy" in defendants' prior production (plaintiff submitted an e-mail sent by one of the defendants to one of plaintiff's customers that had not been produced by defendants) and the fact that the alleged wrong had been committed by using the computers at issue [41]. In regard to costs, the court stated [42]:

> In performing the good cause inquiry, the Court is also permitted to set conditions for discovery, including but not limited to payment by the requesting party of part or all of the reasonable costs of obtaining information from the sources that are not reasonably accessible. See Fed. R. Civ. P. 26(b)(2) advisory committee's note. As plaintiff does not object to incurring the costs for the requested procedures and defendants do not perform these procedures in the regular course of their business, plaintiff will incur the costs involved …

Postamendment Technology Trends

As technology continues to advance and evolve, new and better tools are becoming available for organizing, maintaining, and searching large data sets more efficiently. Businesses and courts license and use Google's search technology, for example [43]. New online storage services such as Amazon's Simple Storage Service (S3) [44] are being offered at competitive prices, making online storage more affordable. Businesses will continue to drive toward making operational data as accessible as feasible. More sophisticated ESI management will be required both for operational and legal purposes—to meet substantive, business, or regulatory demands in financial services (consider the possibility of hedge fund regulation), accounting (Sarbanes Oxley or its successor), health (HIPAA), export/import controls, government security requirements, or other highly regulated or closely monitored data. All of these trends will likely render truly inaccessible data a rare commodity.

Endnotes

[1] Oppenheimer Fund Inc. v. Sanders, 437 U.S. 340 (1978).

[2] Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) (Zubulake I), quoting Rowe Entm't, Inc. v. William Morris Agency, 205 F.R.D. 421, 429 (S.D.N.Y. 2002).

[3] Oppenheimer Fund Inc. v. Sanders, 437 U.S. at 358.

[4] Zubulake I, 217 F.R.D. at 316.

[5] 202 F.R.D. 31 (D. D.C. 2001).

[6] 205 F.R.D. 421 (S.D.N.Y. 2002).

[7] Zubulake I.

[8] 202 F.R.D. at 34.

[9] *Id.* at 35.

[10] "If a party maintains electronic data for the purpose of utilizing it in connection with current activities, it may be expected to respond to discovery requests at its own expense." "Conversely, however, a party that happens to retain vestigial data for no current business purposes, but only in case of an emergency or simply because it has neglected to discard it, should not be put to the expense of producing it." 205 F.R.D. at 430–431.

[11] The benefit to the requesting party would be obvious. As for the responding party, it could benefit by the process of production "if a program created to conduct a search for purposes of discovery could be useful for business purposes, or if its review of the data would assist it in the litigation." 205 F.R.D. at 431.

[12] *Followed by, e.g.,* Medtronic Sofamor Danek, Inc. v. Sofamor Danek Holding, Inc., 2003 U.S. Dist. LEXIS 8587 (W.D.Tenn. 2003).

[13] 217 F.R.D. 309 (S.D.N.Y. 2003).

[14] Defendant also argued that it had produced all responsive documents, which, based on the record, the court found "unpersuasive" because defendant had not searched the backup tapes, and Zubulake had in her possession e-mail that would have been responsive to her requests but that the defendant had not produced. 217 F.R.D. at 317.

[15] *Id.* at 320.

[16] *Id.* at 324.

[17] *Followed by, e.g.,* OpenTV v. Liberate Technologies, 219 F.R.D. 474 (N.D. Cal. 2003).

[18] 217 F.R.D. at 323.

[19] 222 F.R.D. 594 (E.D. Wis. 2004).

[20] 229 F.R.D. 568 (N.D. Ill. 2004).

[21] *Id.* at 573.

[22] 2004 U.S. Dist. LEXIS 12957 (N.D. Tex. 2004).

[23] *Id.* at *5.

[24] 219 F.R.D. 474.

[25] 2004 U.S. Dist. LEXIS at *3.

[26] *See also* J.C. Associates v. Fid. & Guar. Ins. Co., 2006 U.S. Dist. LEXIS 32919 (D. D.C. 2006), in which Judge Facciola applies the marginal utility test to claim and litigation files that the defendant had searched electronically and which files were then, presumably, accessible as defined by the court in Zubulake I.

[27] Advisory Committee Note, Chapter 3, p. 35.

[28] Zubulake, I., 217 F.R.D. at 320.

[29] The Committee Note specifies that the good-cause inquiry is "coupled with the authority to set conditions," including the condition that the requesting party pay all or part of the costs of discovery.

[30] As noted elsewhere, the party objecting to discovery has the burden of showing that the ESI at issue is not reasonably accessible because of undue burden or cost.

[31] *Compare* Semroth v. City of Wichita, 2006 U.S. Dist. LEXIS 83363 (D. Kan. 2006) *with* Ameriwood Industries, Inc. v. Liberman, 2006 U.S. Dist. LEXIS 93380 (E.D. Mo. 2006).

[32] For this reason, it is difficult to predict the outcome of our opening hypothetical. Presumably, both sides would have to bolster their arguments with additional factors for the court to consider.

[33] 2006 U.S. Dist. LEXIS 83363.

[34] The defendant argued that the cost that had been incurred in responding to other discovery requests and the cost of reviewing the e-mail recovered from the tapes should also be included in the analysis, but the court found that the former was not directly related to the production, and the latter was not appropriate for cost shifting.

[35] 2006 U.S. Dist. LEXIS 83363 at *23, citing Zubulake I, 217 F.R.D. at 218.

[36] *Id.* at *23, *24.

[37] *Id.* at *22. The court in *Semroth* did not, then, consider the "good cause" analysis as distinct from the cost-shifting analysis, a vexing conflict discussed in this chapter.

[38 *Id.* at *35.

[39] 2006 U.S. Dist. LEXIS 93380 (E.D. Mo. 2006).

[40] *Id.* at *11, 12.

[41] *Id.* at *13, 14.

[42] *Id.* at *15.

[43] For example: Maryland Judiciary at http://mdcourts.gov. is powered by Google.

[44] Amazon's Simple Storage Service (S3) offers online storage service with on-demand scalability. It charges only for actual usage without minimum fees or start-up costs. Prices as of June 1, 2007: $0.15/GB/month of storage used and $0.10/GB of data uploaded; $0.18/GB of first 10 TB per month of data downloaded; $0.16/GB or next 40 TB per month of data downloaded; and $0.13/GB downloaded per month over 50 TB.

Part III
ESI Discovery

7

Planning for Discovery

Introduction

The federal rules and emerging state court rules direct the parties to pay "early attention" to electronic discovery issues [1]. This chapter explains what issues should be addressed by the parties early in the discovery process and sets forth the procedures to be followed for bringing those issues to the attention of the trial court.

In planning for discovery, counsel must also identify the kinds of electronically stored information that might be helpful in support of the party's claims or defenses. This is no simple task: the universe of potentially discoverable ESI is large, complex, and ever expanding. This chapter sets forth different approaches for effectively exploring that universe [2].

We conclude with an overview of computer forensics. We describe, in general terms, what the science of computer forensics is and analyze when counsel should consider engaging a computer forensics expert.

Procedural Rules

The three step procedure for planning discovery in the federal rules—initial disclosures, party conference to develop a discovery plan, and hearing and order to memorialize the plan and determine unresolved issues—now specifically incorporates ESI in the process.

Fed. R. Civ. P. 26(a)(B) requires a party to disclose "a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control

of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment." Before the rule was amended, concern was expressed about requiring the initial disclosure of ESI because it is "often voluminous and dispersed, and can be burdensome to locate and review, and early in the case the parties may not be able to identify with precision the information that will be called for in discovery" [3]. The response of the committee to this concern guides parties in implementing the early disclosure requirement for ESI: "The obligation does not force a premature search, but only requires disclosure, either initially or by way of supplementation, of information that the disclosing party has decided it may use to support its case" [4]. But in order to make sufficient initial disclosures, counsel must have some knowledge of the client's ESI inventory, location, and management systems [5].

Fed. R. Civ. P. 26(f) requires the parties to address issues related to the discovery of ESI in the discovery planning conference. Specifically, Rule 26(f)(3) directs the parties to discuss "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced" [6]. The parties are also to consider "any issues relating to preserving discoverable information" and "any issues relating to claims of privilege or of protection as trial-preparation material including—if the parties agree on a procedure to assert such claims after production—whether to ask the court to include their agreement in an order" [7]. Though the last two items apply to all discoverable information, these were added to the previous version of the rule because preservation and provisions for the assertion of privilege "can be particularly important with regard to electronically stored information" [8].

The particular issues relating to the discovery of electronically stored information that should be addressed depend on the specifics of each case. The Committee Note suggests the following [9]:

> … the parties may specify the topics for such discovery and the time period for which discovery will be sought. They may identify the various sources for such information within a party's control that should be searched for electronically stored information. They may discuss whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information. See Rule 26(b)(2)(B). Rule 26(f)(3) explicitly directs the parties to discuss the form or forms in which electronically stored information might be produced.

Preservation issues should be addressed early because ESI is dynamic and because the "ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information" [10]. *The Manual for Complex Litigation* (4th), § 40.25(2)(2004), lists specific items within the topic of preservation as to which the parties should confer:

(a) The extent of the preservation obligation, identifying the types of material to be preserved, the subject matter, time frame, the authors and addressees, and keywords to be used in identifying responsive materials;

(b) The identification of persons responsible for carrying out preservation obligations on behalf of each party;

(c) The form and method of providing notice of the duty to preserve to persons identified as custodians of documents, data, and tangible things;

(d) The mechanisms for monitoring, certifying, or auditing custodian compliance with preservation obligations;

(e) Whether preservation will require suspending or modifying any routine business processes or procedures, with special attention to document- management programs and the recycling of computer data storage media;

(f) The methods to preserve any volatile but potentially discoverable material, such as voicemail, active data in databases, or electronic messages;

(g) The anticipated costs of preservation and ways to reduce or share these costs;

(h) A mechanism to review and modify the preservation obligation as discovery proceeds, eliminating or adding particular categories of documents, data, and tangible things.

The Committee Note directs the parties to "pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing operations" in discussing preservation.

Rule 26(f) was amended to include the assertion of privilege and work-product protection among the issues to be discussed because of the difficulties of guarding ESI against waiver. Because of the volume of ESI that typically must be reviewed, and the complexity of review—requiring the identification and reformatting of metadata into a readable format, for example—the process may be more expensive and burdensome, and the risk of inadvertent disclosure more substantial, than it is when applied to paper documents [11].

Accordingly, the parties are encouraged to minimize the costs and reduce the risk of waiver by agreeing to protocols for review and production [12]. The Committee Note includes the following exemplars for the parties to consider:

> They may agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection—sometimes known as a "quick peek." The requesting party then designates the documents it wishes to have actually produced. This designation

> is the Rule 34 request. The responding party then responds in the usual course, screening only those documents actually requested for formal production and asserting privilege claims as provided in Rule 26(b)(5)(A). On other occasions, parties enter agreements—sometimes called "clawback agreements"—that production without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances.

Any such agreement regarding the assertion of privilege and work product protection may be included in the case management or other order [13]. The scheduling order may also include other provisions for disclosure or discovery of electronically stored information reached by the parties or imposed by the court.

Counsel practicing in state courts should of course be aware of any local rules of procedure regarding the discovery of ESI [14], and prepared for the courts to become more actively engaged in managing that discovery. For example, *The Guidelines for State Trial Courts* recommend that the court issue an order requiring the exchange of the following information if the parties have not reached an agreement on a discovery schedule for ESI [15]:

> (1) A list of the person(s) most knowledgeable about the relevant computer system(s) or network(s), the storage and retrieval of electronically-stored information, and the backup, archiving, retention, and routine destruction of electronically stored information, together with the pertinent contact information and a brief description of each person's responsibilities;
> (2) A list of the most likely custodian(s), other than the party, of relevant electronic data, together with the pertinent contact information, a brief description of each custodian's responsibilities, and a description of the electronically-stored information in each custodian's possession, custody, or control;
> (3) A list of each electronic system that may contain relevant electronically-stored information and each potentially relevant electronic system that was operating during the time periods relevant to the matters in dispute, together with a general description of each system;
> (4) An indication whether relevant electronically-stored information may be of limited accessibility or duration of existence (e.g., because they are stored on media, systems, or formats no longer in use, because it is subject to destruction in the routine course of business, or because retrieval may be very costly;
> (5) A list of relevant electronically-stored information that has been stored off-site or off-system;
> (6) A description of any efforts undertaken, to date, to preserve relevant electronically-stored information, including any suspension of regular document destruction, removal of computer media with relevant information

from its operational environment and placing it in secure storage for access during litigation; or the making of forensic image back-ups of such computer media;
(7) The form of production preferred by the party; and
(8) Notice of any known problems reasonably anticipated to arise in connection with compliance with e-discovery requests, including any limitations on search efforts considered to be burdensome or oppressive or unreasonably expensive; the need for any shifting or allocation of costs; the identification of potentially relevant data that is likely to be destroyed or altered in the normal course of operations or pursuant to the party's document retention policy.

Identifying Potentially Discoverable ESI

The greatest challenge in discovery is asking for all the relevant information the other party has without knowing in advance exactly what that information will be [16]. Attorneys have tried and true tactics for attacking this problem: conducting a thorough study of the adversary's operations and personnel in publicly available documents; consulting experts in the field; and drafting discovery requests broadly to include all documents that refer or relate to a particular topic or issue are among them. Adding an IT specialist to the list of experts consulted may be all that is necessary to employ these tactics in the discovery of ESI, particularly for those attorneys already adept with technology. But others may find additional tools to be necessary. And ESI is different enough from paper documents that alternative approaches to conceiving of the universe of potentially discoverable information should be useful to any practitioner.

The following are four approaches to planning for the discovery of ESI. For some cases or issues, one alone may suffice. But more commonly these should be used in combination, as explained in the examples of discovery planning that follow the description of the models. And the overall approach should be iterative, using sequential discovery requests. Unlike in the paper world, in which counsel could focus almost exclusively on targeting particular *information,* in discovering ESI counsel may need to seek discovery regarding the responding party's systems and processes for creating and storing information before he or she can effectively ask for the information itself.

The "Where" or the Computing Environment Model

Much attention is paid in the rules of procedure and in secondary legal sources to the need to understand *where* discoverable information might be found. The Committee Note to Fed. R. Civ. P. 26(f) suggests that potential sources for discoverable ESI should be discussed by the parties, and the *Civil Discovery*

Standards of the Litigation Section of the American Bar Association list 15 "platforms" that should be considered in preparing for electronic discovery [17]. Another way to characterize this approach is that counsel should understand the opposing party's computing environment. In addition to storage platforms or devices, that environment would include data processing devices, network architecture, software applications, producers and users of data, the key processes, and the organization that operates and maintains such computing environment.

In a sense, the where approach does not lead directly to discoverable information unless, of course, the existence or nonexistence of some aspect of the opposing party's computing environment is relevant to an issue in the case. That is, knowing that a party has 20 servers on site does not necessarily assist in drafting a request for production of relevant ESI on any of those servers. But the connection between the ESI environment and the actual information being sought may be close enough that this approach would identify discoverable information. A simple example is a BlackBerry: if the responding party provides BlackBerrys for employees' use, any e-mail messages, logs of Web access, SMS or instant messaging messages, organizer data, phone logs, and any logs of remote access to the corporate transactional systems from those BlackBerrys that refer or relate to the facts at issue would be included in discovery requests.

In addition to assisting in the identification of discoverable information, the where approach provides other information that may be useful as discovery proceeds. For example, having a thorough inventory of the sources of potentially discoverable ESI early in the discovery process ensures that such sources are not lost, intentionally or inadvertently, before trial. And by knowing where discoverable ESI is stored, the requesting party may be better able to tailor requests to avoid overbroad objections and to predict whether it may have to pay all or part of the costs of production.

The Data Checklist Model

In the universe of potentially discoverable ESI, certain categories are of common enough usage in any business to be included in a checklist for sources of relevant information. E-mail, word processing documents, spreadsheets, presentation documents, graphics, animations, images, audio, video, and voice mail are obvious candidates [18]. Metadata [19], computer access audit trails [20], and radio-frequency identification (RFID) from goods could be on the list. Data is created in mobile devices, including instant messages and message logs [21], location-identification data in installed GPS systems, and driving data on car computers. And the list should include online data encompassing Web site pages and data stored by third-party providers, such as ISPs and online data backup service providers.

A checklist of types of data, regularly updated, has the advantages of simplicity and familiarity: one has a good sense of what information a Web page can provide, for example. And although a discrete list is not well-suited to capturing ESI in its varying renditions or forms, for specific issues it may work as well as any approach. For example, in *Padilla v. Price Toyota* [22], the plaintiff was injured in an automobile collision and alleged that a malfunction of the air-bag system in the Toyota Corolla in which she was riding caused or contributed to her injuries. In discovery she sought and obtained data from the car's black box, which recorded certain triggering events, including air-bag release.

The Life-Cycle Model

"The records lifecycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and archive to final disposition" [23]. ESI, unlike paper documents, has a complex life cycle through which the form and accessibility of the ESI evolves. A simple example is a Word document created in electronic and accessible form; maintained during the active phase of its life cycle in an active file, on a disc, and/or as a print copy or PDF image; used in any of the forms in which it is maintained; stored during the inactive phase for some period of time in paper or electronic form (and the latter may be accessible or relatively inaccessible); and ultimately shredded or permanently deleted.

The life-cycle model is a natural extension and synthesis of the where and the checklist models. It may prove to be particularly useful in situations in which the previous two approaches have not produced the expected results. In addition, analyzing the same information through its applicable life cycle may produce interesting results. For example, when counsel has obtained ESI in one version of its life cycle, or has a paper document and the information contained therein was at some point in electronic form, reviewing that information from alternative phases of its life cycle can be used to check for completeness, authentication, and alterations, for example. Using the life-cycle model will also facilitate communication with the IT professionals, for whom the concept in regard to managing ESI should be familiar.

Revised Refer-or-Relate Model

Information may be discoverable—and tend to prove or disprove an issue in a case—because it has a logical or causal connection to a known fact. Hence counsel seeks discovery of all documents that refer or relate [24] to the execution of a software licensing agreement, for example, in a dispute regarding the intent of particular terms of that agreement. The responding party has little difficulty responding by producing correspondence between the parties during contract

negotiations and specifications or codes that identify what software is included in the license—because the thought process for identifying documents with a logical or causal connection to the contract is familiar.

That thought process is not so familiar when the task is identifying responsive ESI. Or, even if potentially responsive ESI can be identified, an argument could be made that it does not technically refer, logically or causally, to the licensing agreement. For example, assuming the contract was created electronically, the program used to create the document likely created metadata, including the name of the person who created the document, the names of the persons who edited the contract, and how many times the document was printed. Any of this metadata could be relevant and discoverable. But the responding party might not think to review the metadata. And it could be argued that this embedded data—created automatically, without the knowledge of the persons who negotiated the contract—has no logical connection with the intended meaning of the contract [25]. Another example of this potential problem is a link from one Web site to another. The information in the linked site could be relevant for any number of reasons—to show knowledge of a particular fact, for example. But the linked site may not specifically refer or relate to the *information* in the original page, even though the URLs themselves are of course related in some fashion. Depending on how the request is phrased, the linked information would not be produced.

Determining whether to seek ESI interconnected in some fashion with other ESI or paper documents is no simple task. Asking for all metadata connected to a contract would likely be objectionable as overbroad and, in any event, if responsive data were produced it would be largely redundant or incomprehensible. Yet asking only for ESI that refers or relates to a particular fact is not sufficient. The better phraseology between the two will depend, in part, on the nature of the case, the relations between opposing counsel and the opposing parties, and decisions made during the meet and confer. The way that counsel phrases such requests for production will be significantly more effective if the previous three models have been exhausted first. But in general, the following might be considered: all ESI evidencing, reflecting, incorporating, effecting, or defining all information followed by the appropriate combination of where, data checklist, or life-cycle limiters.

Models in Practice

The following are examples of how to put these models in practice. The discovery requests and responses are hypothetical, but the issues they address have arisen in actual cases [26].

Missing e-mail. In a case against a city's executive, the plaintiffs' class alleged that regulations promulgated by the city's corrections agency in response

to legislation concerning prison conditions failed to meet the objectives of the legislation and were therefore unreasonable as a matter of law. The plaintiffs had acquired the report of a consultant hired by the city to make recommendations for implementing the legislation, which report supported the plaintiffs' position. In the litigation, the city took the position that the consultant's report had been duly analyzed and rejected for good and sufficient reasons. However, the plaintiffs had reason to believe that the prior director of the corrections agency—now deceased—had strongly supported the consultant's recommendations. Evidence of that support, if it could be located, would bolster the plaintiffs' case.

On plaintiffs' checklist for evidence was, of course, e-mail. Plaintiffs requested any e-mail correspondence from or to the director, during the relevant time period, containing specific terms including the name of the consultant, and reference to the legislation at issue, among other things [27]. The defendant produced a paper copy of one e-mail from the director to the consultant, with little of substance in the correspondence.

Plaintiffs then sought to determine where any additional e-mail might be located. Counsel for plaintiffs deposed the network administrator and ascertained that during the relevant time period the agency first used Lotus Notes for e-mail. With that system all e-mail was replicated and stored on the agency's server and, if not deleted by the recipient, also stored on the hard drive of the recipient's desktop or laptop (certain employees, including the director, were issued laptops for business use). The agency then switched to a citywide system using Outlook. Using Outlook, e-mail was backed up every 24 hours, stored on a server for 90 days, then sent to an online backup storage provider. According to the city's contract with that provider, the backed up e-mail would be maintained for seven days.

Through additional questioning, plaintiffs ascertained that all servers and hard drives had been appropriately searched, and only the one e-mail had been located. But plaintiffs had not yet completed their search for additional e-mail through its life cycle. They obtained a copy of the city's contract with the online service provider, which indeed provided, as the network administrator had testified, that the city's e-mail would be maintained for seven days. The contract further provided, however, that in the event of an emergency, and for an additional fee, the city could retrieve its e-mail backup files stored on disc in the provider's backup data storage facility for three years from the date the data was received by the provider. Only after that three-year period had expired, the contract provided, would the data be irretrievably destroyed. Plaintiffs filed a motion to compel the city to retrieve its e-mail from the provider. Because plaintiffs had other evidence that showed the director in fact supported the consultant's recommendations, thus demonstrating the likelihood that relevant e-mail would be discovered, and because the provider maintained the city's e-mail in searchable form—the burden of retrieving selected e-mail would not be undue—the court

granted plaintiffs' motion. E-mail from the prior director of the corrections' agency expressing his support of the consultant's recommendations was retrieved.

Verifying accuracy and completeness. In a medical malpractice case arising from a birth injury, at the request of plaintiff's counsel, the defendant hospital produced a fetal monitor strip, a paper document evidencing the data obtained by the electronic fetal monitor during labor and delivery. Because the hospital had initially taken the position that the fetal monitor strip could not be found, and produced the paper document months after the litigation commenced, plaintiff's counsel had some concern regarding the completeness of the record of the monitoring, and sent the document to an expert obstetrician to review. The expert found that the data was not complete: portions of the record were discontinuous, showing gaps where no data was recorded on the paper.

With the report of the expert and the fact of the belated production of the fetal monitor strip, plaintiff was able to obtain discovery, over the defendant's objection, of the ESI environment and ESI life cycle relative to the electronic fetal monitor used on the plaintiff. Plaintiff determined that the equipment used for fetal monitoring by the hospital stored the data obtained during the delivery on a hard drive [28], and that, pursuant to the hospital's patient record processing system, all hard drives in disparate storage media were searched daily by patient name and data from those hard drives, copied and sent via a secure local network to that patient's electronic archive. The hard drives were purged as required by memory limitations on an irregular basis.

The electronic patient archive was copied to microfiche within 90 days after the patient's discharge, and the fiche was sent to an off-site storage facility. The fiche, and not the electronic archive, was deemed the official patient record. Accordingly, the hospital's document management policy did not require that the archive be maintained for any particular period of time after the data it contained was copied to the fiche. On the other hand, the hospital had not adopted any specific document management policy for deleting patient archives from the server. Accordingly, plaintiff requested that the hospital search the server for her record, and it was produced, presumably complete.

Proving knowledge. In a case arising from injuries sustained by a student in a hazing incident on campus, the defendant, the national fraternity, took the position that its policy prohibiting hazing in any of its chapters exonerated it from any liability. In order to implicate the defendant, the plaintiff sought to prove that the defendant knew, or should have known, of studies and reports showing that the mere prohibition of hazing was clearly insufficient to halt the practice and making recommendations for best practices to prevent hazing injuries.

On the plaintiff's checklist for potential sources of evidence as to defendant's knowledge was the Internet. Plaintiff explored the defendant's Web site

to determine whether any links on the site pointed to any of the relevant information. Plaintiff also checked the Internet Archive's Wayback Machine [29] to review previous versions of the site.

What relevant online information the defendant's principals had accessed could be ascertained from ESI residing on the employee's desktop computer (in bookmarks, history logs, temporary Internet storage logs, and cookies, for example). Other possible sources would be the access logs of sites visited, the ISP's logs, and/or the search engine logs.

Plaintiff explored the issue of the defendant's knowledge of the best practices studies from online information in deposing the defendant's president. (In response to requests for production defendant had denied having any data in its possession or control relevant to the issue.) The witness testified that the Internet was by far his primary source for acquiring fraternity-related information, including risk management information. He also testified that he had "some idea" about the best practices studies, though he denied recalling those studies in any detail, and that it was "probable" he had seen that information on a Web site. Plaintiff asked whether the witness had visited five particular Web sites, which were known by plaintiff to post prominently the relevant information. The witness could not recall. But he admitted that the organizations sponsoring those Web sites were "well known" in the industry, and that it was "possible" that he had visited those Web sites. He denied having bookmarked or otherwise maintained any record of having visited any of the key sites.

One option for plaintiff would have been to request a forensics examination of the witness's computer to confirm that the witness had viewed the key sites and determine how often the sites had been visited. But this option could be costly and time-consuming because of the need to procure an expert and to implement the measures the court would require be taken to prevent the disclosure of irrelevant or privileged information.

Accordingly, plaintiff chose to pursue third-party discovery. Plaintiff first requested the witness's Internet Protocol (IP) address. Defendant objected, but armed with the witness's testimony, and given the importance of the issue to the case, the court granted plaintiff's motion to compel. For the same reasons, the court denied defendant's motion to quash plaintiff's subpoena to the ISP for the subset of log records showing when the device from the witness's IP address accessed any of the target Web sites. Those logs showed multiple visits by the witness to all the target Web sites.

These models should prove useful starting points in planning for the discovery of the opposing party's ESI. But just as ESI continues to evolve rapidly, so, too, must the practitioner continue to develop sophisticated tactics for identifying discoverable ESI. Perhaps the most important overall strategy, and that which informs the models, is to take whatever steps are necessary, including but

not limited to consulting with IT, to understand not only the opposing party's computing environment, but its ESI environment.

Computer Forensics

> Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law. It may include the secure collection of computer data; the examination of suspect data to determine details such as origin and content; the presentation of computer based information to courts of law; and the application of a country's laws to computer practice. Forensics may involve recreating "deleted" or missing files from hard drives, validating dates and logged in authors/editors of documents, and certifying key elements of documents and/or hardware for legal purposes [30].

It is beyond the scope of this book to plunge too deeply into the intricacies of the science of computer forensics. Instead, we cover those issues within the overall topic with which a litigator must be familiar: of what, in general, a computer forensics examination consists and when one should engage a computer forensics expert.

The Forensics Examination

A computer forensics expert can be engaged to fill a number of roles, from assisting in the identification of sources of potentially discoverable information to testifying at trial. The core service provided by such an expert is, however, the capture and processing of ESI.

Nominally, a computer forensics analysis is fairly straightforward. The expert first images the medium under investigation, using specialized equipment to capture the duplicate without altering any of the original ESI. As a part of this process, the expert computes a cryptographic hash value of the data on that medium and of the image, to ensure that the data has been captured intact and unaltered. Different algorithms are used to compute a hash value: two commonly employed are MD5 and SHA-1.

Imaging the drive is the starting point. The recovery and analysis phases follow. The expert employs another set of specialized tools and skills to recover deleted information from the imaged medium, render the recovered ESI to a reviewable form, and order all the imaged ESI for presentation to the attorneys. The data imaging could be accomplished internally—using IT staff—with the expert employed only to do the analysis. But commonly the expert performs the forensic examination as a whole, if for no other reason than to make the chain of

custody shorter and simpler. It should be noted that once the medium is imaged, the analysis can be performed independently by different experts, should the litigator desire more than one analysis or report.

In the analysis, the expert will be reconstructing deleted data but also bringing his or her expertise to bear on uncovering clues about the medium and its user. For example, the expert may be examining the system for hidden files and accessing encrypted and password-protected files. Temporary and swap files may provide information about how the system was used, and unallocated space on disk and slack space in current files may provide additional clues and data fragments. Most operating systems and desktop automation software—Microsoft Windows (including Internet Explorer) and Office, for example—come preconfigured with a number of defaults that automatically capture and preserve data that can be used to reconstruct data accessed by the user. The My Recent Documents list that is accessible from the Start button in Microsoft Windows XP shows documents recently accessed by many popular applications including Microsoft Office, Adobe Acrobat, and others. Similarly, most desktop automation applications, such as Microsoft Word, Excel, PowerPoint, and Adobe Acrobat, keep track of their own recently accessed documents and maintain a list. Internet Explorer stores copies of Web pages, images, and media for faster viewing later in a special subdirectory named Temporary Internet Files. The user can typically control whether or not the recently accessed documents list is tracked and how many of these recently accessed documents the application shows in the list. In addition, the user can typically delete the history of accessed documents directly from the application. But the computer forensic experts may still be able to recover this data from deleted files and from data fragments found in unallocated space on disk and slack space in current files.

The computer forensics examination is not inexpensive. The hourly rate of a large computer forensics firm is commonly as much as $500, and the analysis can be quite labor-intensive. Further, until the analysis begins—and the complexity of the task is known—it may be difficult to obtain a firm estimate of the total cost until the project is well underway.

The significant costs associated with computer forensics are related to specialized equipment, training, and expertise needed properly to image the computer media, and the labor-intensive nature of manual analysis to reconstruct inaccessible ESI. These costs are incurred even before confronting issues of privilege or relevance. Clearly, if computer forensics can be avoided, significant costs can be saved.

Should a Computer Forensics Expert Be Retained?

Most of the time and under most circumstances reliable ESI can be obtained through discovery without resorting to computer forensics. In fact, most people

probably rightfully associate the term *computer forensics* with law enforcement, criminal investigations, computer security, and intrusion detection and prevention, rather than civil litigation. Yet computer forensics has an increasingly important role to play in civil litigation, and we believe that this role will become even more critical over time as litigants and courts continue to grapple with the ever-increasing layers of complexity engendered by ESI.

A computer forensics expert almost always must be engaged in order to obtain some types of inaccessible ESI and should be engaged when necessary to ensure the reliability of ESI when reliability is in question.

One of the most common types of inaccessible ESI is deleted data. The data may have been deleted pursuant to the company's ESI retention and destruction policies and procedures or perhaps even to attempt to conceal ESI evidence. Data is deleted when the medium is reformatted. Unintentionally, data can be deleted as a result of a computer crash, whether caused by software or hardware malfunction, or as the result of a computer virus attack or incident. Data can accidentally be overwritten through user error or inattention, for example, confusing the new data filename with the existing document name.

Regardless of how the data has been deleted, it typically cannot be recovered reliably using ordinary, or in-house tools. Moreover, most information technology departments do not have the expertise or experience to recover deleted data reliably. The reliability of information that has been recovered from deleted data may be challenged. Using a reputable forensic expert to recover as much deleted data as possible will ensure not only that the available ESI is obtained but also that it is reasonably impervious to challenge.

When the recovery of inaccessible data is not at issue, under what circumstances should counsel decide to engage the services of computer forensic expert or not? This decision can be facilitated through a cost-benefit analysis. In some cases the cost-benefit analysis will make the decision obvious. Specifically, if the case hinges on the veracity of ESI that reasonably can be expected to be challenged for authenticity or reliability, it would be prudent to employ the services of a computer forensics expert to ensure that such ESI evidence can withstand the challenge.

How does computer forensics confirm the reliability of ESI as evidence? Computer forensics uses proven tools, techniques, processes, and procedures to capture and recover ESI evidence. Its strict adherence to defined processes and its stringent adherence to documenting each and every step along the way to data capture, analysis, and recovery, make each and every step independently repeatable and verifiable. Computer forensics, like other scientific disciplines, depends on such dependable, predictable, and verifiable processes. Similar to science in general, the credibility of computer forensic protocols is established and maintained through peer-reviewed publications and the process of refuting

and superseding current protocols with more appropriate protocols as the field continues to evolve.

In most circumstances the decision to consult a computer forensics expert will be made as the result of an iterative discovery process that indicates either the lack of expected ESI—expected, based on other evidence in the case—or some type of attempt to hide or tamper with ESI. Another factor indicating the need for computer forensics would be the responding party's claim of lack of knowledge of its own computing environment.

As with any expert, counsel must define the overall objectives of the forensics examination. Care should be taken, however, not to restrict unduly the scope of work, else valuable information may not be uncovered. For example, deleted data is like a basket full of shredded paper. In order to locate information about a particular person from the pile of paper, every shred must be examined. To locate the same type of information from deleted data, all such data must be restored and analyzed.

Endnotes

[1] Advisory Committee Introduction to *Early Attention to Electronic Discovery Issues: Rule 16*, 26(a), 26(f), and Form 35, http://www.uscourts/gov/rules/Reports/ST09-2005.pdf, p. 21; n. 14, *infra*.

[2] This chapter focuses on the stage of formulating discovery requests for ESI. Assuming an argument can be made for the relevance of the ESI sought, and that the request is not ambiguous or overbroad, the targeted ESI should be subject to production. Of course, even if ESI is subject to production, or potentially discoverable, the court may impose limitations on the scope of discovery because the ESI is available from another source, for example, or require the requesting party to pay all or part of the costs. Those issues are covered in other chapters.

[3] Advisory Committee Introduction, n. 1, *supra*.

[4] *Id.*

[5] *The Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* (August 2006), ¶ 2 (hereinafter *Guidelines for State Trial Courts*) *available at* http://www.ncsonline.org/images/EDiscCCJGuidelinesFind.pdf, makes this responsibility of counsel explicit: "In any case in which an issue regarding the discovery of electronically-stored information is raised or likely to be raised, a judge should, where appropriate, encourage counsel to become familiar with the operation of the party's relevant information management systems, including how information is stored and retrieved."

[6] Considerations regarding the form of production are addressed in Chapter 4.

[7] Fed. R. Civ. P. 26(f)(4).

[8] Advisory Committtee note, Fed. R. Civ. P. 26(f), Chapter 3, p. 39. The general duty to preserve evidence before agreement is reached by the parties on the issue is addressed in Chapter 10.

[9] *Id. Guidelines for State Trial Courts*, ¶ 3(A) recommends that the trial judge "encourage" parties to meet and confer on ESI discovery issues—what is to be disclosed, the manner of its disclosure, and a discovery schedule—whether or not an initial party conference is required by the local rules.

[10] *Id.* at 39–40.

[11] The substantive law that determines under what circumstances inadvertent disclosure will be deemed a waiver of privilege is discussed in Chapter 11.

[12] Amended Rule 26(b)(5) sets forth procedures for asserting claims of privilege and work product protection after production. These procedures are explored in Chapter 8, Responding to Discovery.

[13] Fed. R.Civ. P. 16(b)(6). An agreement reached by the parties but not included in an order of the court may not be binding on third parties or protect against a finding of waiver according to the substantive law regarding privileged and confidential information. *See* Hopson v. Mayor & City Council of Baltimore, 232 F.R.D. 228 (D. Md. 2005), as discussed in Chapter 11.

[14] *See, e.g.*, California Code of Civil Procedure § 2017; Illinois Supreme Court Rules 201(b)(1), 214; Rule 196.4, Texas Rules of Civil Procedure; Rule 26(b)(5), Mississippi Rules of Civil Procedure.

[15] *Guidelines for State Trial Courts*, ¶ 3(B).

[16] What is relevant, of course, will depend on the facts and issues specific to each case.

[17] Civil Discovery Standards, Litigation Section of the American Bar Association (August, 2004), pp. 57–58, *available at* http://abanet.org/litigation/discoverystandards (last accessed Sept. 5, 2006).

[18] *Id.* at p. 57.

[19] *See* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005)

[20] *See* Touhy v. Wal-Green Co., 2006 U.S. Dist. LEXIS 41724 (W.D. Okla. 2006). Plaintiff sought this information to prove that defendant's personnel had accessed her medical records without appropriate authorization. Defendant objected on the grounds that it did not track mere access to data, but only alterations to data, and plaintiff was not contending that her information had been altered. Defendant also argued that the request was overbroad. In this case the court agreed that the request was overbroad.

[21] *See* Bill S. v. Marilyn S., 2005 N.Y. Slip Op. 51093 (April 7, 2005). At issue in this case was a request for the production of instant message logs, not the messages themselves. Because the court found that only the content would be relevant to the issues in the case it held that the logs were not discoverable.

[22] 2005 U.S. Dist. LEXIS 25720 (D. N.J. 2005).

[23] "The Sedona Conference Glossary," *E-Discovery & Digital Information Management,* (May 2005 Version), http://www.thesedonaconference.org/content/miscFiles/tsglossarymay05.pdf.

[24] *Webster's Third New International Dictionary* (Merriam-Webster, 1993) defines *refer* as having a "logical or factual connection" and *relate* as having a "logical or causal connection."

[25] *But see* Williams v. Sprint, 230 F.R.D. 640 (D. Kan. 2005), in which the court held: "When a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."

[26] The facts of these cases have been altered to prevent the possibility of adversely affecting either party in an ongoing matter.

[27] Of course, plaintiff also requested other ESI potentially evidencing the director's support for the consultant's recommendations such as letters, memoranda, and so forth.

[28] An alternative would be that the data was created for viewing by the attending physician on a monitor screen and printed on paper for record-keeping purposes, but not stored in electronic form.

[29] The Internet Archive at http://www.archive.org "is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public."

[30] The Sedona Conference Glossary, n. 23, *supra*.

8

Responding to Discovery

Introduction

A party responding to discovery requests must simultaneously achieve multiple objectives. It must "conduct a diligent search" for responsive documents [1]; review and redact as necessary to protect privileged and work-product information; organize and mark documents for identification and production; and throughout the process preserve original documents, manage any chain of custody issues, and ensure that any reproductions are accurate and appropriately identified with the original. Performing these tasks with ESI is more complicated than with paper documents, for many reasons, including increased volume and mutability.

In this chapter, we first review the nature and extent of the diligent search for ESI that the courts will require of a responding party. We next turn to the review process, focusing on product and service options to assist in the review [2]. The information provided on this topic is from the Electronic Discovery Reference Model [3], which was created by a distinguished group of attorneys, consultants, and vendors "to address the lack of standards and guidelines in the electronic discovery market" [4]. We conclude with our recommended strategies for assessing responses to requests for discovery [5].

A Diligent Search

A responding party has no obligation to examine every scrap of paper in its possession, custody, or control, and the same principle of course applies to

responding to requests for ESI [6]. But the party "must conduct a diligent search, which involves developing a reasonably comprehensive search strategy" [7].

A party's claim that it does not have the expertise to respond to a request for ESI is not an excuse. For example, in *Super Film of Am., Inc. v. UCB Films, Inc.* [8], defendant moved to compel plaintiff to produce electronic versions of e-mail, documents, databases, and spreadsheets. Plaintiff objected on the grounds that it had attempted to provide electronic copies of the documents requested within its "knowledge or expertise" of how to retrieve such documents from the company's two computers, that it did not have the expertise to recover any further electronic documents, and an order requiring such production would be unduly burdensome. The court granted the motion to compel on the grounds that a party cannot relieve itself of its discovery obligations based on a conclusory and unsupported assertion that "it does not have the expertise" to produce [9].

A "reasonably comprehensive search strategy" for ESI includes, as it would in a traditional paper case, identifying key employees and reviewing any of their files that are likely to be relevant to the claims in the litigation [10]. A party makes a proper inquiry using "reasonable selection criteria," such as search terms for accessible ESI, and sampling for responsive information in less accessible storage media such as backup tapes [11].

A party, and counsel, must diligently search for potential sources of discoverable information. For example, in *Phoenix Four, Inc. v. Strategic Res. Corp.* [12], in response to Phoenix's request for the production of documents, the defendants searched the computer system in their offices and informed their counsel, Mound Cotton, that they found no responsive electronic files or folders. They did not, however, search the servers because they were unaware that any pertinent information resided on the servers.

Subsequently, a computer technician made a service call to defendant's office in response to complaints about a malfunctioning server. The technician discovered about 25 GB of data stored in a dormant, partitioned section of the server. The computer system in defendants' office was configured in such a way that the desktop workstations did not have a drive mapping to that partitioned section of the hard drive, so that a search on the desktops would not have revealed that data. Defendants advised their counsel of the discovery, the data was retrieved, and several hundred boxes of responsive documents from that data were provided in a supplemental production.

Phoenix sought an adverse inference instruction for the "failure of the SRC Defendants and Mound Cotton to conduct a reasonable and timely inspection of computers and servers in the defendants' possession in December 2005, resulting in the late discovery and production of 200 to 300 boxes of

documents" [13]. The court agreed that the defendants, and counsel, had failed to conduct an appropriate search [14]:

> As to Mound Cotton's obligation, Judge Scheindlin has defined the contours of counsel's duty to locate relevant electronic information in *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D. N.Y. 2004) (*Zubulake V*). Counsel has the duty to properly communicate with its client to ensure that "all sources of relevant information [are] discovered." Id. at 432. To identify all such sources, counsel should "become fully familiar with [its] client's document retention policies, as well as [its] client's data retention architecture." *Id.* This effort would involve communicating with information technology personnel and the key players in the litigation to understand how electronic information is stored. *See id.*

The court found that counsel had failed in its obligations by simply accepting the clients' representations that there were no computers or electronic systems to search. Because the data on the servers was in a "difficult to access source," the defendants were not required to retrieve the information on the server [15]. But they were required to identify the server as a potential source [16].

Finally, a party may need to demonstrate to the satisfaction of the court that an appropriate and diligent search has been made. For example, in *Peskoff v. Faber* [17], Peskoff requested the production of e-mail received or authored by him while he was employed by defendant's venture capital group. Faber produced computer disks containing documents, including e-mail, that were obtained from Peskoff's computer, but the disks did not include any e-mail sent or received within a two-year period, and Peskoff moved to compel production.

Faber objected that he had produced copies of all the electronic files on Peskoff's computer hard drive and that no responsive electronic documents had been withheld. Noting that responsive e-mail could reside on, *inter alia*, the recipients' hard drive or backup tapes, and that, even if deleted, the e-mail might be recoverable, the court stated that it could not determine based on the record before it whether a reasonable search had been made. "All I know is that an archive was created 'of all Peskoff electronic files, including documents stored on his computer hard drive, e-mail, and any other Peskoff electronic documents.' (Citation omitted.) This statement tells me little, if anything about the scope of Faber's search" [18]. Accordingly, the court ordered Faber to file a "detailed affidavit specifying the nature of the search it conducted" [19]. Plaintiff would have an opportunity to respond, at which point the court would consider whether additional searches would be necessary.

Electronic Discovery Reference Model

The following is guidance from the Electronic Discovery Reference Model, reprinted from http://edrm.net [20].

Use of Technology

There are many vendors and software applications which facilitate the management, review, and production of electronic evidence. The use of these constantly evolving technologies and services should be considered for the following key phases of the review process:

Deduplication/Scope Reduction

Reducing the volume of data in a review collection translates directly into cost savings. One of the best methods of data reduction is a process known as deduplication. For instance, an e-mail message sent to three people in an organization could potentially exist in more than 10 locations within the company's systems (each user's computer, the e-mail server, backup tapes of e-mail server, etc.). Deduplication technology allows duplicate e-mail messages and other files to be tracked and reduced to one item in the review set. Because the file only appears once, it is only reviewed once which dramatically reduces the billable hours spent on the review. Deduplication also facilitates a more consistent and accurate production as the item can only be marked one time as "privileged" or "responsive" without the risk of another reviewer marking a copy differently.

Data Conversion

As … discussed [below], there are many ways to conduct a review of electronic data. Regardless of the format (native, HTML, paper or TIFF/PDF) the key is to get the review collection into a uniform state with the ability to move from item to item quickly and efficiently. Because the data gets processed, it can quickly be presented to the reviewer without the need to open the item in its native application. (See the EDRM Processing chapter). For instance, one could instantly go from an e-mail message (.msg) to a Word document (.doc) to an Excel spreadsheet (.xls) with the click of a button. Converting, or processing the data also makes it possible to tag or annotate documents with the issues and subjective codes set forth in the review objectives. (Citation omitted.) Additionally, the use of data processing technologies facilitates redaction or confidential information and production/bates numbering of responsive documents. (Citation omitted.)

Searching

Once processed, electronic data can be easily searched for names and terms. Search techniques can be applied to exclude, prioritize, and organize data thus making the review more efficient. For instance, a search of attorney names would create a review set likely to be privileged. Rapidly evolving technologies such as concept searching, visualization, and data grouping tools can help reviewers get through documents faster. The following examples illustrate the scope and benefits of these new tools:

- Concept/Context Searching—can bring issues to the surface and identify unknown items related to the case or bring similar documents together.
- Visualization Tools—show documents in a way to let the reviewer manage the information or groups of information in a more efficient way.
- Near Duplicates—indicates documents which are almost alike such as different versions of an excel worksheet.
- E-mail Thread Management Tools—lets the reviewer see all the threads of the same e-mail chain and apply consistent coding across all iterations.
- Linguistic Experts—special companies who use advanced language analysis to find and group important documents.

Selecting a Vendor—Form of Review

Determining the format for the review should … be established during the initial planning stages. A review may take many forms and utilize several different formats: manual paper review; internal review using an in-house review system; internal review using a hosted online system; external review using temp attorneys set-up in a war room with the necessary review tools. The nature and needs of the matter as well as the following factors will help determine the format of the review:

Agreements made by counsel during the meet and confer phase, or ordered by the court,

Time and cost constraints for the project at hand,

How the documents were collected,

Training required by each member of the review team,

Available resources to support different formats.

The focus of our discussion is on electronic discovery, so the format decisions will typically be in-house versus online and native versus TIFF/PDF.

Platform—In-house Versus Online

A critical decision in your vendor selection process is to determine whether you are performing an in-house review, that is, using an application that is loaded and supported within your internal network, or if you are using an online, or Web-based review tool with hosting provided by a third-party vendor.

Software vendors, responding to the demand for better ways to manage and present evidence, have developed off-the-shelf solutions that litigation firms can leverage instead of trying to build the solutions themselves. The top in-house litigation support systems all have their pros and cons. It is essential that each firm carefully select the system best suited for the type of litigation the firm handles the most. Standardizing on one of the systems will provide the ability to implement standard policies and guidelines for conducting electronic reviews. Many firms have standardized on more than one system to provide them with the ability to scale up, or down, regardless of the size or type of case that comes in the door. In-house legal departments have an opportunity to standardize on one of these systems allowing for better control of what gets turned over to outside counsel for review

This type of endeavor involves a significant up-front investment and the following may need to be acquired:

1. Scanning, coding and OCR software and hardware,
2. Electronic data processing software,
3. Document repository and review tools,
4. Adequate storage and file space on the corporate network,
5. Trained staff and ongoing support.

Another option is to go with a Web-based or online review tool. These systems typically allow access through any Internet browser. While an online tool offers less direct control over the project, it does offer increased flexibility as there are a multitude of vendors on the market with different review features and functionality that can be matched to the needs of your matter. Most online vendors will provide the full range of services needed to scan, code, process, and load your data into an online repository and make that system available through a secure

Web site. Added security may be enhanced through the use of a virtual private network (VPN) or secure socket layer (SSL).

There are an increasing number of vendors that offer the best of both worlds—providing you with an in-house software application similar to their online environment. Depending on the nature and size of the case, you can use your in-house tool, or migrate to their online system seamlessly at any point in the project.

The volume and format of the documents collected for review will often dictate where the repository will be hosted. Also, the distribution of the review team will determine whether or not the repository needs to be hosted on an enterprise wide area network, on a Citrix-type system, or on a secure extranet. Every firm has limitations to what it can host internally. Items which need to be considered to determine if the project will be hosted internally or by a third party include the following:

> Who will need access? Different organizations have policies which might prevent other organizations any access to its network. With a multiparty litigation, it may be necessary to use a Web-based system to allow all parties equal access to the data.
>
> Timing—hardware, software, and security may not be able to be established in time for the needs of the review.
>
> Expertise—there are companies who manage the workflow of a review and if your firm is new to the process it could be a good help to utilize a third-party's experience.
>
> Staffing—needs for reviews can cause peaks and valleys in resources needed. Planning for this in a review process can be managed by using a third-party hosting company.
>
> Support and training—Be aware that availability of ongoing support and training is a critical factor to consider. If you choose an in-house product, you will need to dedicate time and resource to upgrades to the system and additional user and administrator training. By contrast, any top tier vendor will offer on-going training, support, and 24-hour customer service.
>
> Security and infrastructure—can the firm's internal network handle the proposed amount of data and users estimated for the project?

Native Versus TIFF/PDF

Historically, most electronic review was done using a TIFF or PDF image of the document. The electronic data was converted to an image, the text and metadata may also have been extracted and entered into a

database so that the documents were searchable and the reviewers would look at the rendered image.

Today, most electronic discovery vendors provide the ability to perform your review in a TIFF or PDF format, and several vendors also provide a review platform that allows you to convert the data to an image (TIFF/PDF) if you so chose, but also keep a link to the data in its native format, if native format review is desired. When we speak of a native format review, we mean retaining documents in their native application (Microsoft Word, Microsoft Excel, etc.) and reviewing the documents on a platform that allows you to view the document from within that program or with a generic viewer rather than converting the documents to an image file.

Vendors who offer review within the native format must retain the integrity of the native file so that the review does not cause any spoliation of the underlying native file. This is typically done by extracting the metadata and text of the file into a database for searching purposes and retaining a link to the native file in a read-only format. These safeguards may not be in place if you review documents natively from your workstation. The mere act of opening a document may change pertinent metadata, so be cautious and understand the differences between a native review through an electronic discovery vendor and a native review performed on unprocessed files at your workstation.

E-mail files are typically not retained in their native format but may be handled in several different ways with most vendors converting e-mail files to html or a plain text format, while keeping the e-mail attachments and file system data in their native format. Because relationships between e-mails and attachments must always be maintained, reviewing e-mail in a format that preserves the metadata, conversation threads, and attachments is most desirable.

To address the inherent difficulty in making sure that every reviewer's hardware has all of the necessary applications properly loaded on their workstations in order to view the native documents, many vendors also offer the use of a generic viewer. These viewers (such as QuickViewPro) convert the native document to a plain html format that can be viewed in any browser or within the viewer itself. This eliminates the need to have the application loaded on the workstation.

This issue can also be eliminated by having all documents converted to a standard image format, such as TIFF or PDF. A benefit of this type of review is that they may reduce the amount of time it takes to open and close the applications as the reviewer moves through the documents.

There are pros and cons to each of these review formats. Using an electronic discovery vendor whose system keeps the documents in their native format during review provides these benefits:

1. It saves the time and expense of converting the entire dataset to TIFF/PDF prior to review, thereby saving the cost of imaging documents that are not going to be produced;
2. It allows you to see and review data that may not appear in some types of images such tracked changes, formulas, and hidden rows or columns;
3. It ensures that potential spoliation from inadvertently opening a native file is eliminated.

Conversion to TIFF/PDF for review provides these benefits:

1. It gives reviewers a standard, locked in formatting for all documents;
2. It gives you control over what metadata, and hidden information is produced to the opposing side;
3. Click-through rates from document to document may be faster;
4. Documents are in a production ready state so production timelines may be reduced.

It should also be noted that if you choose to perform a purely native review, and then produce in a TIFF or PDF format, you should ensure that your reviewers examine the documents fully including hidden rows, columns, headers, footers, and track changes. This information may be exposed in an image production so you must be sure that it is reviewed for privilege. A TIFF/PDF production from native documents may take longer to perform if there are conversion issues, or a high percentage of large spreadsheet files.

Many vendors are now offering TIFF-on-demand service which generates a TIFF/PDF image as soon as the user requests it. This process can greatly speed up the production process as well as instantly provide an image for redaction. Some vendors also generate image files during the initial processing and offer access to both the native and the image within their platform.

The native versus TIFF/PDF decision may be driven by the requirements of your production. If the requesting party has asked you to produce in a native format, it may not be a wise choice to convert

everything to TIFF/PDF first, only to have to revert back to the native format for production purposes. On the other hand, you might have more control over your production if your images are in a uniform converted format.

The review platform of choice should provide access to the metadata contained in the documents. This is the case whether you are doing a native or TIFF/PDF–based review. Depending on the nature of the case and the issues at hand, the metadata may be extremely important. Consider a situation where there is an allegation that an e-mail has been altered or falsified. Analysis of the metadata for that e-mail will verify where and when the message was sent, where and when it was received, and the size of the message.

Metadata is typically described as data about data. There are three sources of metadata. Most often we think of it as the operating system data that appears in Windows Explorer when you view a file list (title of document, date created, date modified, size, folder name, etc.) and the "Properties" of the document (original author, page count, template used to create, date printed, etc.). E-mail metadata contains even more information regarding the creation, forwarding information, delivery path, and receipt of the email.

Metadata is also the data found in the body of the document such as comments inserted by the author or document deletions or revisions. This type of metadata is viewable in a native document with just a few mouse clicks. Depending on the review platform being used and whether you are viewing native documents, html-rendered documents or TIFF/PDF files will impact your ability to access and review this information.

A review platform should not only accommodate the display of this data for review, it must also allow for searching of the data in conjunction with as well as separate from the text of the actual document. The system should also allow sorting by these fields for ease of organization and review.

Another issue to consider regarding metadata is the ability of the vendor's platform to "normalize" the metadata fields for ease of searching. A single document collection may have Microsoft Word documents, Microsoft Excel, Adobe PDF, Microsoft Powerpoints, RTFs or plain text files as well as e-mail. Each of these software applications contains metadata, but the naming conventions used for their individual metadata fields are not standardized.

To make things even more complex, different versions of the same application may also use a different naming convention. This may result in metadata fields with labels such as: creation date, created data,

created on, and create date. Intuitively, we all know that these field names mean the same thing, but computers, as smart as they may be, are not that intuitive.

It is critical that the vendor's platform or conversion process have the ability to normalize these field names and offer one aggregated date field for searching and sorting purposes. It is also imperative that the vendor retain the original naming convention so that when the data is produced, the original name can be used in the load file or other accompanying documentation.

Comments and revisions made to documents can be incriminating or exonerating, so ignoring them can be potentially damaging. Not only must be reviewed for responsiveness, but also for privilege. The review platform must allow this data to be easily exposed to the reviewers, either in a native application or in the accompanying data load file.

The preceding excerpt is reprinted with permission of edrm.net.

Assessing Production

In *Zubulake v. UBS Warburg LLC* [21], an employment discrimination case, almost two years after the plaintiff first requested e-mail, after a series of discovery disputes spawning three reported decisions, and after the defendant repeatedly claimed that it had produced all responsive e-mail, defendant discovered additional, relevant e-mail and admitted that other e-mail had been destroyed. In *Thompson v. United States HUD* [22], a suit brought by city housing residents against city and federal housing authorities, the defendants produced 80,000 responsive e-mails on the eve of trial, after claiming that no responsive e-mails existed and/or that all had been produced. The list of reported cases with similar fact patterns—belated and incomplete production of discoverable e-mail—goes on and on.

It can almost be presumed that the first response to a request for e-mail will not be complete: an employee instructed to retrieve certain e-mail simply does not know that deleted messages are in backup files. An e-mail that cannot be located on the sender's computer may be retrievable from a computer to which that e-mail was forwarded, or found buried in a chain e-mail discussion. The responding party's IT personnel may not yet be in the loop to prevent backup files from being overwritten.

Not all of these problems can be solved by the requesting party. Nonetheless, the requesting party can and should carefully assess the production process

and the information produced in order to maximize the amount of information adduced, and set the stage for a motion for sanctions, if necessary.

First, through interrogatories and/or a deposition of a corporate designee, the requesting party should elicit a description of what, when, and how electronic storage media were searched for potentially discoverable information. Second, fact witnesses should be examined regarding their pattern and practice of using and storing e-mail. For example, in a wrongful termination suit in which the employer alleges that the plaintiff was terminated because of a disciplinary infraction, human resources personnel might be deposed regarding reporting practices. If reports were regularly made to management via e-mail (which would not be unlikely these days), e-mail regarding the plaintiff's alleged infraction should have been produced. Many e-mail users copy or forward important e-mails from an office to a home computer or BlackBerry. This topic should be explored in deposing key fact witnesses. If e-mail is not produced from the office computer system, serve supplemental requests directed at these other media.

E-mail that is produced should be compared to other documents in counsel's possession. For example, the client's e-mail might contain a chain of messages, one of which should, but did not, appear in the documents produced. Of course, the information in that e-mail has already been uncovered. But the failure to produce that one e-mail portends a more significant problem. It is of course possible to miss one responsive e-mail, just as one can miss one page of paper from among a stack. But given the way electronic data is stored and searched, it is more likely that one entire storage medium, rather than the one e-mail, was missed, or not searched for responsive information.

Perhaps the most effective tool for assessing e-mail production is just common sense. People write lots of e-mail messages about what they think and see, and what they are going to do. If no e-mail is produced from a witness whom you know has personal knowledge of relevant facts, you probably have a problem with that production.

Endnotes

[1] *E.g.,* Treppel v. Biovail Corp., 223 F.R.D. 363, 374 (S.D.N.Y. 2006). *But see* Zakre v. Norddeutsche Landesbank Girozentrale, 2004 U.S.Dist. LEXIS 6026 (S.D.N.Y. 2004), in which the court approved the production of thousands of e-mails on CDs that the defendant had searched for privileged, but not for responsive documents, because the information was in searchable format and in as close a form as possible to how the e-mails were maintained in the ordinary course of business.

[2] Reviewing ESI for production at any level of volume or complexity requires some type of software or document management services support, if only the availability of an application to open and view the ESI and print or image responsive ESI. For a production of any

significant size, discovery-specific support will be required, and all practitioners should consider the advisability of obtaining specialized e-discovery services.

[3] Reprinted with permission from http://edrm.net, Socha Consultants, LLC, and Gelbmann & Associates, copyright edrm.net (2006).

[4] http://www.edrm.net/wiki/index.php/Main_Page.

[5] Chapters 11 and 14, respectively, address the topics of inadvertent disclosure of privileged information and authentication.

[6] *See* Treppel v. Biovail, n. 1, *supra.*

[7] *Id.; see also* General Elec. Capital Corp. v. Lear Corp., 215 F.R.D. 637, 640 (D. Kan. 2003).

[8] 219 F.R.D. 649 (D. Kan. 2004).

[9] *Id.* at 657. Plaintiff proposed, as an alternative to its retrieving ESI, that it would make its computers available to the defendant for inspection and copying. The court agreed with the defendant that this alternative would inappropriately shift the costs of production to the requesting party.

[10] *Treppel v. Biovail*, 223 F.R.D. at 374; General Elec. Capital Corp. v. Lear Corp., 215 F.R.D. at 640.

[11] *See* In re Ford Motor Co., 345 F.3d 1315, 1316–17 (11th Cir. 2003); McPeek v. Ashcroft, 202 F.R.D. 31, 35 (D. D.C. 2001); *see also* The Sedona Conference Working Group Series, "The Sedona Principles: Best Practices Recommendations for Addressing Electronic Document Production," Principle 11 (2005), http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf. ("A responding party may satisfy its good-faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of select criteria, to identify data most likely to contain responsive information.")

[12] 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. 2006).

[13] *Id.* at *14.

[14] *Id.* at *16, *17.

[15] The court relied on then-pending Fed. R. Civ. P. 26(b)(2)(B) in making this distinction.

[16] *Id.* at *21. The court found counsel's failure in this regard to constitute "gross negligence," and the defendants' failures to be at least negligent. However, the court declined to impose an adverse inference instruction as a sanction because the responsive information had been produced, if belatedly. It did, however, impose costs. *Id.* at *28.

[17] 2006 U.S. Dist. LEXIS 46372 (D. D.C. 2006).

[18] *Id.* at *14.

[19] *Id. See also* Williams v. Mass. Mutual Life Ins. Co., 226 F.R.D. 144 (D. Mass. 2005) (court denied a motion to compel production of computers for imaging where defendant had made a detailed search for responsive ESI and "sworn to its accuracy.")

[20] *See* n. 3, *supra*, and accompanying text.

[21] 229 F.R.D. 422 (S.D.N.Y. 2004) (Zubulake V).

[22] 219 F.R.D. 93 (D. Md. 2003).

9

Discovery from Third Parties

Introduction

Much has been written here and elsewhere about the extraordinary volume and dispersal of ESI, facts which underscore the advisability of considering discovery of ESI from third parties. Fed. R. Civ. P. 45 has been amended specifically to authorize the issuance of a subpoena for the production of ESI, but also provides limitations in addition to the avoidance of undue burden or expense on the duty to respond. In this chapter we describe these additional limitations and analyze undue burden or expense in the context of ESI. We explore specific issues that arise in the discovery of ESI from Internet service providers (ISPs)—a rich trove of potentially discoverable information—and the potential hurdle to the discovery of information published on the Internet posed by the Stored Communications Act, 18 U.S.C. § 2702(a)(1).

Fed. R. Civ. P. 45

The amendments to the rule "keep Rule 45 in line with the other amendments addressing electronically stored information" [1]. Thus, Rule 45(a)(1)(C) provides that a subpoena shall "command each person to whom it is directed to attend and give testimony or to produce and permit inspection, copying, testing or sampling of designated books, documents, electronically stored information, or tangible things in the possession, custody or control of that person …." This section of the rule further provides that a subpoena "may specify the form or forms in which electronically stored information is to be produced" [2].

A person subject to subpoena may object to producing ESI in the form or forms requested [3]. If the court, upon motion to compel by the requesting party, orders production, such order "shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection, copying, testing, or sampling commanded" [4]. If the subpoena does not specify the form for producing ESI, "a person responding to a subpoena must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable" [5].

Rule 45(d)(D) provides that a person responding to a subpoena "need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost." The court may order discovery from such sources if the requesting party shows good cause [6].

Undue Burden

Rule 45 provides that "on timely motion, the court by which a subpoena was issued shall quash or modify the subpoena if it … subjects a person to undue burden" [7]. Of course, "if the sought-after documents are not relevant, nor calculated to lead to the discovery of admissible evidence, then any burden whatsoever imposed would be by definition undue" [8]. Assuming that the requesting party has adequately demonstrated that information sought pursuant to subpoena is otherwise discoverable, what constitutes "undue burden" on a nonparty recipient of a subpoena for ESI?

One might argue that, unless the information sought is not reasonably accessible because of undue burden or cost, it is presumptively discoverable [9], unless another basis exists for excusing production, such as that the subpoena is overbroad [10]. On the other hand, third parties are accorded particular protection from burdensome production. "Underlying the protections of Rule 45 is the recognition that 'the word non-party' serves as a constant reminder of the reasons for the limitations that characterize third-party discovery'" [11]. Thus, in assessing whether the burden on a third party subject to a subpoena is undue, the court assesses whether the subpoena is "reasonable" [12], which assessment includes a balancing of factors including the relevance of the discovery sought, the requesting party's need, and the potential hardship to the party subject to the subpoena [13].

Nonetheless, the extent to which ESI sought pursuant to subpoena is accessible should be a significant factor in the balance. For example, in *United States ex rel Tyson v. Amerigroup Ill., Inc.* [14], a *qui tam* action alleging that false claims were made to an Illinois state agency, defendants subpoenaed a third party for the production of e-mail from three specified employees. The third party objected that producing the e-mail would constitute an undue burden

because the e-mail resided on backup tapes that would have to be located and restored. The court agreed, noting that "in the hierarchy of accessibility, it is clear that electronic data stored on media such as the backup tapes involved here is near the bottom" [15]. The court quashed the subpoena even though defendants offered to pay the costs to be incurred in retrieving the e-mail because of the burden on the third party that could not be shifted, including the use of equipment and internal manpower [16].

When the information sought via subpoena is readily searchable the calculus is different. In *Crandall v. City & County of Denver* [17], a suit brought pursuant to the Resource Conservation Recovery Act (RCRA), 41 U.S.C. §§ 6901–6992, alleging injuries due to exposure to harmful chemicals or other adverse environmental conditions at Denver International Airport, plaintiffs subpoenaed two nonparties—United Air Lines, Inc. (United) and Gallagher Bassett Services, Inc. (GBS)—seeking documents relating to incidents in which United employees complained of exposure to fumes. The nonparties moved to quash on various grounds, including that the production would be unduly burdensome. United and GBS claimed that over 66,000 worker's compensation claim files existed that would have to be physically searched. The court required the parties to explore an alternative to a physical search [18]:

> … the Court does not believe that the issue of whether GBS can electronically identify only files that concern complaints of fumes, and whether those files can be further electronically limited to incidents involving the substances in which the Plaintiffs are interested, has been sufficiently clarified. Plaintiffs should be aware that the Court will not require GBS or United to physically review 66,000 files to determine whether they are related to fumes. If GBS, however, can use some search commands that would reduce the number of potentially responsive documents, the Court would permit production of a significantly smaller universe of documents.
>
> Therefore, before any documents must actually be produced, the Court will direct United and/or GBS to provide a good faith, educated statement of whether there exists the technological capability of searching the records for a smaller subset of potentially responsive documents (and, if not, a declaration under oath to that effect should be provided).

The information sought in *Gonzales v. Google, Inc.* [19], lay between readily searchable data and data on backup tapes on the accessible spectrum. In this case, a miscellaneous action filed to subpoena evidence in the case of *ACLU v. Gonzales* [20], the Government subpoenaed Google to produce a sample of URLs from Google's search index and a sample of search queries (text) [21]. Google objected, in part because production would impose an undue burden [22]. Google argued that it did not maintain search query or URL information in the ordinary course of business in the format requested by the government,

and that it would have to create new code to format and extract query and URL data from many computer banks. Noting that Google had not, however, represented that it would be unable to extract the information from its existing systems, and that the government had agreed to compensate Google for the costs of production, the court held that the "technical burden" did not excuse Google from complying with the subpoena [23]. However, the court quashed the subpoena insofar as it required production of the search queries, in part because producing that information would have imposed a different type of burden on Google—the loss of user trust in using Google anonymously and privately—and in part because of the court's concerns, apart from the potential loss of goodwill to Google, regarding users' privacy [24].

ISPs

The quantity and quality of information in the possession of ISPs makes those entities a potentially fruitful target for third-party discovery. But in addition to the usual roadblocks of establishing relevance and showing, if objection is made, that responding to the subpoena does not impose an undue burden or otherwise run afoul of Rule 45, other issues may rear their heads in issuing subpoenas to ISPs.

First Amendment Issues

Suits for defamation, breach of contract, misappropriation of trade secrets, and other causes of action can arise from information posted anonymously on the Internet. The anonymous poster can be identified by obtaining information from the ISP. The ISP may require message board users to provide identifying information before posting information, in which case the complaining party can unearth the identity of the allegedly offending party by obtaining that information from the ISP. Alternatively, the IP address of a purely anonymous poster or blogger can be obtained from the Web site or blog operator, and that person's identity then obtained from the ISP, which has assigned the IP address to a named person.

First Amendment protections extend, however, to speech on the Internet [25]. First Amendment rights are protected even when exercised anonymously [26]. At the same time, of course, plaintiffs have the right to assert recognizable claims based on the speech of anonymous persons. But because of First Amendment considerations, these plaintiffs must make a strong showing that their claims are well-founded before they can unmask the identities of the putative defendants by obtaining discovery from third parties.

For example, in *Dendrite Int'l v. Doe No. 3* [27], in the New Jersey state courts, Dendrite brought suit against several John Doe defendants alleging defamation, breach of contract, and other claims arising from statements posted anonymously on a Yahoo! message board. Dendrite sought an order to show cause why it should not be granted leave to conduct limited discovery for the purpose of ascertaining the identities of John Doe defendants Nos. 1 through 4 [28]. The trial court denied the motion to compel discovery as to John Doe No. 3 on the grounds that Dendrite had not made a *prima facie* case of defamation against that defendant. On appeal, Dendrite argued that the court erred in applying "in effect" a summary judgment standard, that its claims would survive a motion to dismiss and that, therefore, it was entitled to discovery.

The court of appeals affirmed [29]:

> We offer the following guidelines to trial courts when faced with an application by a plaintiff for expedited discovery seeking an order compelling an ISP to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations or businesses. The trial court must consider and decide those applications by striking a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants.
>
> We hold that when such an application is made, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board.
>
> The court shall also require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech.
>
> The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. In addition to establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to R. 4:6-2(f), the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.

In *John Doe No. 1 v. Cahill* [30], a Delaware case, Defendant-appellant John Doe anonymously posted information on an Internet blog regarding Patrick Cahill's performance as a councilman. Cahill and his wife filed suit, alleging that the information was defamatory. The Cahills obtained leave of the trial court to conduct a preservice deposition of the owner of the Internet blog, obtained the IP addresses associated with the blog postings, and obtained a court order requiring Comcast, the ISP, to disclose the identity of the subscriber assigned the relevant IP address. As required by 47 U.S.C. 551(c)(2) (regarding protection of cable subscriber privacy), the ISP notified Doe of the order, and Doe subsequently filed a motion for a protective order. The trial court denied the motion on the grounds that the Cahills had shown a "good faith" basis for bringing the underlying claim.

The Supreme Court of Delaware rejected the good-faith standard because of the First Amendment protections to which anonymous speech on the Internet was entitled. "We are concerned," the court stated, "that setting the standard too low will chill potential posters from exercising their First Amendment right to speak anonymously" [31]. In light of that concern, the court held that before a defamation plaintiff can obtain the identity of an anonymous defendant through the compulsory discovery process, he must support his defamation claim with facts sufficient to defeat a summary judgment motion [32]. In regard to the case at bar, the court found that no reasonable person could conclude that Doe's statements were other than opinion: the guidelines on the blog specifically stated that the forum was devoted to opinions. Accordingly, it reversed and remanded with instructions to dismiss [33].

The court in the United States District of Arizona also employed a summary judgment standard in *Best Western Int'l v. Doe* [34], in which plaintiff brought suit alleging, *inter alia*, defamation and trademark infringement against persons who had anonymously posted information on an Internet site. The plaintiff sought expedited, ex parte discovery in the form of subpoenas to Internet service providers to obtain information to identify the defendants. The court held that because the type of speech at issue was "purely expressive," it was entitled to substantial First Amendment protections and, therefore, that plaintiff would be required to meet the higher standard before obtaining discovery to uncover the speaker's identity [35]. The court denied plaintiff's motion for discovery because its complaint did not identify a single false statement allegedly made by the John Doe Defendants or describe a single instance where its mark was improperly used. The court noted that if plaintiff intended to renew its motion for discovery, it should give notice to the John Doe defendants over the Internet site and afford them an opportunity to oppose the discovery. "When First Amendment interests are at stake, we disfavor ex parte discovery requests that afford the Plaintiff the important form of relief that comes from unmasking an anonymous defendant" [36].

A different type of speech was at issue in *Sony Music Entm't, Inc. v. Does 1 – 40* [37]. Plaintiff in this case sued 40 unknown defendants for alleged copyright infringement in downloading and distributing songs using a peer to peer network and sought to identify the defendants by serving subpoenas on an Internet service provider. Four defendants moved to quash on the grounds that, *inter alia*, the subpoena violated their First Amendment rights.

The court agreed with the defendants that peer-to-peer file sharing constituted protected expression, but found that such expression was not entitled to the broadest protection as would be political speech [38]. Drawing upon a number of other decisions addressing the appropriate analysis for weighing First Amendment protections against copyright property rights, the court considered the following factors as relevant to consider: (1) whether the plaintiff had made a concrete showing of a *prima facie* claim of actionable harm, (2) the specificity of the discovery request, (3) the absence of alternative means to obtain the subpoenaed information, (4) a central need for the subpoenaed information to advance the claim, and (5) the party's expectation of privacy. The court found all these factors weighed in favor of the plaintiff's request for discovery and denied the motion to quash [39].

The Stored Communications Act

Title II of the Electronic Communication Privacy Act [the Stored Communications Act, (SCA)] provides a cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided … and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. §§ 2701(a)(1), 2707(a). *Electronic storage* means either "temporary, intermediate storage … incidental to … electronic transmission," or "storage … for purposes of backup protection." *Id.* § 2510(17). The act exempts, *inter alia*, conduct "authorized … by the person or entity providing a wire or electronic communications service," *Id.* § 2701(c)(1), or "by a user of that service with respect to a communication of or intended for that user," *Id.* § 2701(c)(2). Under certain circumstances, disclosure of communications stored on an ISP's service, pursuant to a subpoena or purported subpoena, may violate the SCA.

In *Theofel v. Farey-Jones* [40], plaintiffs, officers of Integrated Capital Associates, Inc. (ICA), were involved in litigation against defendant Farey-Jones in New York. In the course of discovery in that matter, Farey-Jones, through counsel, issued a subpoena to ICA's ISP, NetGate. The subpoena ordered the production of "all copies of e-mails sent or received by anyone" at ICA, with no limitation as to time or scope. NetGate, which was apparently not represented by counsel, objected to producing such a volume of e-mail but produced a sample it posted on a Web site. Defendant Farey-Jones and its counsel read the e-mails, many of which were unrelated to the litigation, privileged, and/or

personal. When plaintiffs found out what had happened, they moved the court in New York to quash the subpoena and issue sanctions, which the court did, finding that the subpoena was "patently unlawful" and that it "transparently and egregiously" violated the federal rules. Plaintiffs then filed this action claiming defendants violated the Stored Communications Act, the Wiretap Act [41], and the Computer Fraud and Abuse Act [42], as well as various state laws. The district court held that none of the federal statutes applied, dismissed the claims without leave to amend, and plaintiffs appealed.

The Ninth Circuit reversed on the SCA claim. The district court had found that NetGate authorized defendants' access. The Court of Appeals, looking to the law regarding trespass, found that NetGate's consent had been vitiated by deceit. "NetGate disclosed the sample in response to defendants' purported subpoena. Unbeknownst to NetGate, that subpoena was invalid. This mistake went to the essential nature of the invasion of privacy. The subpoena's falsity transformed the access from a bona fide state-sanctioned inspection into private snooping" [43].

Defendants also argued that the e-mail was not "stored" because it had already been delivered to the recipient, relying on Section 2701(a)(1)(A), which defines *electronic storage* as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." But the court found that the e-mail at issue fit "comfortably" into subsection (B), which includes "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The court noted that other courts had reached a contrary conclusion, holding that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage" [44]. But the court rejected that view as contrary to the plain language of the act. "By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission" [45].

The Digital Millennium Copyright Act (DMCA)

17 U.S.C. § 512(h)(1) provides that a copyright owner may "request the clerk of any United States district court to issue a subpoena to [an ISP] for identification of an alleged infringer" when no action is pending in a court. However, recent decisions interpreting the DMCA have severely restricted the applicability of this provision. In *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services* [46], the court held that a subpoena may be issued pursuant to § 512(h) only to an ISP engaged in storing on its servers material alleged to be infringing, and not if that ISP is only acting as a conduit for the transmission of the material. The Eighth Circuit [47] and other courts have agreed with this interpretation [48].

Internet Publishers and the SCA

O'Grady v. Superior Court [49] arose from an action brought by Apple Computer in California state court alleging that persons unknown wrongfully published on the Internet Apple's secret plans to release a new product. Apple sought and obtained subpoenas to the publishers of the Web sites where the information appeared and to the e-mail service provider for one of the publishers. One of the publishers moved for a protective order, which the trial court denied. The publisher sought a writ of mandamus, which the appellate court granted, directing the trial court to set aside its initial order and enter a protective order.

In regard to the subpoena to the e-mail provider, the court held that it was unenforceable pursuant to the SCA, 18 U.S.C. § 2702(a)(1). Apple contended that this prohibition of the act did not apply because it was only seeking the identities of subscribers to the e-mail service, which the act specifically authorizes in § 2703(c)(1) [50]. But the court disagreed, because in the subpoena Apple had requested not only "documents relating to the identity" of persons who had allegedly supplied secret information to the publisher but also "all communications from or to any disclosing person" [51]. Further, the court noted that the effect of any response to the subpoena would be to disclose the contents of communications by confirming that the persons identified had sent or received the offending communications [52].

Endnotes

[1] Advisory Committee Introduction to Rule 45, http://www.uscourts.gov/rules/Reports/ST09-2005.pdf, p. 89.

[2] See Chapter 4, "Requesting a Form or Forms," for factors to consider in specifying the form in which ESI is to be produced pursuant to a subpoena.

[3] Fed. R. Civ. P. 45(c)(2)(B).

[4] *Id.* For reasons why an order to compel production in the specified form may, or may not, be justified, see Chapter 4, "Object to Specified Form of Production."

[5] Fed. R. Civ. P. 45(d)(B). For a discussion of the "default options," see Chapter 4, "Production–Default Options."

[6] Fed. R. Civ. P. 45(d)(D).

[7] Fed. R. Civ. P. 45(c)(3)(A)(iv). Other grounds justifying an order to quash or modify a subpoena include a failure to allow reasonable time for compliance and that the subpoena requires disclosure of a trade secret or other confidential information.

[8] Compaq Computer Corp. v. Packard Bell Elecs., Inc., 163 F.R.D. 329, 335-36 (N.D. Cal. 1995).

[9] See keynote speech, ARMA 2006 Conference and Expo, The Honorable Shira A. Scheindlin, p. 4, so describing "reasonably accessible" ESI in the context of Fed. R. Civ. P. 26(b)(2)(B), *available at* http://www.arma.org//podcast/Speech.pdf (last visited March 20, 2007).

[10] *See* Quinby v. WestLB AG, 2006 U.S. Dist. LEXIS 1178 (S.D.N.Y. 2006), in which the court quashed subpoenas to plaintiff's e-mail service providers seeking "all e-mail" to or from the plaintiff during a specific period of time, except for communications with counsel, because the responses would yield a "vast amount" of irrelevant material including spam e-mail, Internet purchase orders, etc., and the subpoenas were therefore overbroad.

[11] Gonzalez v. Google, Inc., 234 F.R.D. 674, 680 (N.D. Cal. 2006), *citing* Dart Industries Co. v. Westwood Chemical Co., 649 F.2d 646, 649 (9th Cir. 1980).

[12] See 9A Charles Alan Wright & Arthur R. Miller, FEDERAL PRACTICE AND PROCEDURE, § 2463 (2nd ed., 1995).

[13] *E.g.,* Gonzalez v. Google, Inc., 234 F.R.D. at 680 (citations omitted); Positive Black Talk, Inc. v. Cash Money Records, Inc., 394 F.3d 357, 377 (5th Cir. 2004).

[14] 2005 U.S. Dist. LEXIS 24929 (N.D. Ill. 2005).

[15] *Id.* at *13, *citing* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

[16] *Id.* at *13. Under a similar set of facts presented after the amendments to the rules, the subpoena would presumably have been quashed pursuant to Fed. R. Civ. P. 45(d)(1)(D).

[17] 2006 U.S. Dist. Lexis 35051 (D. Colo. 2006).

[18] *Id.* at *8. The nonparties were also ordered to provide information regarding the number of potentially responsive documents and the effort it would take to review and redact, as necessary, which the court would consider should the parties not agree on the scope of production. Thus, information sought in a subpoena might be readily searchable, yet its production would still constitute an undue burden.

[19] 234 F.R.D. 674 (N.D. Cal. 2006).

[20] Civil Action No. 98-CV-5501, pending in the Eastern District of Pennsylvania, on remand from Ashcroft v. ACLU, 542 U.S. 656 (2004).

[21] The Government had initially sought a massive number of URLs and queries, but had significantly scaled down the request by the time the court rendered its opinion.

[22] Google also argued, *inter alia*, that the government had not demonstrated relevance, that the requests were duplicative of information already obtained by the government, and that the information constituted confidential trade secrets.

[23] 234 F.R.D. at 683.

[24] *Id.* at 683-84, 687. The court also imposed conditions on the production of the URLs, including subjecting the information obtained to a protective order.

[25] Reno v. ACLA, 521 U.S. 844, 885 (1997).

[26] Buckley v. Am. Law Found., 525 U.S. 182, 197–99 (1999).

[27] 342 N.J. Super. 1345, 775 A.2d 756 (2001).

[28] The order which issued was posted on the Yahoo! message board.

[29] 342 N.J. Super. at 141, 775 A.2d at 760.

[30] 884 A.2d 451 (Del. 2005).

[31] *Id.* at 456.

[32] *Id.* The court noted that it was thereby agreeing with and following the holding of *Dendrite*, though it did not adopt the entirety of *Dendrite*'s preconditions to authorizing the discovery that were sought.

[33] *Id.* at 467–68.

[34] 2006 U.S. Dist. LEXIS 56014 (D. Ariz. 2006).

[35] *Id.* at *11.

[36] *Id.* at *16 (citations omitted).

[37] 326 F.Supp. 2d 556 (S.D.N.Y. 2004).

[38] *Id.* at 564.

[39] *Id.* at 565–566.

[40] 359 F.3d 1066 (9th Cir.), *cert. denied* 543 U.S. 813 (2004).

[41] The court affirmed the dismissal of the Wiretap Act claim because the e-mail was in "storage" and therefore was not "intercepted," *citing* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir.), *cert. denied* 537 U.S. 1193 (2003) as dispositive on this issue. *But see* United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).

[42] The district court had dismissed the Computer Fraud and Abuse Act (CFAA) claim on the grounds that the CFAA did not provide a remedy for unauthorized access of a third-party's computer. The Court of Appeals disagreed. The statute authorizes "any person" suffering damage or loss to seek relief, which would include individuals other than the computer's owner. Because plaintiffs had not, however, alleged specific damage as required by this act, the dismissal was appropriate but plaintiffs should have been granted leave to amend.

[43] 359 F.3d at 1074.

[44] *See* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635–36 (E.D. Pa. 2001).

[45] 359 F.3d at 1076. The United States, as *amicus curiae*, disputed the court's interpretation of the act.

[46] 351 F.3d 1229 (D.C. Cir.), *cert. denied* 543 U.S. 924 (2004). A number of other issues were raised in this suit, including Verizon's contention that § 512(h) violated the First Amendment (the district court had questioned Verizon's standing to raise this argument), which were not reached by the court in light of its holding.

[47] In re Charter Communs. Inc. Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir.), *reh'g denied by, reh'g, en banc, denied by* Recording Indus. Ass'n of Am. v. Charter Communs., Inc., 2005 U.S.A., LEXIS 5599 (8th Cir. 2005).

[48] *See* Recording Indus. Ass'n of Am. v. Univ. of N.C. at Chapel Hill, 367 F.Supp. 2d 945 (M.D. N.C. 2005).

[49] 139 Cal. App. 4th 1423 (Cal. Ct. App. 2006).

[50] Apple argued that the SCA did not render the subpoena unenforceable for a number of other reasons. It contended, for example, that the SCA should be interpreted as providing an "implied exception" for civil discovery. None of these arguments convinced the court.

[51] *Id.* at 1447–1448.

[52] *Id.* at 1448. In regard to the subpoenas to the publishers, the court held that insofar as they sought unpublished information they would be unenforceable through contempt proceedings in light of the California's reporter's shield, and discovery of the publishers' sources would also be barred by the conditional constitutional privilege against compulsory disclosure of confidential sources.

Part IV
ESI and the Attorney-Client Relationship

10

Duty to Preserve

Introduction

> *A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter* [1].

The duty to preserve ESI does not differ, in many regards, from that duty as interpreted in regard to paper documents [2]. That is, the law pre-existing the advent of ESI comfortably answers the questions of who has the duty and when it attaches [3]. "The preservation duty runs first to counsel, who has 'a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction'" [4]. The client is also responsible for preserving evidence, and for communicating the requirement to do so to its employees [5]. The duty arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation [6]. At this point a litigation hold must be put in place.

Other aspects of the duty to preserve are, however, more problematic because of characteristics of ESI that differ from paper documents. ESI can be purged or destroyed easily—with a key stroke—or automatically by computer or software systems. During its life cycle ESI may change in form and be moved from one storage medium to another. Like "disappearing ink," ESI is created and appears on a computer screen, but may never be stored for any period of time for business purposes. These facts lead to the issues that are explored in this chapter. First, what steps must be taken to prevent ESI destruction? Second, when is reformatting or moving ESI from one storage medium to another

appropriate and when is it not? Third, must ephemeral ESI ever be "captured" and stored for litigation purposes even though it is not for business purposes?

Preventing Destruction

The duty to preserve of course forbids the intentional destruction of relevant ESI, just as it does the intentional destruction of paper documents [7]. "Unintentional" destruction by computer or software systems may also violate the duty to preserve. That is, the courts are generally in agreement that "… in the world of electronic data, the preservation obligation is not limited simply to avoiding affirmative acts of destruction" [8].

Absent exceptional circumstances, a party may not be sanctioned under the Federal Rules of Civil Procedure for failing to provide ESI lost "as a result of the routine, good-faith operation of an electronic information system" [9]. But good faith "may involve a party's intervention to modify or suspend certain features of that operation to prevent the loss of information, if that information is subject to a preservation obligation" [10].

Much of the controversy in regard to ESI destruction has concerned backup tapes because they are routinely overwritten or recycled. On the one hand, the duty to preserve does not require a party to suspend all routine destruction of backup tapes [11]. But the automatic erasure of potentially relevant ESI on backup tapes would violate the duty to preserve [12]. In general, though not all courts define the duty to preserve in regard to backup tapes quite the same [13], tapes that can be identified as storing the documents of "key players" to the litigation should be preserved if the information contained on those tapes is not available elsewhere [14].

Just ask the executive at Morgan Stanley responsible for the e-mail backup tapes involved in the Coleman litigation. According to one account, when Morgan Stanley personnel were interviewed about how many backup tapes existed, at least six different answers (ranging from six to hundreds), were provided by six different employees, including the CFO [15]. Counsel had already represented to the court that the cost of retrieving the e-mail was too great, and in any event, no backup tapes existed for e-mails in 1997 and 1998. While the court-imposed sanctions escalated over time, ultimately the court ordered what was tantamount to a directed verdict in Coleman's favor. The jury awarded Coleman $640 million in compensatory damages and $850 million in punitive damages.

Instead of backup tapes, businesses are increasingly using online backup services to store ESI. Most commercially available online services allow the subscriber full control over its own data as long as the subscriber is paying for the service. Such ESI would be in the subscriber's possession or control and subject

to the preservation obligation. Prudent practice dictates that these contracts contain provisions providing for the suspension of any data destruction by the vendor in the event the subscriber is subjected to a litigation hold.

In the event of contract termination, the vendor is typically authorized to destroy ESI. The contract should specify when that authority can be exercised. In regard to the duty to preserve, the party should ensure that any service contracts do not expire and discoverable data is not destroyed while a litigation hold is in place.

Of course, routine destruction policies may be in place for ESI other than backup data. And even if that data is normally destroyed for legitimate business reasons, good faith requires the party to take steps to preserve discoverable ESI that otherwise would be destroyed. For example, in *Computer Assoc. Int'l, Inc. v. Am. Fundware, Inc.* [16], the defendant software developer maintained a single, updated version of software code and destroyed all other versions to maintain the integrity of the code and prevent loss and unnecessary duplication. When it continued this practice after litigation commenced, the plaintiff sought sanctions for spoliation of evidence. The court held that the destruction of code relevant to the issues in the litigation was inappropriate, even assuming the destruction policy was for bona fide business reasons. Similarly, in *Broccoli v. Echostar* [17], the defendant failed to suspend its ordinary document retention policy pursuant to which e-mail was deleted, without backup, 21 days after it was created, and files in employee hard drives were destroyed 30 days after termination. The court granted plaintiff's motion for sanctions though, as the court noted, "under normal circumstances such a policy might be a risky but arguably defensible business practice …."

Not only is ESI routinely destroyed pursuant to policy or practice, but also through the ordinary use of the data or the operating system used to create and alter the data [18]. Active ESI is typically stored on magnetic discs in a server, desktop, or laptop computer. ESI on magnetic discs is readily overwritten and modified. A modification to the computer's operating system can effectively destroy pre-existing, active ESI. A standard method for preserving active ESI is to create a mirror image of computer hard drives at the time the litigation hold is instituted [19]. The drives of servers, desktops, laptops, and handheld computing devices that are reasonably likely to contain relevant information should be imaged [20]. Copying ESI from hard drives to CDs or DVDs comprises one alternative, but risks omitting data that would be copied in a true imaging. While copying captures only specific active ESI, computer storage imaging creates a complete copy of the contents and structure of a data storage medium, including all data marked as deleted but still found on the medium. Having noted that technical distinction, in some circumstances it is probably sufficient to copy the specific database or set of records likely to contain discoverable ESI. Typically, a server will run more than one application and store more than one

database. Imaging the whole drive may constitute overkill that eventually increases the cost of production and the burden of review.

ESI that constitutes potentially relevant information that must be preserved from destruction could include anything stored in bits and bytes: e-mail and other correspondence, time sheets and databases, voice messages recorded on digital media [21], satellite tracking data [22], data created in a car's electronic data storage units [23], and online data, including information on Web sites and that in Internet-accessible data storage centers. What steps must counsel take to halt destruction in the wide universe of potentially discoverable ESI?

In *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (*Zubulake V*), Judge Scheindlin described counsel's obligations:

> Once a "litigation hold" is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed "on hold" … To do this, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation, in order to understand how they stored information. In this case, for example, some UBS employees created separate computer files pertaining to Zubulake, while others printed out relevant e-mails and retained them in hard copy only. Unless counsel interviews each employee, it is impossible to determine whether all potential sources of information have been inspected.

Suspending automatic or routine ESI destruction procedures, preventing the inadvertent destruction or loss of active data, and prohibiting the intentional destruction of relevant ESI require counsel to thoroughly communicate the nature and extent of the litigation hold to the client. Advising persons likely to have knowledge of relevant information may not accomplish the objective; the network administrator should also be aware of a litigation hold [24], as well as appropriate vendors and consultants. Employees and others should be informed of the kinds of ESI that are relevant [25], and how that ESI is to be preserved.

Preserving Form

Preventing the destruction of ESI necessarily follows from the duty to preserve ESI. To what extent the duty requires a party to maintain ESI in a particular form is not as clear.

The issue is important because the conversion of ESI from one form to another has significant consequences for the discovery process. As the data

becomes less accessible, the cost to produce it in discovery increases, thereby increasing the probability that the requesting party may have to bear all or part of the costs. If the data is not reasonably accessible a party responding to discovery need not search or produce it. Instead, it need only "identify by category or type, the sources containing potentially responsive information that it is neither searching nor producing" [26].

At the one extreme, the intentional conversion of ESI from accessible to inaccessible form would presumptively violate the duty to preserve. During the comment period on proposed Rule 26(b)(2), concerns were expressed that corporations would make information inaccessible in order to frustrate discovery [27]. In light of those concerns, the committee clarified that "[a] party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence" [28]. In regard to conversion of ESI, the committee stated: "A party that makes information 'inaccessible' because it is likely to be discoverable in litigation is subject to sanctions now and would still be subject to sanctions under the proposed rule changes" [29]. One might argue as to what exactly *inaccessible* means, but at least the duty is fairly clear: one has not appropriately preserved ESI if it has been converted to an inaccessible form after the duty to preserve has attached.

The routine or inadvertent conversion of ESI to an inaccessible form is not so clearly in violation of the duty to preserve. In *Quinby v. WestLB AG* [30], the court declined to find such a violation. The ESI at issue in that case was data in the possession of the defendant's consultant. The data had been stored in an accessible form and converted to a backup form after certain projects the consultant had undertaken ended, a date after the litigation arose. The plaintiff argued that the defendant violated its duty to preserve evidence by converting the data from accessible to inaccessible form. The court summarily rejected that argument: "Plaintiff fails to cite, and I am unaware of any case, that states that the duty to preserve electronic data includes a duty to keep the data in an accessible form." But in *Treppel v. Biovail Corp.* [31], without specifically deciding the issue, the court noted with approval that hard drives had been preserved through mirror imaging to "ensure that it was not destroyed or downgraded from an accessible to an inaccessible format."

A lesser offense would be converting relevant ESI to a less readily useable, but not inaccessible form: converting searchable Adobe Acrobat (PDF) files into nonsearchable Tagged Image File Format (TIFF) image files, for example. By reference to the rules regarding production of ESI—and those rules are certainly relevant to what must be preserved—this type of conversion, if a "significant downgrade," even if unintentional, might not pass muster. Fed. R. Civ. P. 34(b)(ii) provides that a party may produce ESI "in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably useable" if the

requesting party has not specified the requested form of production. The Committee Note states:

> … the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly downgrades this feature.

It remains to be seen whether, as a general rule, the courts will decide that the routine or inadvertent downgrading of ESI violates the duty to preserve. It should be noted, however, that the court in *Zubulake V,* without specifically deciding the issue, stated that electronic documents should be preserved "in the state they existed" at the time the duty attaches [32].

Capturing Ephemeral ESI

Must a party preserve ephemeral ESI, the ESI that is created even if it is never stored for any period of time for business purposes?

This question was considered in *Convolve v. Compaq Computer Corp*. [33]. At issue was electronic data comprised of serial iterations of waveforms produced by a particular software program and displayed on an oscilloscope. The production of the waveforms allegedly infringed on the plaintiff's software patent. The engineer who produced the waveforms testified that he kept no record of the serial iterations. Convolve argued that Seagate, the engineer's employer, wrongfully failed to preserve the data either by printing the screen each time a different wave form was produced or by saving the data to a disk.

The court rejected the argument, in part because the disputed data would be available elsewhere, in the testimony of the engineers or perhaps from documents. But more importantly,

> … the preservation of the wave forms in a tangible state would have required heroic efforts far beyond those consistent with Seagate's regular course of business. To be sure, as part of a litigation hold, a company may be required to cease deleting e-mails, and so disrupt its normal document destruction protocol. But e-mails, at least, normally have some semi-permanent existence. They are transmitted to others, stored in files, and are recoverable as active data until deleted, either deliberately or as a consequence of automatic purging. By contrast, the data at issue here are ephemeral. They

> exist only until the tuning engineer makes the next adjustment, and then the document changes. No business purpose ever dictated that they be retained, even briefly. Therefore, absent the violation of a preservation order, which is not alleged here, no sanctions are warranted.

But what if ephemeral ESI was highly likely to be relevant, was not available from another source, and would not require "heroic efforts" to store? Consider, for example, pharmaceutical scientists working in teams that use instant messaging; the transcript of each session is posted during the session. The transcript could easily be stored, and with minimal expense. But as a matter of company policy, those transcripts might not be stored. An argument could be made that those transcripts, if they contain relevant information, should be stored if a litigation hold is in place.

It is certainly likely that ephemeral ESI, if discoverable, would be relevant to claims and defenses because it is virtually ubiquitous. Any reasonably sophisticated Web site changes constantly. Patient vital signs appear on a computer screen. Payment for a retail purchase is entered on a touch screen menu which disappears after that payment is recorded. Boarding passes are issued from information entered on a touch screen: that information also disappears [34]. At least the topic of capturing ephemeral ESI is one that should be considered in a meet and confer.

Endnotes

[1] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)(Zubulake IV).

[2] This chapter is devoted to the general duty to preserve evidence. A preservation order may be in place requiring additional or different obligations than those discussed here. *See* Chapter 16.

[3] *See* The Sedona Conference Working Group Series, "The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production," principle 5.a. (2005), ("The first inquiry [when does the duty to preserve attach] remains unchanged in the world of electronic data and documents, although the need to recognize when a duty arises may be more important in light of the volatility of certain data."), *available at* www.thesedonaconference.org.

[4] Heng Chan v. Triple 8 Palace, 2005 U.S. Dist. LEXIS 16520, *16 (S.D.N.Y. 2005), *quoting* Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 73 (S.D.N.Y. 1991); National Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 554 (N.D. Cal. 1987).

[5] *Id.*; *see also* Zubulake IV, 220 F.R.D. at 217.

[6] *E.g.,* Fujitsu Ltd. v. United States, 247 F.3d 423, 436 (2d Cir. 2001); Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001), Kronisch v. United States, 150 F.3d 112, 126 (2nd Cir. 1998). As stated by the court in *Kronisch*, the initiating event is "most

commonly" the filing of a complaint. 150 F.3d at 126. However, if the facts show that defendant was "fully aware" that a claim would be filed, the obligation to preserve may arise at that point. *See* Capullupo v. FMC Corp., 126 F.R.D. 545, 550 (D. Minn. 1989).

[7] *See* Inst. for Motivational Living, Inc. v. Doulos Inst. For Strategic Consulting, Inc., 110 Fed. Appx. 283 (3rd Cir. 2004)(imposing sanctions where defendant deleted files from laptop computer the morning he turned it over to plaintiff); Rambus, Inc. v. Infineon Technologies, 222 F.R.D. 280 (E.D. Va. 2004)(imposing sanctions when plaintiff's employees engaged in a "shred day" and destroyed some 2 million pages of documents).

[8] Convolve v. Compaq Computer Corp., 223 F.R.D. 162, 176 (S.D.N.Y. 2004).

[9] Fed. R. Civ. P. 37(f).

[10] Advisory Committee note to Fed. R. Civ. P. 37(f), Chapter 3, p. 49.

[11] *E.g.,* Zubulake IV, 220 F.R.D. at 217; Hester v. Bayer Corp., 206 F.R.D. 683 (M.D. Ala. 2001).

[12] *E.g.,* E*Trade Secs. LLC v. Deutsche Bank AG, 230 F.R.D. 582, 592 (D. Minn. 2005).

[13] In Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004)(Zubulake V), the court noted that all accessible backup tapes—those actively used for information retrieval —would likely be subject to the litigation hold, whereas inaccessible backup tapes—those maintained solely for disaster recovery purposes—would be only if they contained documents created by persons likely to have created or received discoverable information. Other courts do not make this distinction.

[14] Zubulake IV, 220 F.R.D. at 218.

[15] *See* Paul, G. L., and B. H. Nearon, THE DISCOVERY REVOLUTION, at 55–58 (American Bar Association, 2006).

[16] 133 F.R.D. 166 (D. Colo. 1990). As the courts interpret the good faith operation standard of Fed. R. Civ. P 37(f), some decisions decided before the amendment to the rule may be rendered unpersuasive or inapplicable. The authors have carefully chosen precedent they consider consonant with the amended rule.

[17] 229 F.R.D. 506 (D. Md. 2005).

[18] Data is not necessarily destroyed when the user issues the delete command. The delete command simply marks the space occupied by such data as available to be overwritten. Depending on a number of factors, including the total available unused storage on the disk and subsequent usage of the computer, such deleted data could persist on the disk for a very long time.

[19] Zubulake IV, 220 F.R.D. at 218; Treppel v. Biovail Corp., 233 F.R.D. 363 (S.D.N.Y. 2006).

[20] *See* Leon v. IDX Sys. Corp. 464 F. 3d 951 (9th Cir. 2006).

[21] *See* Del Campo v. Kennedy, 2006 U.S. Dist. LEXIS 85462 (N.D. Cal. 2006).

[22] *See* Frey v. Gainey Transp. Servs., 2006 U.S. Dist. LEXIS 90639 (N.D. Ga. 2006).

[23] *See* Padilla v. Price Toyota, 2005 U.S. Dist. LEXIS 25720 (D. N.J. 2005).

[24] *See* Wiginton v. CB Richard Ellis, Inc., 2003 U.S. Dist. LEXIS 19128 (N.D. Ill. 2003).

[25] *See* Samsung Elecs. Co. Ltd. v. Rambus, Inc., 440 F. Supp. 2d 512 (E.D. Va. 2006).

[26] Advisory Committee Note to Fed. R. Civ. P. 26(b)(2), Chapter 3, p. 33.

[27] Advisory Committee Introduction to Discovery into Electronically Stored Information That Is Not Reasonably Accessible: Rule 26(b)(2), http://www.uscourts.gov/rules/Reports/ST09-2005.pdf, p. 42.

[28] Advisory Committee Note to Rule 26(b)(2), Chapter 3, p. 33.

[29] Advisory Committee Introduction, n. 27, *supra,* p. 43.

[30] 2005 U.S. Dist. LEXIS 35583 (S.D.N.Y. 2005).

[31] 233 F.R.D. 363 (S.D.N.Y. 2006).

[32] 220 F.R.D. at 217.

[33] 223 F.R.D. 162 (S.D.N.Y. 2004).

[34] Of course, the airline captures the information entered on the touchscreen, but in another place and in another form.

11

Inadvertent Disclosure of Privileged Information or Work Product

Introduction

> *The Committee has repeatedly been advised that the risk of privilege waiver, and the work necessary to avoid it, add to the costs and delay of discovery. When the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed* [1].

As noted in Chapter 7, Fed. R. Civ. P. 16(b) and 26(f) encourage counsel to facilitate discovery by reaching an agreement on minimizing the risk of waiver of privilege or work-product protection through inadvertent disclosure. To the same end, Rule 26(b)(5)(B) provides a procedure for addressing a claim of privilege or protection of trial-preparation material after the information has been produced. But the rules do not address whether the privilege or protection has been waived by such production. "The courts have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information" [2]. This chapter reviews those principles, or the substantive law of waiver. We also analyze the interplay between a voluntary agreement on waiver and the substantive law, which interplay Proposed Federal Rule of Evidence 502, set forth below, addresses.

Substantive Law of Waiver Through Inadvertent Disclosure

Fed. R. Evid. 501 states:

> Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision shall be determined in accordance with State law.

The federal law governing privilege and, in particular, the waiver of privilege through inadvertent disclosure varies by Circuit [3]. That variation is magnified by the fact that in federal cases based on diversity jurisdiction, state law determines the application and scope of the attorney-client privilege [4]. The three general approaches adopted in federal cases are "strict accountability" or automatic subject-matter waiver; the "lenient" view that truly inadvertent disclosure rarely if ever constitutes waiver; and a middle-of-the road, multifactor "balancing test."

The first approach is exemplified by the District of Columbia Circuit decision in *In re Sealed Case* [5]. In this case a government contractor refused to produce six documents it claimed were protected by the attorney-client privilege. The government argued that the privilege had been waived because one of the documents had previously been disclosed to a government accounting agency [6], and the contractor countered that that disclosure had been inadvertent and due to a "bureaucratic error." The district court had found otherwise, but the Court of Appeals (Silberman, J.) found the distinction irrelevant [7]:

> Although the attorney-client privilege is of ancient lineage and continuing importance, the confidentiality of communications covered by the privilege must be jealously guarded by the holder of the privilege lest it be waived. The courts will grant no greater protection to those who assert the privilege than their own precautions warrant. We therefore agree with those courts which have held that the privilege is lost "even if the disclosure is inadvertent." (Citations omitted.)
>
> To hold, as we do, that an inadvertent disclosure will waive the privilege imposes a self-governing restraint on the freedom with which organizations such as corporations, unions, and the like label documents related to

> communications with counsel as privileged. To readily do so creates a greater risk of "inadvertent" disclosure by someone and thereby the danger that the "waiver" will extend to all related matters, perhaps causing grave injury to the organization. But that is as it should be. Otherwise, there is a temptation to seek artificially to expand the content of privileged matter. In other words, if a client wishes to preserve the privilege, it must treat the confidentiality of attorney-client communications like jewels—if not crown jewels. Short of court-compelled disclosure, *cf. Transamerica Computer Co. v. IBM Corp.*, 573 F.2d 646, 651 (9th Cir. 1978) or other equally extraordinary circumstances, we will not distinguish between various degrees of "voluntariness" in waivers of the attorney-client privilege.

Judge Silberman also held that the waiver extended to "all other communications relating to the same subject matter," and remanded to the district court for a finding as to whether the documents at issue fit within the waiver [8].

At the other end of the spectrum are cases that apply a "no waiver" rule, at least when counsel and not the client is responsible for the disclosure. In *Mendenhall v. Barber-Greene Co.* [9], for example, the court held that the inadvertent disclosure of privileged information by counsel did not constitute a waiver [10]:

> We are taught from first year law school that waiver imports the "intentional relinquishment or abandonment of a known right." [footnote omitted] Inadvertent production is the antithesis of that concept. In response to a production request encompassing all Mendenhall files, [Mendenhall's counsel] provided [his adversary] with 28 complete files. When he pored over the files (as was his right) [the adversary] found the four letters now at issue. Mendenhall's counsel now says their delivery was unintended.
>
> Mendenhall's lawyer (not trial counsel) might well have been negligent in failing to cull the files of the letters before turning over the files. But if we are serious about the attorney-client privilege and its relation to the client's welfare, we should require more than such negligence *by counsel* before the client can be deemed to have given up the privilege. (Emphasis in original.) (Citation omitted.) No waiver will be found here.

The court in *Georgetown Manor, Inc. v. Ethan Allen, Inc.* [11], also found "no waiver" to be the better reasoned approach, relying on *Mendenhall* and also the following from the American Bar Association Section of Litigation [12]:

> Where the disclosure resulted because of the attorney's negligence and not that of the client, the client's privilege has not necessarily been relinquished. The more modern rationale, therefore, is that the negligence-free client, whose privilege it is in all events, should not bear the burden of global loss

> of an expectation of confidentiality because of the attorney's negligence in protecting that confidentiality. [citing *Mendenhall*]

The third approach takes the middle road, and focuses on the reasonableness of the steps taken to preserve the confidentiality of privileged documents. The courts taking this approach apply a balancing test to determine whether disclosure constitutes a waiver. The specifics of these tests vary.

For example, the general consensus in district courts within the Second Circuit is that the court should balance four factors: (1) the reasonableness of the precautions taken by the producing party to prevent inadvertent disclosure of privileged documents; (2) the volume of discovery versus the extent of the specific disclosure at issue; (3) the length of time taken by the producing party to rectify the disclosure; and (4) the overarching issue of fairness [13]. Other courts employ a five-factor test, including the reasonableness of the precautions taken to prevent inadvertent disclosure; the number of inadvertent disclosures; the extent of the disclosure; the delay and measures taken to rectify the disclosure; and fundamental fairness [14].

Magistrate Judge Pitman's decision in *In re Parmalat Secs. Litig.* [15] is emblematic of the balancing test analysis. Bank of America argued that it had not waived the privilege when Italian authorities investigating the Parmalat scandal seized BOA correspondence in Italy. Since the parties did not dispute the involuntary nature of the seizure or its legal consequence (involuntary or compelled disclosure does not give rise to a waiver), the magistrate's focus was on what steps BOA took after seizure to "protect and preserve the privilege." Holding that "the length of delay in claiming the privilege should be 'measured from the time the producing party learns of the disclosure, not from the disclosure itself,'" the court found that BOA followed a course of conduct "reasonably designed" to preserve its privilege over the seized documents.

The opposite result was reached in *In re Philip Serv. Corp. Secs. Litig.* [16], even though the court applied the same test. The distinction was Philip's failure to take timely action to preserve the privilege after inadvertent disclosure. Indeed, Philip did not object to its adversary's use of the documents and even "sat idly by" when the documents "were marked as deposition exhibits and witnesses were questioned about them."

As these precedents suggest, the analysis is case specific, and the facts may suggest that the consideration of additional factors is appropriate. For example, in *Curto v. Medical World Communs., Inc.* [17], the plaintiff worked from home on company-issued computers. She "deleted" files from her computers when defendant terminated her employment. The defendant subsequently engaged a computer forensics expert who restored the deleted files, which included communications between plaintiff and her attorney. Plaintiff demanded the return of the privileged documents on the grounds that the disclosure had been

inadvertent. Defendant argued, in effect, that the communications were not protected by the attorney-client privilege because plaintiff had agreed to a company policy specifying that employees waived any right of privacy to any communication created on a company computer. The magistrate judge did not agree that this waiver trumped the attorney-client privilege, at least given the specific facts of the case. Further, the magistrate considered defendant's lack of enforcement of this policy as a factor in the waiver analysis. That is, because the court found that defendant did not enforce the policy, that fact was relevant to whether plaintiff had taken reasonable steps to prevent disclosure. The district court approved the consideration of this subfactor and the magistrate judge's decision that, taking all the factors into account, the privilege had not been waived [18]. The district court gave particular weight to the fact that the former employee (1) was operating from home, (2) used her personal AOL account for communicating with her attorney, not her company account, and (3) attempted to delete privileged communications from the computer prior to returning the company computer.

In general, the courts do not seem inclined to accept a party's contention that the inadvertent disclosure of ESI should be viewed more leniently, because of particular difficulties in processing and reviewing ESI. For example, In *Hernandez v. Esso Std. Oil Co.* [19], Esso recognized documents filed by a third party as being privileged and claimed that they were inadvertently produced due to an "errant mouse click." Esso contended that an electronic file with a particular prefix was created for all documents that were responsive to plaintiffs' written discovery requests, and a separate electronic file with the same prefix created for documents that were either privileged or not responsive to plaintiffs' written discovery. In the rush to meet the court's discovery deadline, the two files were unintentionally merged. As a result, approximately 1,500 potentially privileged documents were inadvertently produced.

Based on its interpretation of First Circuit cases, the court applied the totality of the circumstances test, roughly equivalent to the balancing test. "Said test holds that inadvertent disclosure only constitutes a waiver, if, in view of the totality of the circumstances, adequate measures were not taken to avoid the disclosure" [20]. The circumstances to be considered include the reasonableness of the precautions taken to prevent inadvertent disclosure, the amount of time it took the producing party to recognize its error, the scope of the production, the extent of the inadvertent disclosure, and the overriding interest of fairness and justice.

The court was particularly unimpressed with the precautions taken by Esso to prevent disclosure. Though the documents had been reviewed for privilege before they were converted to PDF and burned to a disc, the discs themselves were, apparently, not reviewed. "This Court is not compelled to protect privileged information inadvertently disclosed by an 'errant mouse click'. If

parties opt to use technological resources to store privileged information, they should also provide the necessary protection for precisely that information" [21]. Finding that the other factors did not compel a contrary conclusion, the court held that Esso had waived the privilege through the disclosure.

Similarly, in *MSF Holding, Ltd. v. Fiduciary Trust Co. Int'l* [22], the defendant moved for a protective order requiring the return of two e-mails produced in discovery that, it argued, contained privileged information. Applying the four-factor balancing test, the court denied the motion. In particular, the court found that the defendant had failed to take reasonable precautions to prevent against inadvertent disclosure [23]. In regard to the steps taken by the defendant to protect against inadvertent disclosure, the court stated, "Neither of the e-mails in question bears any legend identifying it as an attorney-client communication or as a document prepared in anticipation of litigation. Had FTCI intended to preserve the confidentiality of these documents, it should have taken such an elementary precaution. Furthermore, although the two documents produced were initially reviewed by counsel and identified for redaction, FTCI has offered no explanation of how they then came to be released in unredacted form" [24].

Given this potential for calamity, it has become increasingly common for parties to enter into nonwaiver agreements, or seek a confidentiality order from the court. To what extent these agreements trump the substantive law of waiver, and what effect a voluntary agreement or a confidentiality order has on the assertion of privilege as against a third party are issues examined next.

Nonwaiver Agreements

Nonwaiver agreements, as contemplated by Fed. R. Civ. P. 26(f)(4) [25], in which the parties agree to produce documents without first doing a full-fledged privilege review and not waive privilege/work product protection, have been approved by a number of courts in the past [26]. But as Magistrate Judge Paul Grimm stated in *Hopson v. Baltimore* [27], an oft-quoted discussion of the issue, these agreements "certainly are not risk-free" [28]. As noted by Judge Grimm, "[s]ome commentators appear to be openly skeptical of their ability to insulate the parties from waiver" [29], and "it is questionable whether they are effective against third-parties" [30].

As to the first question—whether the parties could by agreement protect against waiver by inadvertent disclosure when by application of the substantive law disclosure would constitute a waiver—Judge Grimm's decision suggests that the answer might be no, at least in those jurisdictions in which the strict accountability approach is taken to inadvertent waiver. Noting that the Fourth Circuit's position on this issue was uncertain, Judge Grimm concluded that the

relevant decisions "express a very strict interpretation of the attorney-client privilege, and an unambiguous willingness narrowly to confine it to its essential function—preserving communications intended to be kept confidential" [31].

> Thus, after nearly ten years of extensive study of the discovery rules by the Advisory Committee on the Federal Rules of Civil Procedure, the procedures proposed to address the burdens of privilege review associated with production of electronically stored information surely would ameliorate them, but at the price of risking waiver or forfeiture of privilege/work product protection, depending on the substantive law of the jurisdiction in which the litigation was pending. Absent a definitive ruling on the waiver issue, no prudent party would agree to follow the procedures recommended in the proposed rule [32].

Judge Grimm found a solution in the doctrine from the substantive law, which provides that a party compelled to produce privileged material does not waive the privilege, even as to third parties [33]. That is, if the nonwaiver agreement is incorporated into a court order, compliance with the procedures in that order should not result in any waiver of privilege for protected information inadvertently produced [34].

However, the substantive law of waiver imposes limits on blanket disclosure provisions [35]:

> A casual reading of … Rules 16 and 26 and their accompanying commentary, without evaluation of the governing substantive law of privilege waiver, could lead counsel to conclude that the … rules permit them to, with a wink and a nod, forego reasonable pre-production review altogether, or to do only a cursory screening. This would be a mistake. Reviewing appellate courts are unlikely to accept the doctrine of compelled disclosure … if it is offered to justify transparently inadequate pre- and post-production privilege review and assertion. If the producing party had adequate opportunity to do full pre-production review, or greater privilege review than was done, but, through sloppiness or want of diligence failed to do so, the reviewing court is unlikely to find present the level of compulsion necessary to immunize the production from waiver of privilege. Similarly, absent any clear signal from the appellate courts that they should do otherwise, district courts called upon to "bless" the production procedures agreed upon by counsel with a court order should independently satisfy themselves that full privilege review reasonably cannot be accomplished within the amount of time court allowing [sic] for the production. The court should also satisfy itself that the production agreed upon by counsel are in fact reasonable and that more could not be accomplished within the production period given the scope of electronic records production permitted by the court.

It should be noted that the substantive law of waiver may also come into play when the parties dispute the terms of a nonwaiver agreement. Thus, in *Koch Materials Co. v. Shore Slurry Seal, Inc.* [36], the parties had entered into a blanket nonwaiver agreement during discovery. The defendant subsequently moved for an order requiring the return of information that had been produced, on the grounds that it was privileged and not within the intended scope of the parties' agreement. The court noted that blanket disclosure provisions were generally disapproved of by the courts, because such provisions immunized attorneys from negligent handling of documents and improper disclosure. "Moreover, where the interpretation of the provision remains hotly disputed, as it is in this case, broad construction is ill advised. Consequently, the court shall not apply the plaintiff's proffered blanket provision in the litigation. Instead, the court shall review the parties' substantive waiver arguments" [37].

Proposed Fed. R. Evid. 502

In regard to the substantive law of waiver for inadvertent disclosure, the proposed rule adopts the "middle ground:" inadvertent disclosure constitutes a waiver only if the party did not take reasonable precautions to prevent disclosure and did not make reasonable and prompt efforts to rectify the error (Proposed Rule 502(b)).

The Committee Note to the proposed rule states that though confidentiality orders are becoming increasingly common, "the utility of a confidentiality order in reducing discovery costs is substantially diminished if it provides no protection outside the particular litigation in which the order is entered." And because there is "some dispute" on whether a confidentiality order entered into in one case can bind nonparties from asserting waiver by disclosure in a separate litigation, the rule clarifies that a confidentiality order entered into in a federal proceeding is enforceable against nonparties in any federal or state proceeding (Proposed Rule 502(d)).

Subdivision (e) of the proposed rule "codifies the well-established proposition that parties can enter an agreement to limit the effect of waiver by disclosure between or among them," as the Note states. But that agreement "can bind only the parties to the agreement" unless the agreement is made part of a court order.

The Proposed Rule 502 is reproduced in its entirety here [38].

> Rule 502. Attorney-Client Privilege and Work Product;
> Limitations on Waiver

The following provisions apply, in the circumstances set out, to disclosure of a communication or information covered by the attorney-client privilege or work-product protection.

(a) Disclosure made in a federal proceeding or to a federal officer or agency; scope of a waiver. When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if:

(1) the waiver is intentional;

(2) the disclosed and undisclosed communications or information concern the same subject matter; and

(3) they ought in fairness to be considered together.

(b) Inadvertent disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:

(1) the disclosure is inadvertent;

(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and

(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Fed. R. Civ. P. 26(b)(5)(B).

(c) Disclosure made in a state proceeding. When the disclosure is made in a state proceeding and is not the subject of a state-court order, the disclosure does not operate as a waiver in a federal proceeding if the disclosure:

(1) would not be a waiver under this rule if it had been made in a federal proceeding; or

(2) is not a waiver under the law of the state where the disclosure occurred.

(d) Controlling effect of court order. A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court. The order binds all persons and entities in all federal or state proceedings, whether or not they were parties to the litigation.

(e) Controlling effect of party agreement. An agreement on the effect of disclosure is binding on the parties to the agreement, but not on other parties unless it is incorporated into a court order.

(f) Controlling effect of this rule. Notwithstanding Rules 101 and 1101, this rule applies to state proceedings in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if state law provides the rule of decision.

(g) Definitions. In this rule:

(1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and

(2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.

Endnotes

[1] Advisory Committee Note to Fed. R. Civ. P. 26(b)(5), Chapter 3, p. 36.

[2] *Id.*

[3] This chapter does not address other aspects of waiver, such as selective waiver. See *Report of the Advisory Committee on Evidence Rules*, May 15, 2007, *available at* http://www.uscourts.gov/rules/Reports/EVOS-2007.pdf.

[4] Fed. R. Evid. 501.

[5] 877 F.2d 976 (D.C. Cir. 1989); *see also* Texaco v. P.R., Inc. v. Dep't of Consumer Affairs, 60 F.3d 867, 883 (1st Cir. 1995); Carter v. Gibbs, 909 F.2d 1450, 1451 (Fed. Cir. 1990) (en banc), *superseded in nonrelevant part,* Pub. L. No. 103–424, § 9(c), 108 Stat. 4361 (1994), as recognized in Mudge v. United States, 308 F.3d 1220, 1223 (Fed. Cir. 2002).

[6] The government also argued that the privilege was waived because the documents contained only information that had been or presumably would be reported to the IRS. The court was not convinced that the documents contained only accounting "details" supporting the information in the returns, as opposed to advice of counsel regarding the returns.

[7] 877 F.2d at 980. The court cited In re Grand Jury Proceedings, 727 F.2d 1352 (4th Cir. 1984), as one of those courts, but it should be noted that at least one district court in the Fourth Circuit disagrees that the issue of inadvertent disclosure was expressly addressed by that court. Hopson v. Mayor & City Council of Baltimore, 232 F.R.D. 228, 236–37 (D.Md. 2005).

[8] 877 F.2d at 980–981.

[9] 531 F. Supp. 951 (N.D. Ill. 1982).

[10] *Id.* at 954.

[11] 753 F. Supp. 936 (S.D. Fla. 1991).

[12] *Id.* at 938, *quoting* THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK PRODUCT DOCTRINE, p. 66 (2d ed. 1989).

[13] *See, e.g.,* Lava Trading, Inc. v. Hartford Fire Ins. Co., 2005 U.S. Dist. LEXIS 466 at *5 (S.D. N.Y. 2005); Atronic Int'l, GmbH v. SAI Semispecialists of Am., Inc., 232 F.R.D. 160 (E.D. N.Y. 2005). This is not to say there is a consensus even among the district courts comprising the Second Circuit. In fact, all three approaches can be found within the circuit. For example, compare In re Horowitz, 482 F.2d 72, 80–82 (2d Cir. 1973) (Friendly, J.) (privilege waived when legal documents were provided to accountant for other purposes with no admonition not to review them); Connecticut Mut. Life Ins. Co. v. Shields, 18 F.R.D. 448 (S.D.N.Y. 1955) (no waiver without intent to waive); and SEC v. Cassano, 189 F.R.D. 83 (S.D.N.Y. 1999) (multifactor balancing test applied to find waiver).

[14] *See, e.g.,* F.C. Cycles, Int'l, Inc. v. FILA Sport S.p.A., 184 F.R.D. 64, 76 (D. Md. 1998).

[15] 2006 U.S. Dist. LEXIS 88629 (S.D.N.Y. 2006).

[16] 2005 U.S. Dist. LEXIS 22998 (S.D.N.Y. 2005).

[17] 2006 U.S. Dist. LEXIS 29387 (E.D. N.Y. 2006).

[18] *Id.* at *14.

[19] 2006 U.S. Dist. LEXIS 47738 (D. P.R. 2006).

[20] *Id.* at *10.

[21] *Id.* at *15.

[22] 2005 U.S. Dist. LEXIS 34171 (S.D.N.Y. 2005).

[23] The court assessed the issue of waiver, though it also found that the information was mainly commercial in nature and therefore not protected by the attorney-client privilege. *Id.* at *3.

[24] *Id.* at *4. The court also noted that the entire production consisted of only 202 pages, contrasting the situation with "a disclosure of numerous electronic documents where privilege review might legitimately be based on an imperfect computerized search rather than individual document review." *Id.* at *5.

[25] *See* Advisory Committee Note to Fed. R. Civ. P. 26(f), Chapter 3, p. 41.

[26] *See* Hopson v. Mayor and City Council of Baltimore, 232 F.R.D. 228, 234–35 (D. Md. 2005) for a review of the case law. But as the court noted in *Hopson,* not all courts approved such agreements. *See* Koch Materials Co. v. Shore Slurry Seal Inc., 208 F.R.D. 109, 118 (D.N.J. 2002).

[27] 232 F.R.D. 228.

[28] *Id.* at 235.

[29] *Id., citing* 24, Charles Alan Wright and Kenneth W. Graham, FEDERAL RULES OF EVIDENCE, Ch. 6 §, 5507, 579, n. 22 (1986).

[30] *Id.* (Citations omitted.)

[31] *Id.* at 238. In addition, the cases "take an unforgiving view of the results of its waiver—subject matter waiver." *Id.*

[32] *Id.* at 233–234.

[33] *Id.* at 241–244, *citing, e.g.,* Transamerica Computer Co. v. IBM Corp., 573 F.2d 646 (9th Cir. 1978).

[34] *Id.* at 246. The proposed amendment to Fed. R. Evid. 502 provides that an agreement between the parties is binding on the parties, but not on other parties, unless the agreement is incorporated into a court order, as set forth, *infra.*

[35] *Id.* at 244, n. 39.

[36] 208 F.R.D. 109 (D. N.J. 2002).

[37] *Id.* at *29, 30.

[38] The proposed rule is of course subject to revision; the version in the accompanying text is dated May 15, 2007.

12

Ethical Issues in Litigating with ESI

Introduction

One of the fascinating aspects of ethics issues for most practitioners is the multitude of circumstances in which they arise, the variety of unexpected scenarios that they address, and the pervasive question of whether a given precedent has any application in other jurisdictions. It is somewhat rare for a particular set of facts to replicate precisely. For example, in *Grievance Administrator v. Fieger* [1], the Michigan Supreme Court was called upon to consider allegations that an attorney's radio description of his appellate panel as "three jackass Court of Appeals judges" who had "changed their names from Hitler, Goebbels, and … Eva Braun," and all of whom deserved to be anally violated, constituted an ethical violation [2]. A divided Michigan Supreme Court held a violation had occurred. There were three dissents. While the careful reader may take immediate steps to consider how such precedent might affect his or her appellate caseload, prudent practice at least suggests that we all seek to brush up on those abstruse, mystical rules addressing respect for the tribunal and civility for those involved in the judicial process.

Turning to ESI, the nature and extent of the attorney's obligations in regard to the client's duty to preserve and produce ESI has loomed large as an issue in the reported decisions on e-discovery and is covered in Chapters 10, 11, and 17. The perils of inadvertent disclosure of privileged ESI in discovery are covered in Chapter 11. Any number of other ethical issues may arise in litigating with ESI [3]. This chapter raises certain issues likely to be encountered (and as above, hopefully some that aren't) by every practitioner. We describe these issues quite broadly because, of course, the specific ethical rules vary by jurisdiction. We also include some practical recommendations for addressing these

issues, though we do not by any means suggest that compliance with ethical obligations requires adopting them.

Safeguarding Confidential Information

Rule 1.6(a) of the Model Rules of Professional Conduct provides:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

The Comment notes:

> A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

Protecting confidential information from unauthorized disclosure is an obligation incumbent on every attorney. Complying with that obligation in regard to ESI raises a number of issues.

Law Office Security

An attorney must make reasonable efforts to protect the office IT system from unauthorized entry and resultant potential for disclosure of confidential information [4]. The State Bar of Arizona describes what efforts will satisfy that obligation as follows [5]:

> … an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end. An attorney who lacks or cannot reasonably obtain that competence is ethically required to retain an expert consultant who does have such competence.

The ethical standard set by the Arizona Bar may be higher than that in other jurisdictions. But when practical considerations are also taken into account—that a breach of security can result in loss of firm productivity,

corruption of data, and adverse effects on client relations—the calculus may usually "weigh in favor of overprotection" [6].

A short list of basic security issues to be addressed and reevaluated often to keep abreast of new developments, includes the following:

- Protection from unauthorized entry by viruses, worms, Trojan horses, spyware, and Internet probes;
- Intrusion detection;
- Encryption of stored information;
- Security of information on mobile devices, such as laptops.

Other issues to consider in regard to security of ESI include relationships with third parties. For example, lawyers should ensure that computer maintenance companies have reasonable procedures in place to protect the confidentiality of information to which the service provider has access [7]. The same requirement, of course, applies to online service providers, including billing services, document storage [8], and litigation support services. Attorneys from different firms who share office facilities should ensure that access to client files is appropriately restricted [9].

Finally, we note that proposed Rule of Evidence 502 and its ultimate treatment of the selective waiver issue may have implications for procedures governing ESI security. As drafted, the rule would allow disclosure to regulatory or enforcement authorities without waiving the privilege for purposes of future civil litigation. Carefully identifying, segregating, and protecting ESI that is to be disclosed to one entity, but no other, will be critical. And the language of the proposed rule addressing inadvertent disclosure requires that, to prevent waiver, the party must take reasonable steps to prevent disclosure and promptly attempt to rectify the error [10].

Client E-Mail

Whether communicating client confidences via unencrypted e-mail complies with the confidentiality rules is an issue that was considered early and by many state bars. When e-mail was in its infancy, and its susceptibility to access by third parties suspect, the answer was often no, at least absent specific client consent [11]. In the spring of 1999, however, the American Bar Association (ABA) Standing Committee on Ethics and Professional Responsibility issued its opinion that a lawyer may transmit information related to the representation of a client using unencrypted e-mail "because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint" [12]. That remains the prevailing view today [13].

Nonetheless, lawyers are also obligated to "use good judgment and discretion" concerning the sensitivity and confidentiality of electronic messages [14]. In the comment to Model Rule 1.6, the ABA Committee states that "[s]pecial circumstances … may warrant special precautions." Further, "[f]actors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule" [15]. Some practitioners strongly suggest that encrypting attorney-client e-mail is a best practice that should be adopted [16].

Another tactic for protecting client e-mail from inadvertent disclosure—and from inadvertent loss or corruption—is to maintain a policy of segregating client e-mail. Many process options exist for instituting such a policy. Most e-mail software provides search capabilities making it possible, retrospectively, to find any specific e-mail by many different search criteria. A single e-mail message or even a group of related e-mail messages can be found quickly. It may be more desirable and productive, however, to set up an approach to help segregate correspondence as it is received in real time. These approaches vary in cost, sophistication, and degree of automation. One simple approach is to set up a separate subdirectory (folder) for each client and then to remember to move all correspondence and respective attachments to the client's folder as they are received and reviewed. This option involves no incremental out-of-pocket cost, but having to remember to archive each e-mail message appropriately may be too burdensome. At the other end of the spectrum, sophisticated case-management systems can be configured to automatically archive correspondence from different clients in their respective archives. Because the cost of online hosting has gone down, the scope of services included increased, and reliability improved, some may find the preferred option to set up separate e-mail addresses dedicated to different clients.

Metadata

Senders of electronic communications also have a responsibility to protect metadata from disclosure. The American Bar Association admonishes [17]:

> A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by "scrubbing" metadata from documents or

by sending a different version of the document without the embedded information.

Some state bars simply require members to take reasonable steps to prevent the inadvertent disclosure of metadata. For example, the New York State Bar Professional Ethics Committee issued an opinion directing attorneys to use "reasonable care" to protect metadata from disclosure. In regard to what constitutes "reasonable" steps to preserve confidentiality, the committee states: "What constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a template used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document. Reasonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission." N.Y. State 782 (2004). Similarly, the Florida State Bar Professional Ethics Committee issued a proposed advisory opinion requiring a lawyer to take "reasonable steps" to protect confidential information in metadata from disclosure.

Maryland's recent ethics opinion 2007–09 made it clear that the onus regarding the ethical duty rested squarely on the sender of e-mail transmissions including metadata. In Maryland, the recipient is under no obligation to return the data received, to avoid looking for such data, or even to disclose to the sending party that such metadata was transmitted [18].

Web Sites

Presumably practitioners have already drafted appropriate disclosures and disclaimers, conformed their Web sites to the applicable rules regarding advertising, and otherwise managed the more obvious issues arising from hosting a Web site. With respect to advertising, the Telephone Consumer Protection Act of 1991, 47 U.S.C. Section 227, most frequently invoked with respect to facsimile transmissions, also prohibits "unsolicited advertisements" sent by computer [19]. This proscription would also appear to create issues for those attorneys who engage in chat room discussions, as discussed more fully next.

J. T. Westermeier's *Ethics and the Internet* (Web Sites)

In J. T. Westermeier's *Ethics and the Internet*, 17 GEO. J. LEGAL ETHICS 267 (2004), the author analyzes other interesting ethical issues related to operating or accessing Web sites that may not seem so obvious The remainder of this chapter is an excerpt from *Ethics and the Internet* [20].

Which Ethical Rules Apply?

Web sites may be visited by residents of any state or country. This raises obvious questions as to what ethical rules the attorney or law firm with a Web site must comply. Model Rule 8.5(b)(2) provides a choice-of-law rule for disciplinary purposes when lawyers are licensed in more than one jurisdiction [21]. Under this choice-of-law rule, the Web site would be subject to the rules of the jurisdiction in which the lawyer principally practices, "unless the particular conduct clearly has its predominant effect in another jurisdiction in which the lawyer is licensed" [22]. This choice-of-law rule is likely to prove very difficult for lawyers and law firms to apply, especially in determining with any kind of certainty in which jurisdiction a Web site will have its predominant effect. In the context of the Internet, the "predominant effect" choice-of-law test is especially difficult to apply "because it is difficult to discern where the predominant effect of Internet activity is felt" [23]. Model Rule 8.5(b) potentially subjects lawyers to the ethics rules of states in which they are not licensed to practice [24]. One commentator believes the "predominant effect" test poses an unacceptable level of uncertainty and risk for lawyer Web sites and Internet communications, and urges bar associations to promulgate a choice-of-law rule that gives lawyers confidence in their choice of whose rules to follow [25]. This commentator believes the competing state interests are outweighed by the need for greater certainty for lawyers employing Web sites [26].

To deal with the uncertainty and risk presented by the choice-of-law rule, it is desirable for lawyers to comply with the ethics rules on advertising for all states in which they are licensed to practice. It is also desirable for law firms to comply with the ethics rules in all states in which members of the law firm are licensed [27]. William Hornsby, staff counsel to the American Bar Association Commission on Lawyer Advertising, believes that determining which state rules apply to a law firm marketing its services on the Internet requires consideration of the states in which members of the firm are admitted to practice, the states in which the firm seeks clients, and the states in which the firm practices [28]. All of this is easy to say, but compliance would be a nightmare, and for large law firms with geographically dispersed offices, compliance is likely to be virtually impossible.

There is also concern with jurisdictions where lawyers or members of the firm are not licensed, since the Web site can be viewed by residents of states where they are not licensed. Some state ethical codes specifically limit legal advertising to a specified jurisdiction [29]. Vermont, for example, provides that in the exercise of Vermont's disciplinary

authority a court may apply Vermont rules to the conduct of a lawyer not licensed to practice in Vermont who engages in the practice of law in Vermont [30]. Similarly, Mississippi's recently adopted Disciplinary Rules subject lawyers who are not admitted in Mississippi to the disciplinary authority of Mississippi if the lawyer advertises, provides, or offers to provide, any legal services to be performed in Mississippi [31]. Such limitations are inappropriate on the World Wide Web; but nevertheless, they exist. Another concern is that the state where the lawyer is licensed might apply the state's prohibition against misleading advertising and claim that a lawyer's or law firm's Web site is misleading because it suggests that the lawyer or firm can practice in other jurisdictions [32]. The Web site should clearly indicate the jurisdictional limitations of lawyers in the law firm. The minimum standards of avoiding deception or confusion can probably be satisfied by indicating the state or states in which each lawyer is admitted to practice [33]. It is also desirable to identify where each lawyer's offices are located physically.

Chat Rooms

One lawyer goes so far as to say that to talk about legal matters in public chat rooms is to invite disaster [34]. Participating in online chat room discussions definitely has some ethical risks. In online chat groups or conference areas, the participants are not necessarily known to each other [35].

> The attorney participating in one of these [chat room] forums may not have all the relevant facts before giving advice, the attorney may have a conflict of interest, the attorney may be communicating with someone who is already represented by counsel, or the attorney may be publicly discussing confidential information.

You do not know who you are really chatting with or who is listening to your communication. Lawyers have to be particularly sensitive in chat rooms attended by nonlawyers. Attorneys do not want to create attorney-client relationships unknowingly. Furthermore, direct solicitation in chat rooms is likely to be covered by direct solicitation rules [36]. The same is likely to be true for news groups, discussion groups, or other forms of interactive communications.

The District of Columbia has issued an ethics opinion on chat room communications by attorneys with Internet users seeking legal information [37]. This D.C. ethics opinion provides that "it is permissible for lawyers to take part in on-line chat rooms and similar arrangements through which attorneys engage in back-and-forth

communications, in 'real time' or nearly real time, with Internet users seeking legal information, provided they comply with all applicable rules of professional conduct" [38]. This D.C. opinion warns attorneys to not give specific legal advice in such chat room communications to avoid the formation of an attorney-client relationship through such chat room conversations [39].

This D.C. ethics opinion on attorney communications in chat rooms emphasizes that the same prescriptions in other attorney communications apply to chat rooms or similar services [40]. "The communications must be accurate" [41]. "Lawyers may not imply that they are disinterested in particular matters when they are not" [42]. "Lawyers must disclose any fees they pay in order to participate and such fees may not be linked to or contingent on the amount of legal fees the lawyer may obtain … through on-line services" [43]. Such communications, the D.C. ethics opinion warns, must not involve solicitations using "undue influence" [44] or "seeking employment by a potential client whose 'physical or mental condition' makes rational judgment 'about the selection of any attorney unlikely'" [45] These concerns are perfectly understandable, but, as a practical matter, are likely to be very difficult to discern in virtual chat room communications where the person you are chatting with is anonymous.

The D.C. opinion offers practical advice on avoiding the formation of attorney-client relationships in chat rooms or other situations [46]. The D.C. opinion emphasizes that the key is to avoid providing legal advice in such communications [47]. Legal advice, the D.C. opinion notes, "involves offering recommendations tailored to the unique facts of a particular person's circumstances" [48]. Thus, the D.C. opinion advises, "in discussing legal information, lawyers should be careful to emphasize that it is intended as general information only, which may not be applicable to an individual's specific situation" [49]. Furthermore, the D.C. opinion recommends that "where a communication is lengthy or otherwise might leave room for misunderstanding, lawyers should remind inquirers that the chat room communication is not a substitute for specific legal advice, and that the lawyer is providing general legal information only" [50]. If any attorney-client relationship is formed by such chat room communications, the D.C. ethics opinion advises "the full panoply of ethical considerations [apply], including conflict avoidance, confidentiality, competence," diligence, zeal, and adequate communications [51].

A number of state bars have also issued ethical opinions respecting chat rooms. Florida specifically prohibits attorneys from soliciting prospective clients through Internet chat rooms, which are defined broadly

as real-time communications between computer users [52]. Besides Virginia and Florida, several other states have considered the issue of whether attorney participation in chat rooms constitutes impermissible solicitation. For example, Michigan rendered an ethics opinion concluding that while e-mail communications were akin to direct mail communications [53]:

> A different situation arises if a lawyer is participating in interactive communication on the Internet, carrying on an immediate electronic conversation. If the communication was initiated by the lawyer without invitation, such 'real time' communications about the lawyer's services would be analogous to direct solicitations, outside the activity permitted by [Michigan Rules of Professional Conduct Rule] 7.3.

Similarly, the West Virginia Lawyer Disciplinary Board stated [54]:

> The Board is of the opinion that solicitations via real time communications on the computer, such as a chat room, should be treated similar to telephone and in-person solicitations. Although this type of communication provides less opportunity for an attorney to pressure or coerce a potential client than do telephone or in-person solicitations, real-time communication is potentially more immediate, more intrusive and more persuasive than e-mail or other forms of writing. Therefore, the Board considers Rule 7.3(a) to prohibit a lawyer from soliciting potential clients through real-time communications initiated by the lawyer.

In an ethics opinion issued by the Illinois State Bar Association, the Ethics Committee stated [55]:

> The Committee does not believe that merely posting general comments on a bulletin board or chat group should be considered solicitation. However, of [sic] a lawyer seeks to initiate an unrequested contact with a specific person or group as a result of participation in a bulletin board or chat group, then the lawyer would be subject to the requirements of Rule 7.3. For example, if the lawyer sends unrequested electronic messages (including messages in response to inquiries posted in chat groups) to a targeted person or group, the messages should be plainly identified as advertising material.

As communications become more interactive, lawyers need to be very sensitive to whether the communication is advertising or direct solicitation. The potential for undue influence is probably the greatest in chat rooms where a prospective client may feel pressured to obtain legal representation [56]. On the other hand, there is some recognition that chat room attorney communications are probably less potentially coercive than face-to-face communications because the potential client always has, even with respect to real-time communications, the option of simply "not responding" [57].

Communicating with Adverse Client's Web Site

May a lawyer access the Web site of the adversary lawyer's client? Oregon recently issued a formal ethics opinion covering this issue [58]. The Oregon opinion noted that if the contact would be prohibited in nonelectronic form, then it is prohibited in electronic form [59]. Here, the opinion concluded that "[a] lawyer who reads information posted for general public consumption is not communicating with the represented owner of the Web site [60]. If, however, a lawyer visiting the Web site of a represented person sends a message with "the expectation of receiving a personal response," then in that situation, if the subject of the communication with the represented person is on or directly related to the subject of the representation, the lawyer violates DR 7-104" [61]. In this opinion, Oregon observed [62]:

> Without doubt the Internet will be an increasingly common form of advertising and communication in commerce and law practice. It is not possible to foresee all the variations on how that communication will occur. The essence of this analysis, however, is whether the Internet-based communication has the character of a telephonic or face-to-face conversation. For the same reasons that conversing directly or indirectly with a represented person is forbidden by telephone or in person, it is also forbidden in any electronic format. Lawyers who wish to obtain information from a represented person's Web site must exercise the same caution they would use in eliciting information by other means.

Linked Sites

Providing links to other Web sites also raises ethical considerations. The lawyer or law firm providing the link from its Web site does not control the completeness, accuracy, or timeliness of the content in the linked Internet sites. How do the linked sites affect compliance with the ethical rules on lawyer advertising? What, if any, of the content in the

linked materials is false, misleading, deceptive, or otherwise contravening of the advertising rules? One ethics committee advises that law firms with "links to outside sites should, of course, clearly indicate to the Web browser that [the outside sites] are not maintained by the law firm" [63].

There is also concern over the possibility of the lawyer or law firm being viewed as an endorser, or being liable for negligent referral [64]. The same issues may arise in connection with allowing other Internet sites to provide linkage to a lawyer's or law firm's Web site, as well as the ethical rules pertaining to referrals [65]. There is also the possibility that a link to another site might serve as a basis for a contributory copyright infringement claim or a claim for inducing copyright infringement by promoting other infringing sites [66].

Endnotes

[1] 476 Mich. 231, 719 N.W. 2d 123 (2006).

[2] The particular rules in question included Michigan Rules of Professional Conduct 3.5(c), 6.5(a), and 8.4(a) and (c).

[3] *See, e.g.*, http://www.legalethics.com.

[4] *See, e.g.*, John D. Comerford, *Current Developments 2005–2006: Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and Computer Networks*, 19 GEO. J. LEGAL ETHICS (2006).

[5] Opinion no. 05-04.

[6] Daniel Kamitaki, Note: *Beyond E-mail: Threats to Network Security and Privileged Information for the Modern Law Firm,* 15 S. CAL. INTERDIS. L. J. 307, 344 (2006).

[7] J. T. Westermeier, Article*: Ethics and the Internet*, 17 GEO. J. LEGAL ETHICS 267, 302 (2004).

[8] The attorney has an obligation to preserve client communications by employing appropriate backup procedures. *Id.* at 301.

[9] *See, e.g.*, D.C. Bar Legal Ethics Comm. Op. 303 (2001).

[10] *See* proposed Federal Rule of Evidence 502.

[11] *E.g.,* North Carolina State Bar Ethics Op. no. RPC 215 (7/95).

[12] ABA Comm. on Ethics and Professional Responsibility, Formal Op. 413 (1999). *See also* Comment to Model Rule 1.6: "This duty … does not require that the lawyer use special

security measures if the method of communication affords a reasonable expectation of privacy."

[13] *See* Matthew J. Boettcher and Eric G. Tucciarone, Article*: Concerns over Attorney- Client Communications Through E-mail: Is the Sky Really Falling?* 2002 L. REV. M.S.U.-D.C.L. 127 (2002). Other jurisdictions require express client consent to the use of unencrypted e-mail, at least for sensitive communications. *Nat'l Rptr. on Legal Ethics and Prof'l Responsibility*, Iowa Formal Op. 97-1 (1997). The attorney must consult the rules relevant to his or her practice.

[14] Model Rules of Professional Conduct, Rule 1.6, Comment 16.

[15] Model Rule 1.6, Comment 17. For example, it has been suggested that special care should be given when communicating to a client via e-mail to the client's workplace because of the prevalence of e-mail monitoring by the employer. *See* Dion Messer, Article: *To: Client@Workplace.com: Privilege at Risk?* 23 J. MARSHALL J. COMPUTER & INFO. L. 75 (2004).

[16] *See* Jack Seward*, Failure to Encrypt E-Mail Jeopardizes the Privilege and Work-Product Doctrine: Protect or Perish*, 25-1 ABIJ 44 (2006).

[17] Formal Opinion 06-442 (August 5, 2006). The model rules do not prohibit a lawyer who receives metadata that has been inadvertently disclosed from reviewing or using it, though he or she is required to notify the sending party. *See id.*; Rule 4.4(b). *But see, e.g.*, N.Y. State 749 (2001) (a lawyer may not use technology to get behind what is visible on the screen).

[18] Maryland Ethics Opinion 2007–09, issued October 19, 2006.

[19] Stern v. Bluestone*,* 2006 N.Y. Misc. LEXIS 2495 (Aug. 18, 2006).

[20] Reprinted with permission of the publisher, *Georgetown Journal of Legal Ethics* © 2004. Vol. 17, No. 2, pp. 267–312.

[21] [NB: Because we have reprinted excerpts from the article the footnote number in this text does not correspond to the number in the original. Internal footnote references correspond to the original. For full references to certain footnote citations, reference must be made to the original.] MODEL RULES Rule 8.5(b)(2); *see also* Rogers, *supra* note 26, at 45.

[22] Rogers, *supra* note 26, at 45.

[23] Backer, *supra* note 2, at 2411.

[24] *See id.*

[25] *See* Backer, *supra* note 2, at 2423.

[26] *See id.*

[27] *Id.; see* Pa. Op. 98–85, *supra* note 6, at 2–4.

[28] *See* Hornsby, *supra*, note 2.

[29] Iowa, for example, provides that electronic ads are permitted only in the geographic area in which a significant part of the lawyer's clients reside, and the lawyer has offices. IOWA CODE OF PROFESSIONAL RESPONSIBILITY DR 2-101(B)(5)(2003); *see* Rogers, *supra* note 26, at 42. Pennsylvania has expressed concern about the Florida Bar taking the

unique position that lawyers, whether or not admitted to practice law in Florida, and those who disseminate advertisements within Florida, including computer-accessed communications (defined to include World Wide Web sites), are subject to the lawyer advertising rules and procedures promulgated by the Supreme Court of Florida. *See* Pa. Op. 98-85, *supra* note 6, at 2–4.

[30] *See* Backer, *supra* note 26, at 46.

[31] See MISS. RULES OF PROFESSIONAL CONDUCT Rule 8.5 (2003).

[32] Rogers, *supra* note 26, at 46.

[33] *See id.*

[34] *See* Maureen Castellano, *Policing Cyberspace,* N.J. L.J., Apr. 8, 1996, at 1 (attributing comment to William Voorhees, vice chair of the New Jersey State Bar Association's Special Committee on malpractice insurance).

[35] Kirkey, *supra* note 3, at 47.

[36] *See* Va. Op. A-0110, *supra* note 93 (prohibiting the solicitation of employment in chat rooms from victims or their immediate family in personal injury or wrongful death cases).

[37] *See* D.C. Op. 316, *supra* note 205.

[38] D.C. Op. 316, *supra* note 205.

[39] *See id.*

[40] *See id.*

[41] *Id.*

[42] *Id.*

[43] D.C. Op. 316, *supra* note 205.

[44] *Id.*

[45] *Id.*

[46] *See id.*

[47] *See id.*

[48] D.C. Op. 316, *supra* note 205.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *See* Fla. Op. A-00-1, *supra* note 99.

[53] Mich. RI-276, *supra* note 93.

[54] W. Va. Op. 98-93, *supra* note 99.

[55] Ill. Op. 96-10, *supra* note 90.

[56] Darren Franklin, *Hanging a Shingle on the Information Superhighway*, 2001 STAN. TECH. L. REV. 2 (2001).

[57] *See* D.C. Op. 316, *supra* note 205.

[58] Or. State Bar Ass'n Bd. of Governors, Formal Op. 2001-164 (2001) [hereinafter Or. Op. 2001-164]. D.C. Rule 4.2(a) prohibits communications by attorneys with a party known to be represented by another lawyer in the matter. *See* D.C. RULES Rule 4.2(a)(2003).

[59] *See* Or. Op. 2001-164, s*upra* note 324.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] N.Y.C. Op. 1998-2, *supra* note 1.

[64] *See* Woody, *supra* note 2.

[65] *See id.; see also* Rogers, *supra* note 26, at 45.

[66] In Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999), the district court determined that by providing links on its site to three other sites displaying the infringing work that defendant could be liable for contributory copyright infringement.

13

Fundamentals of ESI Management

Introduction

ESI management is a broad topic that overlaps or implicates many discovery issues. The duty to preserve evidence, spoliation and sanctions, cost-shifting, methods of production, as well as trial issues, such as authentication and the hearsay exclusions, are all legal issues that somehow intersect with ESI management. For the attorney, ESI management is further complicated by the fact that she has obligations in regard to the client's ESI management during litigation, as well as her own office ESI. And because the tools and techniques for managing electronically stored information are different from the well-known paper document management procedures—and constantly changing—the challenge of managing electronic documents to satisfy multiple, sometimes competing objectives, is significant.

But that challenge must be undertaken for any number of reasons. Litigation counsel may be called upon to defend a charge that statutory requirements for the preservation of ESI have not been met, or oppose a motion for sanctions on the grounds that a client's regular operational ESI destruction procedures violate preservation obligations. Properly managing ESI avoids the risk of inadvertent disclosure of privileged information, or inadvertent loss of evidence that could have been introduced to support claims or defenses at trial. Developing an effective ESI management plan requires an investment of time and resources, but the returns on that investment may be substantial. A good plan will, *inter alia*, reduce the time and expense of finding and reviewing documents for audit, investigation, and litigation; eliminate duplication and storage costs; prevent court-imposed monetary sanctions for failure to preserve; avoid inadvertent production of sensitive trade secret, proprietary, or privileged information; and, in

general, harness the efficiencies of electronic data creation and exchange to the litigation process.

Of course, every business already has some type of plan in place for creating and storing ESI, if only that of segregating client or subject matter documents into separate electronic folders. And many will have been forced by operational needs or legal requirements to develop sophisticated ESI management practices. But it may be time to upgrade and update the plan, commit corporate custom and practice to a written policy, or review existing plans to ensure that evolving legal and technology issues are adequately addressed.

ESI management is only effective if an institutionalized plan is enforced. In a recent survey of 300 business technology professionals, only 18% of respondents said their organizations use products that delete data so thoroughly that it is completely unrecoverable [1]. A key part of developing or reviewing an ESI management plan is ensuring that custodians of ESI are assigned the tasks necessary to execute the plan, including data destruction, and are in fact executing the plan.

There are a number of ways to approach ESI management. For example, one could begin with software vendors: evaluate the available solutions at the desired price points, select the optimal solution for anticipated needs, purchase, and install. Another approach is to focus on functionality and derive ESI management needs from operational needs.

Our approach is technology-neutral, to avoid the risk of rapid obsolescence. Our ESI Management Matrix is a practical, step-by-step approach to developing or reviewing an ESI management plan. Our guideline incorporates the legal oversight that counsel must bring to the process, but it is also industry-neutral: it can be used for drafting an ESI management policy for a law firm or for assisting a client in doing so [2]. It can and should be tailored to suit the nature of the business and its level of maturity, though the same basic framework applies to both small and large companies.

ESI Management Planning

Our approach to developing an ESI management plan is as follows. First, create a matrix comprised of an inventory of the ESI created, used, and stored by the business and of the legal and functional requirements and preferences for ESI throughout its life cycle. Second, using a 10-part checklist, create a management plan that matches ESI to the requirements and preferences. The inventories and items on the checklist are discrete items, but creating the plan as a whole is a process requiring referral among the items and cross-checking. For example, item five on the checklist is deciding how ESI is to be organized. Ensuring compliance with the inventory of legal requirements may dictate how particular categories of ESI will be organized.

Before reaching the substance of this approach, an important procedural matter merits brief attention. Ultimately, ESI management is a business issue. How much should be invested by whom to develop and implement the plan is a business decision, as is a determination as to the desired scope of the plan. In addition, developing an ESI management plan requires the participation of persons of differing professional backgrounds who may have conflicting interests. For example, information technology staff and vendors, if the latter are brought into the process, may be focused on maximizing data retention or storage, for achieving these ends demonstrates their proficiency and the capabilities of the technology. Attorneys considering the burdens of the litigation production process and privilege review, while mindful of their duty to preserve evidence, have an interest in limiting data storage.

What this means is that top-level management, the managing partner or chief executive officer, must sponsor and support any initiative for successfully developing an ESI management plan. Without management's imprimatur, and approval of the commitment of resources to develop and implement the plan, it stands much less of a chance of accomplishing its objectives. And to develop a plan for a large or complex business, management must designate C-level personnel (CEO, COO, and so forth), with decision-making authority and subject-matter expertise, to participate.

Once management has approved, developing the plan begins by creating the matrix, and the first component of the matrix is the inventory of ESI. How extensive this component of the project will be depends on, of course, whether the necessary information has already been collected, and how recently; on the overall size and complexity of the business; and the volume and type of ESI that the business creates, exchanges, and stores. The inventory will start from scratch for only a very few businesses: IT and operational units will have lists or indices. But those lists should be assessed for completeness.

ESI Management Matrix

ESI Inventory

The inventory should include all information the business creates and stores in electronic form and a description of where it is located. The what should include, quite simply, all information stored in bits and bytes. A working list to consider would include the following:

> The original (or identical duplicate when the original is not available) and any nonidentical copies (whether nonidentical because of notes made on copies or attached comments, annotations, marks, transmission notations, or highlighting of any kind) of writings of any kind and description

> whether inscribed by mechanical, facsimile, electronic, magnetic, digital, or other means and shall include computer programs (whether private, commercial, or work-in-progress), programming notes or instructions, activity listings of electronic mail receipts and/or transmittals, output (including any intermediate data) resulting from the use of any software program, including word processing documents, spreadsheets, database files, charts, graphs and outlines, electronic mail, instant messaging, operating systems, source code and executable code of all types, peripheral drivers, batch files, ASCII files, and any and all miscellaneous files and/or file fragments, regardless of the media on which they reside and regardless of whether said electronic data exists in an active file, deleted file, or file fragment. Electronic data includes any and all items stored on computer memories (including any temporary storage such as caches), hard discs, floppy disks, CD-ROMs, DVDs, removable media such as Zip discs, Snap servers, USB servers, Jaz cartridges and their equivalents, magnetic tapes of all types, microfiche, punched cards, punched tape, computer chips, or in any other vehicle for digital data storage and/or transmittal. The term electronic data also includes the file, folder tabs and/or containers and labels appended to, or associated with, any physical storage device associated with each original and/or copy.

The inventory of ESI should also include any indices, tags, or other organizational information. And it is important to remember that one electronic document may simultaneously reside in multiple storage media—on a desktop and server, for example—and may also exist in different versions or forms on one or more storage media. All should be included in the inventory. In many cases, only one of the multiple versions will be considered the official record. That designation should be included in the inventory, too.

ESI may be stored, temporarily or permanently, in many different locations. The inventory should include ESI stored in any of the following media:

> Any magnetic or other storage media and media device used to record electronic data and may include, but is not limited to, computer memories, hard disks, floppy discs, Snap servers, DVDs, CD-ROM, and removable media and their equivalent, backup locations, PDAs, and any other vehicle for digital data storage and/or transmittal, whether such storage was temporary or permanent, and shall include any electronic media in the possession or control of any agent, servant, or employee, wherever such media is located.

The list of where should also identify the person who manages or controls each storage medium and all those persons who have access to the data.

Finally, the ESI inventory should include the date of creation of each file, database, or document, its duration in every storage medium in which it resides,

and the date, or expected date, of destruction. Additional data should be included in the inventory, depending on the specific content and nature of such ESI. For example, an inventory entry for ESI containing health insurance claims that were originally processed on a legacy system that has been replaced should also note the specific system and software application needed to access such claims, and whether or not the organization has access to that legacy application (even if limited) or how such ESI can be accessed.

Legal/Regulatory Requirements and Preferences

The second component of the matrix is a list of all legal requirements applicable to the business for document creation, access, storage, and retention that are met with ESI, and those that apply to any information created by the business, regardless of form. For example, if employment records are created in electronic form or original paper documents are converted to electronic form for maintenance and storage, state and federal statutes requiring the maintenance of such records are included on this list. For a broker-dealer, the securities laws and regulations contain explicit record-maintenance requirements. For a law firm, professional ethical obligations with regard to maintaining the confidentiality of client communications and file preservation are, of course, included. All statutes and regulations governing information retention, access, and transmittal require review; the long list of possible candidates would include the Sarbanes-Oxley Act [3], the Health Insurance Portability and Accountability Act [4], ERISA, securities statutes and regulations, regulations regarding government security clearances, export controls, and Food and Drug Administration Good Manufacturing Practices (GMPs), to name just a few.

Third is a list of legal preferences for ESI management. Unlike the legal requirements, the list of preferences is an optional part of the final management policy. That is, it may ultimately be decided, due to limitations on the personnel and technology resources available, because of operational considerations, or for other reasons, not to accommodate these preferences in the policy. But certainly preferences that consist of proactive measures that may ultimately save time and money are well worth considering. For example, for the law firm, many good reasons support a policy of segregating e-mail correspondence between the client and the attorney, not the least of which is to prevent the possibility of inadvertent disclosure. Other reasonable preferences would include imposing restrictions on "thread" e-mail to facilitate search and review for protected work-product and requiring definitive e-mail receipt confirmation (using purchased software) for time-sensitive transmissions.

Operational Requirements and Preferences

The last component of the matrix is an inventory of operational requirements and preferences for ESI creation, access, storage, and retention [5]. For the attorney developing a management plan for his or her own practice or law firm, compiling this list requires a careful consideration of what and how documents and information are used in paper and in electronic form; whether and how paper documents should be digitized; and how to optimize access and reduce storage costs. If resources are available, consideration should be given to hiring a technology consultant in order better to understand the options. The attorney counseling a client on developing an ESI management plan will largely rely on the client's personnel to complete this category, although he or she should confirm that all departments have had the opportunity to contribute and that all contributors understand the outlines and the objectives of the project.

ESI Management Checklist

By compiling these inventories, the policymakers have created a matrix of what is to be managed and the framework for managing it. Overlaying that framework—the legal and operational requirements and preferences—on the identified ESI, one can analyze what fits, and what does not (items one through four on the checklist). The remainder of the plan is for organization and execution.

Item One

Identify any shortfalls in the ESI inventory from the legal requirements. Much of the attention in this regard has been on the loss or destruction of ESI in violation of legal requirements. *See* Chapter 10, *supra*. A systemic and serious deficiency in ESI maintenance requirements should be fairly obvious and readily corrected: a routine and automatic ESI destruction protocol that violates legal maintenance requirements can and should be fixed immediately. The lack of a plan for instituting a litigation hold, or a plan lacking the thoroughness required by the courts in reviewing the issue, is another obvious shortfall that must be addressed. Other shortfalls, or potential shortfalls, will be more subtle and difficult to remedy. For example, isolated and random ESI destruction, through human or technology error or by design, will occur. A litigation hold letter from counsel may fail to reach the appropriate employee because of personnel turnover, and data destroyed as a result. What measures are adopted in the ESI management plan to reduce the possibility of isolated but unlawful data destruction will depend on a number of factors including the specifics of the legal requirement at issue, the ramifications of destruction in terms of sanctions and other penalties, and the resources that can be committed to preventing such loss. The

key is to recognize the shortfall and include reasonable measures to rectify the problem.

The matrix may reveal shortfalls other than the untimely loss or destruction of ESI. Access to certain ESI must be restricted in accordance with legal and professional obligations: client confidences or government clearances, for example. The types of shortfalls in meeting these obligations could be many. For example, ESI that should be accessible only by licensed professionals and their agents or employees that resides on laptops could be viewed by airport security personnel [6]. A salesperson demonstrating software capabilities may be inappropriately revealing trade secrets or other confidential or sensitive data to prospective clients. A disgruntled employee could post confidential information on a blog. Again, what policy is adopted to manage legal ESI access restrictions will depend upon a variety of factors including the degree of risk and probability of harm resulting from unauthorized access.

Item Two

Identify any shortfalls from operational requirements. This aspect of the analysis may well overlap with operational preferences. That is, a functional business is unlikely to have a clear shortfall in managing ESI else it would not be operational. But it is certainly possible that operational requirements could be more effectively met with adjustments to ESI management, and preferences accommodated. For example, modern hospital information systems are designed to process and capture very large amounts of complex data. Managers responsible for various departments need specific information in the form of measures, indicators, or alerts derived from the underlying raw data in the hospital information system. Managing this process so as to reduce or eliminate errors may be considered an operational requirement. Further, the existing system may display the measures and alerts only temporarily. Arguably, all computed alerts should be able to be recreated from the underlying raw data: an operational preference. The objective is, in regard to both operational requirements and preferences, and legal preferences, to focus on the manner in which the company creates, accesses, and stores ESI in order to maximize operational potential, given resource limitations.

Item Three

Identify any overflows of ESI from the legal and operational requirements and preferences, taking into account what preferences are going to be accommodated in the management policy. Is ESI being created that is unnecessary, wasteful, and potentially damaging if accessed by competitors or the public? E-mail is an obvious candidate to be considered in this regard, and many businesses and

other organizations have adopted policies restricting the use of e-mail for personal use [7]. But additional measures could be considered to eliminate excess and unnecessary e-mail correspondence: prohibiting all but approved multiple-recipient lists, for example.

Another possible overflow is ESI that is being stored for a longer period of time than is required by any legal or operational justification, or maintained in multiple versions or forms for no identifiable reason. It is often stated that ESI is more voluminous than paper documents, in part, because it can be stored more cheaply than paper. But storage is not free. And stored ESI might be discoverable, even if the requesting party is required to pay all or part of the costs of recovering the data. It is by no means suggested that excess ESI should necessarily be destroyed. It contains, after all, the history of the company. But a true overflow should be identified and evaluated, and an appropriate destruction policy specific to excess ESI included in the management policy.

Item Four

ESI destruction protocols are the fourth item on the checklist [8]. These protocols flow from what has come before: the legal and operational requirements for data maintenance have been defined. Additional data maintenance and storage needs may arise from decisions made in regard to preferences and excess ESI. The management plan should specify when and how ESI that need not be maintained shall be destroyed. The destruction plan should spell out how to locate all copies of such ESI and specify the procedure for its complete removal, making it unrecoverable by any means. The increasing proliferation of partial or complete copies of ESI makes the task of locating all copies of ESI ever more challenging. The benefits of proactively managing and containing this proliferation seem to be obvious. Software developers who have grappled with the complexity of developing code in teams have long ago accepted the value of explicit code change management including strictly enforced code check-out and check-in.

Item Five

Decide how ESI created and maintained by the business is to be organized. This part of the policy should include protocols for compiling, indexing, and storing ESI. An organization's technology environment is bound to evolve: consider, for example, that in less than 10 years the use of the Internet to establish business presence became almost universal. Such continuous and rapid change makes the development and maintenance of these organizational protocols all the more challenging. The life-cycle analysis should provide a useful framework for assessing what ESI needs to be organized, and any number of software products and services are available to build on that framework and plan for ESI organization.

Item Six

The sixth item on the checklist is to decide on security and emergency backup needs. Two basic overlapping decisions need to be made. First, should the organization invest in dedicated backup hardware and software or rely on one of the backup services that use the Internet for data delivery? Second, should the data that is being backed up be stored in sequential (tape) or direct access (disk) form? In regard to the latter issue, what choice is made may have ramifications on discovery issues, in addition to operational security and backup needs. Decisions on backup needs may also be driven in part by legal requirements.

Item Seven

Assess existing IT resources, including personnel, hardware, and software, to distribute tasks and determine what if any additional resources are needed.

Item Eight

Identify custodians and assign tasks, including ESI organization, security, and destruction. Decide on protocols for access, which may be determined, in part, by legal requirements.

Item Nine

The plan should include specific provisions for assessment or updating. For example, job descriptions and performance evaluations may need to be revised to include tasks assigned to ESI custodians in order to ensure execution of the plan. Depending on the nature and size of the business, the plan may require systemic and ongoing assessment by an employee dedicated specifically to this task. A specific time should be set forth for reviewing the plan for revisions required by law or operational needs, or justified by changes in technologies adopted for business operations or available for data management

Item Ten

The plan should be institutionalized and enforced. The plan should be put in writing and distributed throughout the business. It may be necessary to hold training sessions in order for employees to understand the plan and be prepared to comply with it. Finally, some level of periodic audit should be implemented to ensure ongoing compliance.

ESI Management Planning: Illustrations

The ESI Management Plan described earlier can effectively be used by a sole practitioner to manage his office ESI, or for corporate counsel to understand and provide guidance for managing the ESI of a large and complex business client. The following two examples illustrate this flexibility and demonstrate how our guideline works in practice.

Example 1

A three-lawyer law firm has a personal injury practice representing plaintiffs. The typical client for the firm is an individual injured in an automobile accident or slip and fall. The vast majority of the cases are settled with the insurance carrier before a lawsuit is filed. The settlement value of each case is typically small, but the volume is high.

The firm traditionally obtained the client's authority to settle the case in a written settlement agreement. Increasingly, that authority is memorialized in an e-mail from the client. Depending on the case and the client, that "authority e-mail" could be sent to one of the firm's paralegals or to an attorney. How to manage the authority e-mail after the case is closed is the subject of this example.

Currently, authority e-mail is printed on paper and stored with the rest of the file—in paper form—in a document storage facility leased by the firm. The e-mail may remain in electronic form in the recipient's desktop computer and on the firm's server, as no policy is in place for destruction. The files on the computers are backed up on magnetic tapes at 24-hour intervals. The tapes are stored in the document storage facility.

The specific requirements vary by jurisdiction but, in general, an attorney is obligated by ethics rules to maintain client files for a certain period of time after the case is closed. The prudent attorney would maintain a document evidencing settlement authority for another reason: to defend the settlement in the event it were to be challenged. This legal preference, in the language of the matrix, would be to maintain the authority e-mail until the statute of limitations for any such challenge had run, a period which could be longer than that required by the ethics rules.

The operational requirement for the authority e-mail is that it be accessible in the event the client requests a copy of the file or to defend a challenge to the settlement. The operational preferences are that the e-mail be easily accessible, that it be removed from any redundant storage media, and that it be destroyed when it need no longer be retained.

In formulating its ESI management plan as a whole, the firm decides to maintain authority e-mail in electronic form. It also decides to maintain the e-mail in a searchable form, rather than image it, for ease of access. The e-mail is

to be stored on a CD-R disc, with the remainder of the file, because the firm concludes that the data stored on that medium is not likely to be subject to significant time-dependent degradation for at least 50 years [9]. An alternative technology subject to a faster time-dependent degradation may render the information inaccessible and fail the legal maintenance requirements.

The authority e-mail is made a part of a checklist for compiling the client file CD-R. The recipient of the authority e-mail is charged with ensuring that the e-mail is maintained in electronic form until it is copied to the file CD-R. After an attorney has reviewed the CD-R for completeness, the authority e-mail is to be removed from the server and other office computers. The backup tapes would be available in the event of an unexpected destruction of the client file CD-Rs. The firm does, however, decide to store the CD-Rs on-site and the backup tapes in the storage facility.

Example 2

A managed care organization that grew significantly over a period of several years into a major national health-care provider network is consolidating its information systems. The organization grew through acquisitions and along the way acquired a number of different information systems running on different platforms. The acquired systems are supported by different vendors and in some cases the original vendors no longer exist, having themselves been acquired. Continued support and maintenance of these disparate systems is very inefficient and challenging for the staff. Management decides to consolidate and upgrade all systems to one modern system per major line of business. A sufficient amount of historical data must be converted to the new system to satisfy the regulatory requirement for data retention.

In the process of testing the conversion, it is discovered that not all historical data elements can be converted without a significant customization of the new system. But that customization would defeat the objective of modernizing and simplifying the system. Several alternatives for satisfying the regulatory requirements are explored, including dumping the data into text reports and storing such reports as ESI. Some concerns are raised that some of the data that is associated with the transactions in the system would not be accessible in the report. Finally, a decision is reached to obtain a limited license from the legacy system vendor that would be used only in the event legacy records that have not been converted to the new system are required.

Endnotes

[1] J. Nicholas Hoover, *The Risky Business of Data Deletion*, INFORMATION WEEK, October 2, 2006.

[2] We believe the advantages of a one-size-fits-all guideline, appropriately customized, outweigh the possible disadvantages of generalization. A number of ESI management guidelines specifically tailored for attorneys and law firms are also available. One reputable source is "The Sedona Conference Working group series, Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age," (2005), http://thesedonaconference.org/TSG9_05.pdf.

[3] 18 U.S.C. § 1500 *et seq.* (2002).

[4] 29 U.S.C. § 1180 *et seq.* (1996).

[5] For operational purposes, industry standards developed by licensing or certification entities may be used for reference or may be required.

[6] Joe Shakey, *To Do List: Rename LaptopFiles "Grandma's Favorite Recipes,"* N.Y. TIMES, *November 7, 2006, at C6.*

[7] For example: University of Colorado System, Administrative Policy Statements, Use of Electronic Mail. *Available at* http://www.cusys.edu/policies/General/email.html.

[8] Destruction is used here to mean unrecoverable by any known forensic means, and not simply deleted from one storage medium. Delete command available in most commonly used software typically removes only the index entry pointing to the data and leaves the data intact.

[9] Optical Storage Technology Association, Technology: Q & A, *Understanding CD-R & CD-RW Disc Longevity. Available at:* http://www.osta.org/technology/cdqa13.htm (last accessed November 15, 2006) .

Part V
ESI in the Courtroom

14

Authentication

Introduction

The requirement that evidence be authenticated is intended to exclude unreliable evidence at trial [1]. ESI covers a wide range on the reliability scale. On the one hand, ESI generated by a computer program without human activation or intervention is "presumptively" unbiased and accurate, so long as the computer is functioning properly [2]. On the other hand, instant message logs can easily be manipulated and counterfeited [3], as can e-mail. The reliability issue is further complicated by the process of preparing ESI for production. For example, opening a Microsoft Word document in order to print or image it for production effects changes from the original, including the creation of new metadata.

These issues may well be resolved if the parties employ appropriate procedures to identify and preserve ESI, and document the chain of custody during the production process, as discussed in Chapter 9. But it must be anticipated, at least for the foreseeable future, that not all parties will have these procedures in place. And disputes will inevitably arise regarding the authenticity of documents produced, even with the assistance of sophisticated software and established document-management vendors. Authenticating ESI obtained from third parties may also be an issue. In this chapter we examine the case law on authenticating ESI, and suggest strategies for securing the necessary foundation for authenticity during discovery.

Cases

"The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims" [4]. In general, the courts look to the traditional bases for authenticating ESI: by personal knowledge, circumstantial evidence, or evidence showing chain of custody [5].

Digital Records, General

A paper document printed from a computerized record can, in general, be authenticated by the testimony of a person familiar with the computerized business record and the circumstances of its printing; testimony from the person who actually prepared the computer record is not generally necessary [6]. For example, in *United States v. Whitaker* [7], on appeal from a conviction on a charge of conspiring to distribute marijuana, the appellate argued that the trial court erred in admitting computer printouts that had not been properly authenticated because the government did not supply a witness who had personal knowledge of the computer system's operation or who could confirm the accuracy of the input to and output from the computer. The court held that a sufficient foundation for admission of the records was established by the testimony of a government agent who described the retrieval of the documents from the computer with a specific software program and who personally participated in printing out the documents [8].

E-Mail and Electronic Text Messages

Personal knowledge and circumstantial indicia of authenticity are the usual bases for showing authenticity of e-mail and text messages [9]. Thus, proffering a witness who can confirm that he or she sent [10] or received [11] an electronic communication may be sufficient to authenticate the evidence although, if contested, additional indicia of authenticity may be required [12]. If the purported author denies writing the e-mail or message, or is unavailable, the following circumstantial evidence is of the type the courts consider in determining whether the communication is admissible:

- The from address is one the purported author customarily uses.
- Testimony from another witness that he/she sent the communication to the purported author at that address.
- Testimony that when the recipient hit the reply function the purported author's e-mail address appeared.
- The e-mail contained the purported author's nickname.

- The e-mail contained the purported author's office address and phone number.
- The content referenced information known to only a few people.
- The content referred to the purported author's activities that were known to have occurred [13].

Another type of personal knowledge sufficient to show authenticity of electronic communications is the testimony of a witness with knowledge of the communication's storage and retrieval systems. For example, in *State of North Carolina v. Taylor* [14], the appellant, who had been convicted of first-degree murder, objected that text messages purportedly sent from him to the victim had not been properly authenticated. The government had introduced the testimony of a Nextel Communications representative who testified that Nextel kept a record of all incoming and outgoing messages to and from its customers, the content of messages, and the times they were received. The manager of the store where the victim had purchased her cell phone testified as to the number of that phone, and further testified that, having authority to access the Nextel database, he had retrieved the text messages to and from that number from Nextel. This testimony, the court held, was sufficient to authenticate the messages as having been sent or received by the victim's cell phone on the dates in question [15].

Internet Content

In general, the courts have demanded more to show that Web content is "what its proponent claims" than is the case for electronic communications, particularly in regard to "personal knowledge" of the information at issue. *St. Clair v. Johnny's Oyster & Shrimp, Inc.* [16], decided in 1999, sounded an alarm that continues to reverberate. In *St. Clair*, in opposition to a motion to dismiss, the plaintiff proffered evidence taken from the United States Coast Guard's online vessel database showing that the defendant owned a particular vessel [17]. The court stated [18]:

> Plaintiff's electronic "evidence" is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing

> contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time.

It should be noted that the court's specific grounds for excluding the evidence proffered was that it constituted inadmissible hearsay [19]. However, the case is also cited in regard to concerns about the authenticity of information posted on the Internet [20].

Thus, the problem of possible adulteration bothered the court in *United States v. Jackson* [21]. In this appeal from a conviction for mail and wire fraud and obstruction of justice, appellant objected to the trial court's exclusion of certain Web site postings. The court of appeals affirmed that ruling.

The alleged relevance of the Web site postings arose from the following facts. Appellant had received four packages from UPS that she claimed were damaged and marred with racial epithets, and she submitted a substantial claim for damages to UPS. Subsequently, several prominent African-Americans received letter packs with a UPS logo containing racially inflammatory material. The government adduced evidence that appellant had fraudulently sent these letter packs as a part of her scheme to substantiate her claim against UPS. In her defense, appellant sought to introduce material posted on the Web sites of white-supremacy groups that took credit for the racist mailings. The government objected that the evidence was properly excluded because it was prejudicial, irrelevant, hearsay, and lacked foundation. The trial court excluded the evidence and the Court of Appeals affirmed, agreeing with the government on all counts. In regard to the lack of authentication, the court stated: "Jackson needed to show that the Web postings in which the white-supremacist groups took responsibility for the racist mailings actually were posted by the groups, as opposed to being slipped onto the groups' Web sites by Jackson herself, who was a skilled computer user" [22].

The fact that "anyone can put anything on the Internet" has led several courts to limit the extent to which testimony as to personal knowledge of the content of Web pages is sufficient to show the authenticity of the information contained therein. In effect, doubt is expressed as to the identity of the sender of the information posted. For example, in *Costa v. Keppel Singmarine Dockyard PTE, Ltd.* [23], in opposing a motion to dismiss for lack of *in personam* jurisdiction, plaintiff offered material from a Web site describing defendant's corporate structure. The site was ostensibly maintained by the defendant. A witness testified that he personally downloaded the pages from the Web site. But because plaintiff did not proffer the testimony of a corporate representative attesting that the information on the Web site was placed there by the corporation, the court declined to consider the information [24]. Similarly, in *Monotype Imaging, Inc.,*

et al., v. Bitstream, Inc. [25], a copyright infringement action, plaintiff proffered pages printed from Web sites, the content of which allegedly evidenced the infringement. The court found the information to be hearsay but, in addition, that it had not been properly authenticated. That is, though an expert testified that the proffered evidence was a "true and accurate" copy of the Web sites at those times, "he was not in a position to confirm the authenticity of the actual information on those Web sites at those times …" [26].

However, in *Perfect 10, Inc. v. Cybernet Ventures, Inc.* [27] the court adopted a more lenient approach [28]. In this trademark and copyright infringement action, Perfect 10 proffered, in support of its motion for a preliminary injunction, a number of exhibits printed from Web pages. The exhibits were supported by declarations reciting that they were "true and accurate copies," and included the dates and Web addresses from which the copies were made. Defendant objected that the exhibits were not sufficiently authenticated. But the court found that with the declarations, in combination with the "circumstantial indicia" of authenticity (dates and addresses), Perfect 10 had met its burden of showing that a reasonable juror could find that the exhibits were what Perfect 10 said they were [29].

Securing the Foundation for Authenticity During Discovery

Digital Records, General

The gold standard for authenticating ESI is to obtain a mirror image of the data that has been identified as being responsive to discovery requests, and computing and recording a cryptographic hash value [30] for each document, file, or disc that is imaged [31]. However, unless production has been requested in native form—and the responding party has made no objection and has reviewed and maintained data in native form to comply with the request—it may not be possible to implement this standard. That is, if the responding party has converted responsive ESI to TIFF or PDF, it would undoubtedly object to mirror imaging of the same information solely for purposes of authentication, and that objection would likely be sustained [32]. And even if the parties have agreed to and are prepared to produce in native form, the responding party will likely object to the obtrusiveness and burden of mirror imaging, as opposed to simply copying the data onto a transferable storage medium. Under these circumstances, it is unlikely that a court would order a responding party to make its facilities available for mirror imaging unless there were some indication that the ESI it was prepared to produce was not authentic [33]. Further, the requesting party would most likely have to pay for the imaging [34]. In sum, even though the gold standard provides the highest assurance of authenticity, it will likely be reserved for those few situations where the authenticity of responsive ESI is

seriously in question and the ESI at issue is key evidence in the case, unless the parties agree upon employing it for their mutual benefit.

Short of the gold standard, the requesting party is basically dependent on the representations of the producing party in terms of the reliability of ESI produced [35]. To what extent the procedures used to produce the ESI need to be thoroughly explored in interrogatories and depositions depends, of course, on the possibility of evidentiary disputes as to authenticity. The producing party is hardly in a position to dispute the authenticity of ESI it has produced. However, if the requesting party has any reason to question the authenticity of what it has received, further inquiry must be undertaken, as is also the case regarding ESI subpoenaed from third parties in order to combat a challenge to the authenticity of that ESI by a party.

E-Mail and Text Messages

Assuming the authenticity of the file, image, or document produced or obtained can be shown as set forth above, authenticating e-mail requires the additional step of showing that the correspondence has been sent or received by the ostensible correspondent. As discussed above, evidence of personal knowledge or circumstantial evidence of authenticity should suffice. However, it should be noted that adducing such evidence may be more difficult than it has been in regard to paper correspondence. Users change e-mail addresses and wireless carriers more frequently than street addresses, and commonly have multiple addresses. E-mail addresses are not uniform: initials, nicknames, numbers, and any combination thereof are used. For this reason, e-mail addresses can be difficult to remember, and more difficult than a street address, such as 222 Poplar Lane. Two years hence, a writer may honestly not be able to confirm that he ever used a particular address, and that writer could not, therefore, authenticate the e-mail based on personal knowledge. Many e-mail and text messages are short and cryptic, making it difficult to recall authorship or receipt.

These potential difficulties in authenticating electronic correspondence through personal knowledge can be avoided or at least minimized by addressing authentication as soon as possible after the correspondence is identified. By interrogatories, requests for admission, preparation of affidavits, or stipulation with opposing counsel, confirm the authenticity of e-mail and text messages upon receipt.

Internet Content

As discussed above, a party proffering information from a Web page may have difficulty showing authenticity based solely on personal knowledge of accessing the page and printing the contents. We believe the more lenient approach, that

would accept such a proffer, is the better view because it is more nearly comparable to that applied in the context of authenticating individualized electronic communications such as e-mail and text messages. That is, the testimony of a witness with knowledge of receiving, or accessing the Web-based information, combined with the URL and date (which is typically displayed on the home page) ought to be sufficient to authenticate the content, hearsay objections being another matter. However, additional foundation evidence could be obtained by issuing a subpoena to the Web-hosting service requesting a copy of the relevant page, assuming the exact URL for the relevant date and time has been correctly copied [36].

Endnotes

[1] *See* Lilly v. Va , 527 U.S. 116, 131 (1999). As noted in Leah Voigt Romano, *Electronic Evidence and the Federal Rules*, 38 LOY. L.A. L. REV. 1745, 1770 (2005), evidence that is "unreliable" may be inadmissible on both authentication and hearsay grounds, and some courts "bypass an explicit authenticity analysis and instead look to the requirements of the hearsay exception to determine whether the proponent has established a proper foundation." *Id.*

[2] *Cf.* Adam Wolfson, *Electronic Fingerprints: Doing Away with the Conception of Computer-Generated Records as Hearsay*, 14 MICH. L. REV. 151 (2005).

[3] *See* Andrew M. Grossman, *No, Don't IM Me—Instant Messaging, Authentication, and the Best Evidence Rule*, 13 GEO. MASON L. REV. 139, 1331 (2006).

[4] Fed. R. Evid. 901(a).

[5] The reported decisions on this issue are still few in number.

[6] *See generally* Karen Reynolds and Landie Landry, *Procedural Issues*, 41 AM. CRIM. L. REV. 973, 992 (Spring 2004).

[7] 127 F.3d 595, 601 (7th Cir. 1997).

[8] *Id.* at 601.

[9] *See* United States v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000), *cert. denied* 2001 U.S. LEXIS 4878 (2001); United States v. Safavian, 435 F.Supp. 2d 36 (D.D.C. 2006); Fenje v. Feld, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003); State of North Carolina v. Taylor, 632 S.E.2d 218 (N.C.App. 2006).

[10] *E.g.,* United States v. Safavian, 435 F. Supp. 2d 36, at 40. n. 2 (D. D.C. 2006).

[11] *E.g.,* People v. Downin, 357 Ill. App. 3d 193 (Ill. App. Ct. 2005) (admission of an e-mail from the assailant to the victim properly authenticated by, *inter alia*, the testimony of the victim that she was the recipient).

[12] *Id.* Appellant, who had been convicted of sexual assault, claimed that, in the absence of any evidence of an Internet provider address linking an e-mail to him, there was no way to tell that the e-mail copy was not falsified by the victim. The court found a sufficient

foundation for the admission of the e-mail based on the following facts: the victim testified she met Downin over the Internet; before and after they met in person, they communicated via e-mail; a detective suggested that the victim send an e-mail to defendant from a public safety building, and she used the e-mail address for him that she had used on all prior occasions; the victim testified that she received a reply from defendant's e-mail address at her e-mail address, the same address defendant had previously used to communicate with her; and the reply e-mail was responsive to the e-mail the victim sent and she testified it contained information known exclusively to her and the defendant.

[13] *See* United States v. Whitaker, 127 F. 3d 601 (7th Cir. 1997).

[14] 632 S.E.2d 218 (N.C. App. 2006).

[15] *Id.* at 230. Appellant also objected that the government had not made a sufficient showing of who had sent and received the messages, but the court held that the content showed sufficient circumstantial indicia of authorship (appellant and victim).

[16] 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999).

[17] It is not clear whether plaintiff made the argument in this case, but the information at issue may have been self-authenticating as a public record pursuant to Fed. R. Evid. 902(5). *See* United States EEOC v. E. I. DuPont de Nemours & Co., 2004 U.S. Dist. LEXIS 20753 (D. La. 2004).

[18] 76 F. Supp. at 774–775.

[19] *Id.* at 775.

[20] *See* United States v. Jackson, 208 F.3d 633, 637 (7th Cir.), *cert. denied*, 531 U.S. 973 (2000).

[21] *Id.*

[22] *Id.* at 638.

[23] 2003 U.S. Dist. LEXIS 16295 (C.D. Cal. 2003).

[24] *Id.* at * 29, *citing* United States v. Jackson, 208 F.3d at 638 and St. Clair, 76 F. Supp. 2d at 775.

[25] 376 F. Supp. 2d 877 (N.D. Ill. 2005).

[26] *Id.* at 885. The court suggested that authenticating the Web pages would require testimony by the operator of the Web site. *Id.* at 884.

[27] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[28] In reaching its decision the court relied largely on United States v. Tank, 200 F.3d 627 (9th Cir. 2000), in which the court considered whether the government had properly authenticated chat room logs that had been downloaded onto a computer. The court found that it had, because the person who had downloaded the information testified as a witness and, further, the entries in the log were connected to the defendant by his own admission that he used one of the screen names contained in the log.

[29] 213 F. Supp. 2d at 1154. *See also* United States EEOC v. DuPont, in which the court found exhibits copied from Web pages had been sufficiently authenticated because they contained the Internet domain name and the date printed; the court had also confirmed

authenticity by accessing the Web address given and confirming the existence of the Web page at issue. Further, the court found that the exhibits were self-authenticating as public records.

[30] A hash value is the functional equivalent of an electronic fingerprint of a specific data set (file, set of files, or complete disc). The hash value is obtained by applying a hash algorithm that records or captures all bits in the dataset. If any bit is subsequently altered, the hash value changes correspondingly, thus confirming or recording the alteration.

[31] A party may also seek to obtain a mirror image of the opposing party's computer hard drives in order to inspect, copy, test or sample ESI in order to identify (or restore, in the case of deleted data) discoverable information. *See* Fed. R. Civ. P. 34(a) and Chapter 4, *supra*. We are here referring to using the same process for purposes of authenticating information that has been reviewed and identified by the responding party as responsive to discovery requests.

[32] *Cf.* India Brewing, Inc. v. Miller Brewing Co., 2006 U.S. Dist. LEXIS 50550 (D. Wis. 2006) (applying Fed. R. Civ. P. 34, if a party requests "documents" and the responding party provides hard copies, the requesting party is not entitled to another set of responsive information in electronic form).

[33] *Cf.* Chapter 4, Form or Production, "Inspect, test or sample."

[34]. *Id.* One could imagine a situation where the evidence of tampering was serious enough that the court would allow mirror imaging to confirm or deny the authenticity of ESI produced at the responding party's expense.

[35] Under certain circumstances—but not always—the requesting party may be able to adduce evidence that supports or disproves representations of authenticity through a forensic analysis. *See* Chapter 7, "Computer Forensics."

[36] Establishing the authenticity of other, specific types of ESI may require other, specific evidentiary foundations. For example, for a thorough description of the specific topic of digital photographs, *see* Joe Kashi, *Hi-Tech In the Law Office*, *Authenticating Digital Photographs as Evidence: A Practical Approach Using JPEG Metadata*, 3 AK BAR RAG 14 (Spring 2006).

15

Hearsay

Introduction

Hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted" [1]. ESI offered as evidence can range from what is obviously hearsay—the content of an e-mail message—to computer-generated data, such as ISP logs of incoming IP addresses [2]. In this chapter we examine the exceptions to the rule excluding hearsay that may be applicable to ESI. We also explore the question of whether, and to what extent, certain types of ESI should not be considered hearsay at all.

Electronically Stored Statements

A statement [3] made by a person and stored electronically is hearsay and must fit within one of the exceptions to be admissible as evidence [4].

E-Mail

Proponents of e-mail in evidence have had a difficult time finding an exception that routinely applies. Even though it is a truism that business today runs on e-mail, those electronic communications regularly fail the business records exception because of a lack of evidence that communications via e-mail are a regular business practice. For example, in *United States v. Ferber* [5], the government sought to introduce an e-mail from an employee to his supervisor that recounted a conversation the employee had with Ferber. There was evidence

that it was the employee's routine practice to send such e-mail, but not evidence that the employer required such records to be maintained. The absence of the latter "was fatal" to the proffer of the e-mail as a business record because "there must be some evidence of a business duty to make and regularly maintain records of this type" [6].

Similarly, in *New York v. Microsoft Corp.* [7], a suit brought by various states alleging antitrust and other causes of action arising from allegations of anticompetitive activities, Microsoft objected to the admission of e-mails written by an employee of RealNetworks describing Microsoft's targeting of RealNetworks' technology. The court agreed with Microsoft that the e-mail did not fit within the business records exception, reasoning [8]:

> The justification for this exception is that business records have a high degree of accuracy because the nation's business demands it, because the records are customarily checked for correctness, and because record keepers are trained in habits of precision. While Mr. Glaser's email may have been 'kept in the course' of RealNetworks regularly conducted business activity, Plaintiffs have not, on the present record, established that it was the 'regular practice' of RealNetworks employees to write and maintain such emails. Indeed, the complete lack of information regarding the practice of composition and maintenance of such emails invokes the final clause of Rule 803(6), which permits exclusion of the evidence where 'the method or circumstances of preparation indicate lack of trustworthiness.' Pursuant to this discretion, the Court declines, on this sparse record, to treat Plaintiffs' Exhibit 1237 as a trustworthy business record.

By way of contrast, in *DirecTV, Inc. v. Murrray* [9], the court found that e-mail recording purchase orders, made at or near the time of the order, and retained as the business record of those orders—as verified by affidavit—fit within the business records exception [10]. The court noted, however, that "[t]he question is a close one …" [11].

Of course, depending on the circumstances, any number of other exceptions may apply. For example, the content of e-mail may constitute an admission or an adoptive admission, show state of mind [12], or qualify as an excited utterance.

Computer Printouts and Databases

The proponent of this type of evidence typically invokes the business or public records exception, or the catch-all exception set forth in Fed. R. Evid. 803(24). The traditional criteria are applied to determine whether the ESI at issue fits the exception.

For example, in *United States v. Trenkler* [13], on appeal from a conviction on various charges arising from a bombing incident, appellant challenged the testimony of a government witness regarding the contents of a database, which testimony allegedly linked appellant to a prior bombing incident. The database had been compiled by an Intelligence Research Specialist with the ATF from reports submitted to ATF by various federal, state and local law-enforcement agencies. The testimony had been admitted pursuant to Rule 803(24), the trial court finding that the fact that law-enforcement agencies relied on the database on a regular basis showed "circumstantial guarantees of trustworthiness." The Court of Appeals held that admitting the testimony was error. In particular, though the ATF agent testified extensively on the reliability of the procedures he used to cull information from the reports, "the government offered virtually nothing establishing the reliability of the underlying reports" [14].

As in *Trenkler*, the unreliability of the underlying data concerned the court in *Potamkin Cadillac Corp., et al. v. B.R.I. Coverage Corp.* [15], as did the method by which it was extracted from the computer. At issue in *Potamkin* was an accounting history created by a program that scanned a database, extracted particular information, and created a printout, proffered by B.R.I. as a business record in support of its counterclaims. The district court accepted the recommendation of the special master excluding the history on the grounds that the proponent's own representative admitted that testing of the history showed that it contained inaccuracies resulting from keypunch errors, misapplication of cash or billings among policies, mislabeling of policies, and miscodings [16]. The Court of Appeals affirmed this evidentiary ruling. Though B.R.I. represented that errors had been corrected, "whether or not these errors were corrected, the fact that they were made suggests that the History required significant selection and interpretation of data, not simply a downloading of information previously computerized in the regular course of business" [17].

Otherwise stated, the accuracy of computer records "may be impaired as a result of incorrect or incomplete entry of data, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions" [18]. Any of these impairments may show that the evidence was not made "in the regular course of business," or that the evidence is "untrustworthy" and not admissible as a business record [19].

But with an appropriate foundation, computer printouts qualify as business records. For example, in *United States v. Salgado* [20], appellants, who had been convicted for conspiring to possess cocaine with the intent to distribute, along with other counts, argued that the trial court erred in admitting telephone toll records from Bell South for numbers subscribed to the alleged conspirators [21]. The trial court had admitted the evidence as business records under Fed. R. Evid. 803(6).

On appeal, the court affirmed [22]. It noted that, in order to be admissible as a business record, evidence must meet four requirements: (1) it must have been made in the course of a regularly conducted business activity; (2) it must have been kept in the regular course of that business; (3) the regular practice of that business must have been to have made the memorandum; and (4) the memorandum must have been made by a person with knowledge of the transaction or from information transmitted by a person with knowledge [23]. "This information must be presented through 'the testimony of the custodian or other qualified witness[.]' Fed. R. Evid. 803(6). Business records meeting these criteria are admissible 'unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.' *Id*" [24].

The first three requirements were met for the computer records at issue, the court held, based on the testimony of a representative from Bell South that the telephone numbers involved in the calls were recorded by computer contemporaneous to the phone call being made, and received and stored in a computer to be downloaded as needed; that it was a regular practice of Bell South to make these reports and keep these types of records; and that the records were relied on by Bell South to ensure accuracy of billing [25].

Appellants objected that the fourth requirement was not satisfied because the actual record was memorialized and entered by the computer itself. Therefore, it could not have been made or transmitted by a person with knowledge. The court rejected that argument by relying on other cases finding that computer-generated records are admissible as business records [26]. Appellants argued that those cases were distinguishable because evidence had been adduced showing that the computers at issue regularly checked for errors, and there had been no such evidence introduced in the case at bar [27]. The court rejected this argument on the grounds that specific evidence of computer reliability did not need to be adduced so long as the business relied upon the computer records, thus implying sufficient accuracy [28].

The other major exception under which computer records are admitted is the public records exception [29]. Under this exception, digital records must originate from "public offices or agencies," and set forth (1) the activities of the office, (2) matters observed as part of office employees' jobs, or (3) factual findings resulting from an investigation conducted by the office [30].

For example, in *United States v. Lopez-Moreno* [31], appellant, who had been convicted of unlawfully transporting undocumented aliens, objected to the trial court's admission as public records of computer printouts showing the dates the passengers had been deported. The Court of Appeals affirmed. "While the computer printouts conceivably could be viewed as containing hearsay statements (statements regarding the passengers' deportations from the United States), they are nevertheless admissible under Fed. R. Evid. 803(8), which

permits the introduction of public records and reports containing hearsay statements" [32].

Computer-Generated Records

There is substantial authority for the proposition that information that is neither created nor maintained by a human—or computer-generated records—should not be considered hearsay [33]. The Tenth Circuit adopted this doctrine in *United States v. Hamilton* [34]. Hamilton had been convicted on various charges arising from his uploading allegedly pornographic images to an Internet newsgroup. The district court had admitted copies of the images and the accompanying, computer-generated header, information that listed information about persons posting to the site including the date and the person's IP address. The trial court found that this information was not hearsay and the Court of Appeals affirmed [35].

> Of primary importance to this ruling is the uncontroverted fact that the header information was automatically generated by the computer hosting the newsgroup each time Hamilton uploaded a pornographic image to the newsgroup. In other words, the header information was generated instantaneously by the computer without the assistance or input of a person. As concluded by the district court, this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition of "hearsay." In particular, there was neither a "statement" nor a "declarant" involved here within the meaning of Rule 801.

Similarly, in *United States v. Khorozian* [36], the Third Circuit held that a header generated by a fax machine was not hearsay because "nothing 'said' by a machine … is hearsay" [37].

In *Hawkins v. Cavalli* [38], a District Court in the Ninth Circuit considered this issue in a habeas corpus proceeding following a conviction in a California state court for accessing a computer without authorization (Hawkins had allegedly stolen source code from his former employer). Hawkins challenged the trial court's admission, over his hearsay objection, of file access dates generated by his computer. The question for the *Hawkins* court was whether the evidence was so unreliable that the petitioner's due process rights had been violated by its admission.

The California Court of Appeals had upheld the admission of that evidence on the grounds that the information constituted the results of the computer's own internal operation and therefore did not constitute hearsay, relying on *State v. Armstead* [39], a Louisiana case. In *Armstead,* the court drew a distinction between "computer-generated" information and "computer-stored"

information. The latter would contain information put into the computer by an out-of-court declarant, and be hearsay. But information reflecting only the computer's own internal operations—computer-generated information—did not constitute a "statement" and was therefore not hearsay, according to the *Armstead* court [40].

The court in *Hawkins* noted that this view of computer-generated information had been adopted not only by the Tenth and Third Circuits but also by evidentiary treatises, citing McCormick [41] and Mueller & Kirkpatrick [42]. And it found support for this view in the Ninth Circuit case, *United States v. Cowley* [43]. In that case the court held that a machine-generated postmark on a letter was hearsay because a postal worker was responsible for setting and causing letters to pass through the machine that affixed the postmark [44]. The postmark was "the postal official's written assertion that the letter passed through his hands at the … post office on a particular day" [45]. Under this reasoning, the *Hawkins* court stated, "the computer printouts here would not be considered hearsay because a human was not responsible for setting and coordinating the computer's recording of access dates. Rather, the access dates were completely computer-generated with no human input" [46].

In his article *Electronic Fingerprints: Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151, 160–64 (2005) [47], Adam Wolfson makes the following arguments supporting the view that computer-generated evidence should not be considered hearsay:

> First, the plain language of the hearsay rule suggests that computer-generated records cannot be considered hearsay because they are not made by a "person" and cannot be "statements" for the purposes of the rule. Most courts have historically excluded from the hearsay rule "statements" made by animals and machines because the nature of their creation does not suggest any unreliability. It is not clear why computer-generated records should be treated any differently.
>
> Second, none of the traditional rationales for excluding hearsay apply to computer-generated records. There is no direct testimony with higher probative value. It is impossible to increase the accuracy of computer-generated data by putting the computer under oath, cross-examining it, or observing its demeanor. Since computer-generated records are not statements, any worries about accuracy will be remedied by a simple authentication of the record and its contents. Furthermore, even if portions of such records are taken out of context, the responding attorney can put them back in context by introducing the rest of the record. Considering that none of the rationales for the hearsay rule relate to authenticated computer-generated records, traditional justifications for excluding hearsay do not apply.
>
> Third, the non-hearsay view, in line with hundreds of years of Anglo-American evidentiary precedent, advocates distinctions based on the

nature, trustworthiness, and probative value of each computer record at issue. This is because lumping wide categories of evidence under the hearsay rule requires that they satisfy an exception to the rule, despite the fact that, as a category of evidence, they may be as reliable as any other non-hearsay items introduced at trial. Such a view is supported by both the hearsay rule's principal justifications and more recent additions to the corpus of evidentiary law. Moreover, these principles accurately judge the probative weight that computer-generated records deserve.

Since the hearsay rule is predicated on the untrustworthiness of out-of-court statements, the main concern is whether computer-generated records are trustworthy if properly authenticated. Several characteristics of these records lead to the conclusion that, indeed, they are trustworthy and undeserving of the hearsay label. Businesses, the government, and the average layperson utilize computer-generated records because they are reliable, and, more importantly, they offer an unbiased, accurate portrayal of certain exchanges that occur between computers and humans. Computer-generated records should thus be considered legally reliable because of the nature in which they were created and because this same process eliminates any question of accuracy beyond a preliminary inquiry into the authenticity of the records themselves.

Any inaccuracies found in computer-generated records are not the type the hearsay rule is designed to catch. Whereas a Word document is a mechanism for recording assertions made by a person, a computer-generated record, much like a photograph or sound recording, merely captures information about the state of the world at a particular moment. Although these records may be inaccurate or misleading, as noted by Judge Van Graafeiland in *Perma Research* [*v. Singer Co.,* 542 F.2d 1111 (2d Cir. 1976)(dissenting)], the inaccuracies are best caught by the authentication process, rather than by cross-examining the computer itself. Since the ultimate concern in admitting these types of evidence is authentication, computer-generated records warrant the same treatment.

Fourth, classifying computer-generated records as hearsay may often frustrate the purpose of promoting accurate fact finding for computer crimes like electronic terrorism, internet stalking, computer trespass, and electronic spoliation because it may prohibit highly relevant and trustworthy evidence regarding the crime. While this is a justification based more on policy considerations than it is based on the hearsay rule or evidentiary rules, it suggests that the hearsay rule's justifications may be outweighed by countervailing interests. Furthermore, this rationale exhibits why it is so important to correctly classify computer-generated and computer-stored records: computers are used more and more in business and at trial; evidentiary rules must keep pace.

Finally, the core of the hearsay position is based on an outdated conception of computers and the nature of the records they create, and the minority position is not. *Perma Research* was decided in 1976, and the

> majority of subsequent foundational decisions were handed down twenty years ago. Hearsay courts have not seen fit to question or reexamine these precedents. This is not to say that these results are wrong. In fact, *Perma Research* and its progeny aptly recognize the danger of believing that all computer records are admissible and free from hearsay. The current hearsay conception, however, is based on a notion of computers that does not account for independent activity and recordkeeping, which are often free from any human interaction. Simply delineating between the two types of records would allow these courts to keep their current precedent, but also include a view of computer records that rightly foregoes a hearsay analysis for trustworthy, reliable pieces of evidence contained in computer-generated records.

Though these arguments, and the reasoning of the courts in *Armstead*, *Hamilton*, and *Khorozian* are reasonable, there are problems with attempting to divide ESI into computer-generated and computer-stored categories. For one, as noted by Wolfson in his article, there is a grey area between these two categories that "often confuses judges and attorneys alike" [48]. Wolfson gives as an example a record copied from a computer that contains a statement by the author but also metadata related to the statement that was generated by the computer: should the entire document be classified as hearsay [49]? A more fundamental problem with the very conception of describing evidence as computer-generated is the fact that all computer data is created or at least instigated by a human, at least at some remove. An IP log generated by an ISP's computer was created by software code designed by human beings. Certainly the connection between that code and the log of an Internet access on a particular date and at a particular time is a long chain comprised of many links. But how many steps back must any human intervention have taken place to qualify data as computer-generated? And what would be a workable test that judges could use to decide the issue?

Wolfson proposes an electronic fingerprint test, as follows (citations omitted) [50]:

> The approach proceeds as follows. First, when computer records are introduced, a judge must ask if the purpose of the records is to establish the existence of a transaction by a mechanical or digital object, whether a computer, an ATM card, a telephone number, or some other tangible object. This is a threshold question based on judicial economy; it is easy to answer and gives an accurate view of the record's likely admissibility in one broad swath. If, for example, a prosecutor wishes to introduce an IP log in order to demonstrate that the defendant's computer signed on a network at specified times, this is presented in order to identify the computer conducting pertinent activity on an internet network; therefore, the records are relevant based on identification purposes.

> Second, the judge must decide whether the piece of computer evidence constitutes an "electronic fingerprint" or, instead, an out-of-court statement. In order to accomplish this goal, the judge must evaluate the nature of the offered record itself. Specifically, the judge must ask if the record is an assertion or the preservation of an electronic transaction. If the record is the result of a computer's sole operation, the purpose must be the presentation of the transaction in question. If there was human interaction, what was the assertive quality of the interaction that created the record? Essentially, this analysis is used to determine whether the record is an assertion or if it is the equivalent to the mark left behind when a person holds a tactile object. A hearsay analysis is only appropriate in the former case.

Applying this test to a Microsoft file and its associated metadata, Wolfson explains, the file would be computer-stored and hearsay. But the metadata—though it came into being only because a person acted to create the file—would not be hearsay because it is not "assertive," according to Wolfson's analysis [51].

But what of an e-mail sent as an out-of-office autoreply? The autoreply is the record of a transaction between the ISP and the IP address of the sender. The transaction occurred because the autoreply feature was activated by the sender of the e-mail, so there was human interaction in the creation of the record. And it could certainly be argued that the sender was asserting that he or she was not in the office. But in fact the message was simply sent by the computer, again implicating the reasoning that a computer cannot make a statement that would constitute hearsay.

Another issue that should be considered is the ease with which ESI, including ostensibly computer-generated records can be altered and simulated. A person can send an out-of-office autoreply manually, while sitting in the office, or send an e-mail with a computer-generated send date of last Christmas, though the message was actually sent on the Fourth of July. This problem of unreliability is not solved by the requirement that a record be authenticated: a copy of the faked out-of-office autoreply would be an authentic record. The content would just be misleading, a defect which the rules excluding hearsay were designed to prevent, or at least minimize. A sophisticated computer forensics examination would probably clarify the facts. But it seems a large burden to place on a party objecting to the admission of information generated by a computer that it must obtain that computer and pay to have it analyzed else its objection will be automatically overruled.

Otherwise stated, with all due respect to Wolfson's creative electronic fingerprint test, it does not satisfactorily distinguish between computer-generated and computer-stored evidence. But given the complexity of ESI, and the ever-changing technologies with which ESI is created, it seems unlikely that a reasonable bright-line test could be devised. The electronic fingerprint test also

slides down the slippery slope of viewing computer-generated information as inherently reliable, when more skeptical critics would argue that there is human activity (with all its inherent motivations, complexities, and failures) behind (though sometimes far behind) the computer-generated data.

The better view on this issue would seem to be that so-called computer-generated records should nonetheless be subject to the hearsay rules. Wolfson argues that one reason computer-generated records should not be considered hearsay is that otherwise certain crimes such as Internet stalking and computer trespass would be difficult to prove. But if the elements of those crimes cannot be proven by evidence that passes the hearsay bar because it is a business record [52], a party admission, or fits within another exception—the catch-all exception of Rule 807 would be a likely candidate for much data that is truly computer-generated—perhaps it is simply not reliable enough to pass muster. And as for the objection that a record generated by a computer cannot be a statement, perhaps that objection should be overruled in consideration of two facts. Computers generate whatever information people program those computers to produce; that information is therefore in some regard the statement of a declarant. And in this day and age, vast swaths of the American population make most of their written statements via a computer. If one starts trying to sort out which of those statements are assertive and which not, the hearsay rules could become largely meaningless.

Of course, just because computer-generated data would be subject to the hearsay rules does not mean that it would necessarily be excluded as evidence at trial. The proponent always has the opportunity to demonstrate to the court why the data in question falls within a hearsay exception. If the proponent passes the threshold test of showing that one of the exceptions applies, the burden shifts to the opposing party to show why the provenance of the data makes it suspect. And of course, counsel may stipulate to admissibility.

Endnotes

[1] Fed. R. Evid. 801(c).

[2] It is assumed for purposes of the following discussion that the evidence is being offered for the truth of the matter asserted.

[3] Fed. R. Evid. 801(c) defines a "statement" as "(1) an oral or written assertion, or (2) nonverbal conduct of a person, if it is intended as an assertion."

[4] *See, e.g.,* United States v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (e-mail messages); United States v. Lopez-Moreno, 420 F.3d 420, 436 (5th Cir. 2005) (dates of deportation contained in computer printouts); United States v. Trenkler, 61 F.3d 45 (1st Cir. 1995) (reports of arson and explosives incidents in ATF database); United States v. Zapata, 356 F. Supp. 2d 323, 328 (S.D.N.Y. 2005) (Western Union send orders contained in

database); *cf.* Adam Wolfson, *Electronic Fingerprints: Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151 (2005).

[5] 966 F. Supp. 90 (D. Mass. 1997).

[6] *Id.* at 98 (citations omitted). The e-mail was, however, admitted as a "present sense impression" as discussed *infra.*

[7] 2002 U.S. Dist. LEXIS 7683 (D. D.C. 2002).

[8] *Id.* at *8, 9 (internal citations omitted).

[9] 307 F. Supp. 2d 764 (D. S.C. 2004).

[10] *Id.* at 772.

[11] *Id.* The court noted that by showing the e-mail fit the business records hearsay exception, the proponent had at the same time solved the authentication issue pursuant to Fed. R. Evid. 902.

[12] *See, e.g.,* United States v. Safavian, 435 F. Supp. 2d 36.

[13] 61 F.3d 45 (1st Cir. 1995).

[14] *Id.* at 59. The court noted that the database came closest to falling within the public records exception, but for the restrictions within that rule regarding the admission of police reports and similar records in a criminal prosecution. See Fed. R. Evid. 803(B) and (C).

[15] 38 F.3d 627 (2nd Cir. 1994).

[16] *Id.* at 633. The special master had also considered B.R.I.'s refusal to make the master record available in discovery in ruling that the history was not admissible, and the court approved of including this factor.

[17] *Id.* There was also evidence that the history was work product and, therefore, not a business record.

[18] *Manual for Complex Litigation*, 21.446, *Discovery of Computerized Data,* Federal Judicial Center (Third) at 79.

[19] Evidence that is unreliable is presumably inadmissible on both authentication and hearsay grounds. Some courts "bypass an explicit authenticity analysis and instead look to the requirements of the hearsay exception to determine whether the proponent has established a proper foundation." Leah Voigt Romano, *Developments in the Law: VI. Electronic Evidence and the Federal Rules,* 38 LOY. L.A. L. REV. 1745, 1770 (2005).

[20] 250 F.3d 438 (6th Cir. 2001).

[21] The records contained subscriber-line information, including the subscriber's name, the location where the telephone was installed, the date and duration of local and long-distance telephone calls, the numbers from which calls were placed and at which they were received, and billing amounts.

[22] It should be noted, in regard to the discussion at the text accompanying n. 31 *et seq.* that the Court of Appeals did not hold that the records at issue constituted hearsay. The issue on

appeal was whether the district court's admission of the evidence as business records was erroneous.

[23] *Id.* at 451 (citations omitted).

[24] *Id.*

[25] *Id.* at 452.

[26] *Id.*

[27] The Bell South representative had testified that he did not know the error rate in the billing recording system or how it was checked for accuracy.

[28] 250 F.3d at 453. The court also rejected appellant's argument that the witness did not have sufficient knowledge because he had not programmed the computer or obtained the records himself. The witness, the court held, had demonstrated sufficient familiarity with Bell South's recordkeeping system.

[29] Fed. R. Evid. 803(8). *See* Ronald J. Marzullo-La Russa, *Computer-Generated Evidence: Admissibility*, 20 REV. JUR. U.P.R. 121, 129 (1985).

[30] *Id.*

[31] 420 F.3d 420 (5th Cir. 2005).

[32] *Id.* at 435.

[33] *But see, e.g.,* United States v. Salgado, n. 20, *supra.* It should be noted, however, that the court in *Salgado* did not hold that the telephone logs at issue constituted hearsay. The issue on appeal was whether the trial court had properly admitted the records under the business records exception.

[34] 413 F.3d 1138 (10th Cir. 2005).

[35] *Id.* at 1142.

[36] 333 F.3d 498 (3rd Cir. 2003).

[37] *Id.* at 505.

[38] 2006 U.S. Dist. LEXIS 73143 (N.D. Cal. 2006).

[39] 432 So. 2d 837 (La. 1983).

[40] *Id.* at 840.

[41] *McCormick on Evidence*, § 294(b), at 447 (John W. Strong, ed., 5th ed. 1999).

[42] Federal Evidence, § 380, at 65 (2nd ed. 1994).

[43] 720 F.2d 1037 (9th Cir. 1983).

[44] *Id.* at 1044.

[45] *Id.*

[46] 2006 U.S. Dist. LEXIS 73143, at *38 (N.D. Cal. 2006). The court further noted that, even if the printouts were hearsay, they would likely fall under the residual hearsay exception due to their "high degree" of reliability. *Id.*

[47] *Reprinted with permission from* MICHIGAN LAW REVIEW, October 2005, Vol. 104, No. 1. Copyright 2005 by the Michigan Law Review Association (citations omitted). The authors do not necessarily agree with Mr. Wolfson's description of the view that computer-generated records are not hearsay as the minority position, as stated in the reprinted section of his article.

[48] Wolfson, *Electronic Fingerprints*, n. 4, *supra*, at 165.

[49] *Id.* at 165–66.

[50] *Id.* at 167–68.

[51] *See id.* at 168.

[52] In this regard, we would disagree with Wolfson's conclusion that a company's record of a security breach in its computer network would constitute inadmissible hearsay, an example he gives of the alleged problem with failing to distinguish between computer-generated and computer-stored records. It seems more likely that the proponent of that evidence could readily demonstrate that the record was (1) made in the course of a regularly conducted business activity; (2) kept in the regular course of that business; (3) made as the result of the regular practice of the business to maintain such records; and (4) maintained by a person with knowledge of the record-keeping. As such, it would be admissible as a business record.

16

Preservation Orders

Introduction

Orders requiring the preservation of ESI are becoming increasingly common [1]. The scheduling order may include what measures to preserve ESI the parties have agreed upon in a discovery planning conference [2]. The court may *sua sponte* raise the issue of preservation early in the litigation, and seek agreement by counsel as to what steps shall be taken or resolve the issue if disputed [3]. The court may also grant the motion of a party for a preservation order.

This chapter examines the different standards applied in ruling on a motion for a preservation order over objection by the responding party. The facts of representative cases are examined in detail to illustrate how those standards are applied. Following the analysis of the case law are suggested approaches for crafting a proposed preservation order, for using discovery to monitor compliance, and a sampling of preservation orders.

Standard of Review

In general, the standard of review of a motion for an order requiring the preservation of ESI is the same as that applied to paper documents. The difference in analyses is not between paper and ESI, but among the differing standards that various jurisdictions have adopted.

Some courts have taken the position that a party seeking a preservation order must meet the relatively onerous standards for obtaining injunctive relief. For example, in *Madden v. Wyeth* [4], a drug products liability case, plaintiffs sought an order requiring defendants to preserve all documents, whether in

paper or electronic format, and suspend all routine destruction of documents: recycling backup tapes, deleting e-mail automatically, and reformatting computer hard drives. The court held that a motion to preserve evidence is equivalent to seeking an injunctive remedy which would, therefore, issue only upon a showing that equitable relief was warranted [5].

Other courts have criticized this reasoning. As stated by the court in Pueblo of Laguna v. United States [6]:

> The court … believes that the more recent of these decisions [requiring a showing sufficient to grant injunctive relief] ignore significant changes made to the Federal Rules of Civil Procedure since the 1960s, further establishing the case management powers of judges. In the court's view, a document preservation order is no more an injunction than an order requiring a party to identify witnesses or to produce documents in discovery. While such pretrial and discovery orders take the basic form of an injunction (an order to do or not to do something), the decisional law suggests that, in issuing them, courts need not observe the rigors of the four-factor analysis ordinarily employed in issuing injunctions (citations omitted).

Another consideration for rejecting the traditional injunctive test before a preservation order is issued is that imposing that higher burden conflicts with the fact that the Federal Rules of Civil Procedure impose preservation obligations on litigants in every civil action filed, automatically and without court review [7]. Finally, courts have noted that requiring a plaintiff to demonstrate a likelihood of success on the merits—typically one factor to be considered in determining whether to issue injunctive relief—when deciding whether to protect documents that may evidence the merits of the case is decidedly to put the cart before the horse [8].

One alternative to the injunctive relief standard is a two-pronged test: a party seeking a preservation order must demonstrate that it is necessary and not unduly burdensome [9]. To meet this standard the proponent ordinarily must show that, absent a court order, there is significant risk that relevant evidence will be lost or destroyed, a burden often met by demonstrating that the opposing party has lost or destroyed evidence in the past or has inadequate retention procedures in place [10]. The proponent must also show that the particular steps to be required to preserve evidence will be effective, but not overbroad or unduly burdensome [11].

Other courts use a balancing test, or weigh multiple factors in determining whether a preservation order should issue. For example, in *Treppel v. Biovail* [12], the court adopted a three-part balancing test, considering (1) the danger of destruction, (2) content of destroyed documents, and (3) burden of preservation in ruling on a motion for a preservation order [13]. The difference between these two tests—what the moving party must show with regard to the content of

the documents at issue—may be "more apparent than real" [14]. That is, under the two-part approach, the content of the documents at risk of destruction must still be considered because that content must be relevant. But the balancing test "suggests a more specific demonstration of the importance of the evidence," though content is but one factor to be considered along with others [15].

A fourth approach taken by some courts is to deny a request for a preservation order so long as the responding party has represented that it is in fact complying with its duty to preserve evidence. For example, in *Winig v. Cingular Wireless LLC* [16], without enumerating any specific standard for review, the court denied plaintiff's request for a preservation order because the defendant "expressly assured" plaintiff that it had taken steps necessary to preserve all relevant information. The defendant further proffered that it intended to comply with the recent amendments to the Federal Rules of Civil Procedure with respect to electronic data [17]. In particular, when a party is obligated by statute, in addition to the general duty to preserve evidence, the courts seem disinclined to enter a preservation order over objection, at least absent any showing that evidence has been lost [18].

But the opposite approach was taken by the court in *Al-Marri v. Bush* [19]. Petitioners in this *habeas corpus* proceeding filed a motion for an order requiring the respondents "to preserve and maintain all evidence and information regarding the torture, mistreatment, and abuse of detainees at Guantanamo Bay." The respondents argued that petitioners had failed to meet the standards for issuing a preliminary injunction. Citing *Pueblo of Laguna v. United States*, the court held that the petitioners need not meet such a standard in seeking a preservation order. As for the merits of the motion, because the respondents had represented that the evidence would not be destroyed, the court found that "entering a preservation order will inflict no harm or prejudice upon them," and issued the order [20].

Finally, in *Crown Park Corp. v. Dominican Sisters* [21], plaintiff moved ex parte for an order to preserve electronic and work product discovery. The court ruled that such an order was unnecessary, in light of the defendant's duty to preserve evidence and the "panoply of sanctions" available to enforce that duty. The *Crown Park* court also viewed the motion as premature since the parties had not met to discuss preservation issues. The court denied the motion but entered the following order [22]:

> A. On or before April 28, 2006, the parties shall engage in meet and confer discussions regarding the production of electronic documents in this case. The meet and confer discussions will be attended by an electronic document consultant retained by Defendant who will have sufficient knowledge of Defendant's electronic documents to enable Defendant to participate in a good faith effort to resolve all issues regarding the production of electronic

documents without court action. The meet and confer discussions also will be attended by an electronic document consultant retained by the Plaintiff who will have sufficient knowledge of the Plaintiff's electronic documents to enable the Plaintiff to participate in a good faith effort to resolve all issues regarding the production of electronic documents without court action.

B. Except as set forth in the next sentence, any electronic document consultant who personally attends any meet and confer regarding the production of electronic documents in this case shall not be subject to discovery requests, including requests for depositions, until such time as the parties otherwise agree or this Court orders that such discovery may be taken. If any such electronic document consultant provides testimony on an issue or issues in this case, whether by affidavit, declaration, deposition, or otherwise, he or she may be subject to discovery requests, including requests for depositions, limited to the issue or issues that are the subject of his or her testimony.

C. If after conferring to develop a preservation plan, counsel do not reach an agreement on the material aspects of preservation, the parties are to submit to the undersigned within three days of the conference a statement of unresolved issues together with each party's proposal for their resolution of the issues. The undersigned will consider the statements in framing an order regarding the preservation of documents, data and tangible things.

Standards Applied: Representative Cases

Injunctive Relief

Madden v. Wyeth [23]. Plaintiff claimed that a preservation order was justified because of the possibility that defendants would unintentionally or intentionally destroy or lose relevant materials. The court, applying an injunctive relief approach, found that the plaintiffs had not met their burden of showing a likelihood of harm from the destruction of evidence: defendants were obligated to take "appropriate measures" to preserve documents and plaintiffs had not proven, or even alleged, that defendants had or would fail to comply with that obligation [24].

Two-Part Test

Pueblo of Laguna v. United States [25]. In showing a sufficient risk of destruction, the plaintiff relied on another pending case in which the trial court found that several agencies of the federal government had mishandled and destroyed records, including electronic records, related to Indian tribes. Though the documents at issue in the two cases were different, several of the agencies responsible for document management were involved in both cases. And because the

agencies' failures in the other case had been "so pervasive and systematic," the court in Pueblo found that a preservation order was well justified [26].

The plaintiff tribe sought an order that would prohibit the destruction of records relevant to the case absent its prior written concurrence or further order from the court. It also requested the court to impose restrictions on the inter- and intra-agency transfer of such records by requiring that plaintiff be offered an opportunity to examine such records prior to their movement. The court found that there would be little purpose to imposing the prior concurrence measure because concurrence would never be sought: either the documents would be preserved or inadvertently destroyed. The court found that the proposed transfer restrictions would unduly burden the agencies' operations.

In lieu of the other measures proposed by the Tribe the court ordered the defendant to: (i) preserve all the documents, data and tangible things in question; (ii) index all the documents, data and tangible things reasonably anticipated to be subject to discovery in this case; and (iii) report immediately any destruction or loss of records. In regard to compliance with the order, the court stated: "In the court's view, the looming specter of sanctions—which the case law suggests may be severe, to and including the entry of a default judgment—provides the incentive, albeit in a negative way, needed to effectuate this preservation plan" [27]. (Citations omitted.)

Balancing Test

Treppel v. Biovail [28]. The court denied plaintiff's motion for a preservation order because plaintiff had not shown that any discoverable evidence had been destroyed. Nor did it appear that evidence was at risk of destruction, because the defendant had created a backup of its servers and images of the hard drives of the laptops of persons likely to have discoverable information. And because the plaintiff had not demonstrated that any documents had in fact been destroyed, he necessarily had failed to identify the content of such documents. In this regard, the court noted [29]:

> To be sure, it is not incumbent upon the plaintiff to show that specific documents were lost. It would be enough to demonstrate that certain types of relevant documents existed and that they were necessarily destroyed by the operation of the autodelete function on Biovail's computers or by other features of its routine document retention program. But the plaintiff has not yet made even the most basic showing that any documents potentially relevant to this litigation were lost.

As for the third factor—the burden of the requested preservation—the court noted that the plaintiff had requested a blanket preservation order, or that defendant be ordered "to securely maintain, and not destroy or delete, to the

extent that they currently exist and may contain potentially discoverable information: (i) electronic data, including email data, whether on back-up tapes, computer hard drives, servers, PDAs, Blackberries, or other physical media and (ii) network Back-Up Tapes, created during the Relevant Period (together, the 'Back-Up Tapes'')." Because plaintiff had failed to provide any information as to the burden this would impose, the consideration of this factor also weighed against granting the motion [30].

United States ex rel. Smith v. Boeing Co. et al. [31]. Plaintiffs-Relators brought this *qui tam* action alleging that Boeing and one of its subsidiaries filed false claims with the U.S. government. In ruling on a motion to preserve evidence, including both paper documents and electronically stored information, the court stated that it would be guided by "principles of equity," including consideration of the following factors: (1) how much of a concern there is for the maintenance and integrity of the evidence in the absence of an order; (2) any irreparable harm likely to result absent a specific order directing preservation; and (3) the capability of the party to maintain the evidence sought to be preserved [32]. In support of their argument that evidence was at risk of destruction, the relators cited past conduct including evidence that Boeing concealed certain information from the government and that the subcontractor used two sets of books for government contracts. Boeing disputed these allegations, and also produced evidence that it had taken steps to preserve all evidence relevant to the lawsuit "within days" of finding out about the suit. The court concluded that no showing had been made of a "significant threat" that documents would be lost or destroyed absent an order, and that an order would not serve "any useful purpose in light of the parties' existing legal obligations to preserve relevant evidence" [33]. As for the third factor, the court noted, Boeing clearly had the capacity to preserve the evidence in question.

Drafting Proposed Preservation Orders

Many parties will begin with a model preservation order taken from another case or from available reference materials. The models described in Chapter 7 for planning discovery can be used to confirm the completeness of that model. Those models also provide a framework for crafting a proposed order best tailored for the anticipated discovery [34]. Thus, one can confirm that the following sample preservation order includes the where, (Definitions, Nos. 4, 5, 7, and 14), a checklist of types of data (Definitions, Nos. 1, 3, 11, 12, 13, 16, and 18), data throughout its life cycle (Order, Part D), and a revised refer or relate provision (Definitions, No. 6).

From *Westcoat v. Bayer Cropscience LP*, 2006 U.S. Dist. LEXIS 79756 (E.D. Mo. 2006), entered with the consent of the parties:

I. DEFINITIONS

For the purposes of this Document Preservation Order and thereafter in this litigation, the following definitions shall apply:

1. The term "Active File" means any electronic data file that can be used by an electronic data processing system in any manner without modification or reconstruction. An Active File is any electronic data file that has not been deleted or otherwise destroyed and/or damaged and which is readily visible to the operating system and/or the software with which it was created.
2. The term "Bayer" refers to Bayer CropScience LP, as well as subsidiaries and agents thereof. The Parties currently dispute whether Bayer AG is a properly served party and subject to the personal jurisdiction of this Court. The Parties agree that if Bayer AG is determined by the Court to be a properly served party and subject to personal jurisdiction, that the Parties will meet and confer regarding the scope of Bayer AG's preservation obligations. In the meantime, and if Bayer AG is determined not to have been properly served or not subject to personal jurisdiction, the Parties agree that Bayer AG's preservation obligations are governed by applicable law.
3. The term "Communication(s)" means the transmission, sending, or receipt of information of any kind (in the form of facts, ideas, inquiries, or otherwise), by or through any means including, but not limited to, speech, writings, language (machine, foreign or otherwise), computer electronics of any kind (including, but not limited to, e-mail, or instant messaging), magnetic tape, videotape, photographs, graphs, symbols, signs, magnetic or optical disks, floppy disks, compact discs, CD-ROM discs, other removable or transportable media, sound, radio, or video signals, telecommunication, telephone, teletype, facsimile, telegram, microfilm, microfiche, photographic film of all type, or other media of any kind.
4. The term "Computer" shall include, but is not limited to, microchips, microcomputers (also known as personal computers), laptop computers, portable computers, notebook computers, palmtop computers (also known as personal digital assistants or PDAs), minicomputers, and mainframe computers.
5. The term "Computer System," when used in reference to any computer, includes, but is not limited to, the following information: (a) computer type, brand and model; (b) brand & version of all software, including operating system, private- and custom-developed applications, commercial applications, or shareware; and (c) communications capability, including asynchronous or synchronous, including, but not limited to, terminal to mainframe emulation,

data download or upload capability to mainframe, and computer to computer connections via network modem or direct connection.

6. The term "Concerning" means evidencing, reflecting, incorporating, effecting, including, or otherwise pertaining, either directly or indirectly, or being in any way logically or factually connected with, the subject matter of the inquiry or request.
7. The term "Configuration," when used in reference to any computer, includes, but is not limited to, the following information: (a) computer type, brand, model and serial number; (b) brand and version of all software, including operating system, private and custom developed applications, commercial applications, shareware, or work-in-progress; and (c) communications capability, including asynchronous and/or synchronous, and including, but not limited to, terminal to mainframe emulation, data download or upload capability to mainframe, and computer to computer connections via network, modem, or direct connect.
8. The term "Custodian" refers to any officer, director, employee, or agent of the Parties known or believed to possess Potentially Relevant Information.
9. The term "Data" is equivalent to the term "Electronic Data" as defined herein.
10. The term "Defendants," refers to all of the defendants in this case, and their officers, directors, agents, employees, members, representatives, and attorneys.
11. The term "Deleted file" means any electronic data file that has been deleted or deleted from the electronic media on which it resided, including but not limited to any file whose File Allocation Table (FAT) entry has been modified to indicate the file as being deleted and/or which is not readily visible to the operating system and/or the software with which it was produced.
12. The term "Document(s)" is synonymous and equal in scope to usage of this term in Fed. R. Civ. P. 34(a) and to the terms "[w]ritings and recordings," "photographs," "original" and "duplicate" defined in Fed. R. Evid. 1001. Document means the original (or an identical duplicate if the original is not available), and any non-identical copies (whether non-identical because of notes made on copies or attached comments, annotations, marks, transmission notations, or highlighting of any kind) of writings of every kind and description that are fixed in any medium upon which intelligence or information can be recorded or retrieved—including, but not limited to documents fixed in tangible media or electronically or digitally stored on disk or tape in a native format. This includes, without limitation, all Electronic Data, as defined below (including personal computers, laptop computers, hand held computers, and

all other types of computers), network, or electronic media, including, but not limited to, Active Files (including any file of electronic data that can be used by an electronic data processing system), as well as hard disks, floppy disks, compact discs, and magnetic tapes of any kind, computer memory, optical media, magneto-optical media, and other physical media on which notations or marking of any kind can be affixed. "Document(s)" further includes deleted files, or file fragments, and also includes, without limitation, the original and each copy regardless of origin and location, or any book, pamphlet, periodical, letter, memorandum, diary, calendar, telex, electronic mail message, instant message, telegram, cable, report, record, contract, agreement, study, handwritten note, draft, working paper, chart, paper, print, record, drawing, sketch, graph, index, list, tape, stenographic recording, tape recording, computer diskette or data, photograph, microfilm, invoice, bill, order form, receipt, financial statement, accounting entry sheet or data processing card, or any other written, recorded, transcribed, punched, taped, filmed, or graphic matter, however produced, reproduced, or stored, which is in your possession, custody, or control or which was, but is no longer in your possession, custody, or control. The term "Document(s)" also includes, without limitation, all "Communications" (as defined above), and all inquiries, discussions, conversations, correspondence, negotiations, agreements, understandings, meetings, notices, requests, responses, demands, complaints, or press, publicity, or trade releases.

13. The term "Electronic Data" means the original (or identical duplicate when the original is not available), and any non-identical copies (whether non-identical because of notes made on copies or attached comments, annotations, marks, transmission notations, or highlighting of any kind) of writings of every kind and description whether inscribed by mechanical, facsimile, electronic, magnetic, digital, or other means. Electronic data includes, by way of example only, computer programs (whether private, commercial or work-in-progress), programming notes or instructions, activity listings of electronic mail receipts or transmittals, output resulting from the use of any software program, including word processing documents, spreadsheets, database files, charts, graphs and outlines, electronic mail, instant messaging, operating systems, source code of all types, peripheral drivers, batch files, ASCII files, and any and all miscellaneous files or file fragments, regardless of the media on which they reside and regardless of whether such electronic data consists in an Active File, deleted file, or file fragment. Electronic data includes any and all items stored on computer memories, hard disks, floppy disks, CD-ROMs, DVDs, removable media such as Zip disks, Snap servers, Jaz cartridges, and their equivalent,

magnetic tapes of all types, microfiche, punched cards, punched tape, computer chips, on or in any other vehicle for digital data storage or transmittal. The term electronic data also includes the file, folder tabs or containers and labels appended to, or associated with, any physical storage device associated with each original or copy thereof.

14. The term "Electronic Media" means any magnetic or other storage media device used to record electronic data. Electronic media devices may include, but are not limited to, computer memories, hard disks, floppy disks, Snap servers, DVDs, CD-ROM, and removable media and their equivalent, magnetic tapes of all types, microfiche, punched cards, punched tape, computer chips, or on or in any other vehicle for digital data storage or transmittal.
15. The term "Employee(s)" means any person who acted or purported to act on behalf of another person or persons, including, but not limited to, all past and present directors, officers, executives, agents, representatives, attorneys, accountants, independent contractors, advisors, and consultants of such other person or persons.
16. The term "File Fragment" means any electronic data file that exists as a subset of an original Active File. A file fragment may be active or deleted. The cause of fragmentation can include, but is not limited to the execution of ordinary file management routines such as the creation of new files over parts of previously deleted files, the creation of files on disks which do not have enough contiguous blocks to write the file from beginning to end, where the file has been split up between several sections of the disk (each piece a fragment). Other causes include manual intervention, electronic surges, or physical defects on electronic media.
17. The term "LLRICE601," "LLRICE601" and "LibertyLink Rice," for purposes of this order only, refers to a type of genetically-modified ("GM"), glufosinate-tolerant, rice seed developed and/or field-tested beginning in or about 1998.
18. The term "Native Format" means the default format of a data file created by its associated software program. For example, Microsoft Excel® produces its output as '.xls' files by default, which is the native format of Excel. Microsoft Word® produces native files with a '.doc' extension, which is the native format of Word.
19. The term "Network" means any hardware or software combination that connects two or more computers together and which allows the computers to share or transfer data between them. For the purposes of this definition, the connection between or among the microcomputers need not be either physical or direct (i.e., wireless networks, and sharing or transferring data via indirect routes utilizing modems and phone company facilities). In addition, there need

not be a central file or data server nor a central network operating system in place (i.e., peer-to-peer networks and networks utilizing a mainframe host to facilitate data transfer).

20. The term "Plaintiff(s)" refers to the named plaintiffs in this litigation, individually and on behalf of the proposed class defined in the operative complaint filed herein.
21. The term "Policy" means any rule, procedure, practice, or course of conduct, whether formal or informal, written or unwritten, recorded or unrecorded, which was recognized or followed, explicitly or implicitly, by Bayer.
22. The term "Potentially Relevant Information" means a document or material containing information within the scope of the categories set forth in paragraph II(A) below.
23. The term "Produced," with respect to any document, shall include authored, dictated, edited, reviewed, or approved, in whole or in part.
24. The term "Rotation" means any plan, policy or scheme that involves the re-use of an electronic media device after it has been used for backup, archival or other electronic data storage purposes, particularly if such re-use results in the alteration and/or destruction of the electronic data residing on the device prior to it being re-used.
25. The term "Support" means any help or assistance provided to a user of a computer by another individual, whether or not in an official job capacity. Such help or assistance may take the form of, but is not limited to, answering questions, in person or via mechanical means, direct intervention, training, software troubleshooting, hardware troubleshooting, programming, systems consulting, maintenance, repair, or user forums. Providers of support may be employees, contractors, or other third-party providers.

II. PRESERVATION ORDER

A. The parties to this litigation shall take reasonable steps to preserve all Communications, Documents, Electronic Data, and other tangible objects within their possession, custody or control containing information that is relevant to the allegations and defenses in this litigation or may lead to the discovery of admissible evidence in this litigation, including but not limited to Communications, Documents, Electronic Data and other tangible objects related to:

(1) LLRICE601, including but not limited to research, development, field trials, testing, registration, post-testing destruction, volunteer monitoring, audit and inspection, contracts, communications with

third parties (including parents, predecessors, subsidiaries, agents, and other affiliates), communications with governmental or administrative bodies, and other communications relating thereto;

(2) Initial notification, sampling, investigation, and management of the LLRICE601 biotechnology traces identified in 2006 or prior in samples of commercial rice in the United States;

(3) The purchase, cultivation, possession, sale, or transfer of rice or rice seed by plaintiffs; and

(4) Any alleged damages claimed by plaintiffs including information related to the revenue, costs, profits, or business operation and planning documents from any entity or individual alleged to be affected by LLRICE601.

In addition, the parties agree that plaintiffs shall take reasonable steps to retain—to the extent in their possession, custody, or control—samples of rice or rice seed sufficient to determine the variety, type, quality, and LLRICE601 content of any rice or rice seed purchased, cultivated, sold, or transferred by any entity or individual alleged to be affected by LLRICE601. The fact that a particular document or tangible object may be included in the scope of this Order is not intended to, and does not, establish or suggest that the document is relevant to or admissible in this matter.

B. This preservation obligation applies to currently-existing Communications, Documents, Electronic Data, and other tangible objects within the Parties' possession, custody, or control, as well as Communications, Documents, Electronic Data, and other tangible objects generated, produced, or otherwise created in the future during the pendency of this litigation until an agreement can be reached among the parties regarding a cutoff date.

C. Notwithstanding any other provision of this Order, persons may generate business documents in the future without preserving dictation, drafts, interim versions or other temporary compilations of information if such documents would not have been preserved in the ordinary course of business.

D. The parties to this litigation must take reasonable steps to preserve all Communications and Documents in their original condition and Electronic Data in its native format. Such steps include, without limitation:

(1) Taking reasonable steps to identify all Custodians;

(2) Directing all Custodians and appropriate IT personnel to preserve Potentially Relevant Information (this obligation does not require the parties provide a copy of this order to Custodians so long as reasonable steps are taken to inform Custodians of the substantive provisions of this Order, as well as their individual obligations thereunder);

(3) Taking reasonable steps to preserve the oldest known complete backup of servers reasonably expected to contain information within the scope of this Order (once this obligation is satisfied, Parties may continue to engage in the routine rotation of backup tapes going forward);

(4) Taking reasonable steps to cease all nonroutine defragmentation, compression, purging, or reformatting of digital media that may contain Electronic Data that may be subject to discovery until all Active Files containing information within the scope of this Order have been copied;

(5) Taking reasonable steps to suspend routine document preservation or retention policies that may lead to the destruction of information within the scope of this Order;

(6) Taking reasonable steps to promptly capture and preserve all data within the scope of this Order;

(7) Taking reasonable steps to promptly collect and preserve in their current state all Active Files from Electronic Data sources that contain data that is within the scope of this Order. For all Custodians, a complete backup will be made of all Active Files from their current Computer without altering metadata. In addition, a complete backup will be made of all Active Files that contain information within the scope of this Order identified by Custodians that reside on any servers without altering metadata;

(8) Taking reasonable steps to promptly collect any transcripts or text files reflecting the contents of any voicemail systems, telephone conversation recording devices, and other voice recording systems that may exist; and

(9) Taking reasonable steps to preserve all security keys, encryption/decryption information, and policies that exist or are related to any data contemplated by this Order for the sole purpose of accessing the data.

The parties to this litigation shall take reasonable steps to ensure that Communications, Documents, Electronic Data and other tangible objects that are subject to this Order are not destroyed, removed, mutilated, altered, concealed, deleted or otherwise disposed of. However, any party may delete or recycle Active Files electronically stored on servers or hard drives reasonably likely to contain Documents after the party has made and secured a copy of the Active Files which contain information within the scope of this Order contained on said data storage device. A party need not preserve information electronically stored on servers or hard drives not reasonably likely to contain information within the scope of this Order.

> E. Absent exceptional circumstances, the parties will not seek, and the Court will not impose, sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.
>
> F. This Order shall continue in full force and effect until further Order of this Court.

The following order from *Talbott v. City of O'Fallon et al.*, 2006 U.S. Dist. LEXIS 49461 (E.D. Mo. 2006) takes another approach.

> All employees of the City of O'Fallon shall not delete or destroy any files, documents, e-mail or other electronically stored data which mention "Talbott." Additionally, all employees of the City of O'Fallon shall not delete or destroy any files, documents, e-mail or other electronically stored data which mention "Chief" and which were created before August 11, 2005. Finally, all employees of the City of O'Fallon shall not delete or destroy any files, documents, e-mail or other electronically stored data which mention "Chief" and were created after August 11, 2005 if the reference to "Chief" is a reference to Steve Talbott.

After assessing the planning models, a more focused proposed order might suffice, and be more likely to meet the court's approval. For example, a party trying to prove inadvertent or incidental discrimination in the settlement of a claim by an insurance company could request an order requiring the preservation of a specific subset of its active data (checklist of types of data) stored on the specific mainframe system (where) running the insurance company's adjudication system, and such data in archives and backups. In effect the party is asking only for a subset of ESI records that document transactions during a specific time period, which the party can analyze in its effort to demonstrate such incidental discrimination.

Endnotes

[1] Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 136 (2004).

[2] *See* Fed. R. Civ. P. 16(b)(4) and 26(f). The parties to a discovery planning conference are required to discuss preservation issues. But the Committee Note to Rule 26(f) notes: "The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances."

[3] *See Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information*(August 2006), ¶ 4 (C), *available at* http://www.ncsonline.org/images/EDiscCCJGuidelinesFind.pdf.

[4] 2003 U.S. Dist. LEXIS 6427 (N.D. Tex. 2003).

[5] *Id.* at *2, *citing* Pepsi-Cola Bottling Co. of Olean v. Cargill, Inc., 1995 U.S. Dist. LEXIS 19735 (D. Minn. 1995).

[6] 60 Fed. Cl. 133, 138 (2004). *Accord, e.g.,* United Med. Supply Co., Inc. v. United States, 73 Fed. Cl. 35, (2006).

[7] El-Banna v. Bush, 2005 U.S. Dist. LEXIS 16880 at *4, n. 3 (D. D.C. 2005).

[8] Pueblo of Laguna v. United States, 60 Fed. Cl. at 138; *accord* Williams v. Massachusetts Mutual Life Insurance Co., 226 F.R.D. 144, 147 (D. Mass. 2005); Walker v. Cash Flow Consultants, Inc., 200 F.R.D. 613, 617 (N.D. Ill. 2001).

[9] *See* Pueblo of Laguna v. United States, 60 Fed. Cl. at *14; United Med. Supply Co., Inc. v. United States, 73 Fed. Cl. 35 (2006); Williams v. Mass. Mutual Life Ins. Co., 226 F.R.D. 144, 147 (D. Mass. 2005); Walker v. Cash Flow Consultants, Inc., 200 F.R.D. 613, 617 (N.D. Ill. 2001).

[10] Pueblo of Laguna v. United States, 60 Fed. Cl. at 138.

[11] *Id.*

[12] 233 F.R.D. 363 (S.D.N.Y. 2006); *see also* United States ex rel. Smith v. Boeing Co. et al., 2005 U.S. Dist. LEXIS 36890 (D. Kan. 2005).

[13] 233 F.R.D. 363. The court in Biovail adopted the three-part test from Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429 (W.D. Pa. 2004).

[14] Treppel v. Biovail Corp., 233 F.R.D. at 370–71.

[15] *Id.* at 371.

[16] 2006 U.S. Dist. LEXIS 83116 (D. Cal. 2006).

[17] *Id.* at *8.

[18] *See* Tanne v. Autobytel, Inc., 226 F.R.D. 659, 675 (C.D. Cal. 2005); In re Grand Casinos, Inc. Securities Litigation, 988 F.Supp. 1270, 1273 (D. Minn. 1997) (declining to order the preservation of evidence because preservation was statutorily automatic); Schnall v. Annuity & Life Re (Holdings), Ltd., 2004 U.S. Dist. LEXIS 208, at *5 (D. Conn. 2004) (denying a motion for a preservation order because defendants affirmatively stated they were fully aware of their obligations under the PSLRA and the sanctions for failure to comply).

[19] 2005 U.S. Dist. LEXIS 17195 (D. D.C. 2005).

[20] *Id.* at *2.

[21] 2006 U.S. Dist. LEXIS 19739 (E.D. Mich. 2006).

[22] *Id.* at *3 through *5.

[23] 2003 U.S. Dist. LEXIS 6427 (N.D. Tex. 2003).

[24] Other cases that have applied the injunctive relief standard include In re African-American Slave Descendants' Litigation, 2003 U.S. Dist. LEXIS 12016 (N.D. Ill. 2003); Cunningham v. Bower, 1989 U.S. Dist. LEXIS 3914 (D. Kan. 1989); and Humble Oil & Refining Co. v. Harang, 262 F. Supp. 39, 42-43 (E.D. La. 1966).

[25] 60 Fed. Cl. 133.

[26] Pueblo of Laguna v. United States, 60 Fed. Cl. at 139.

[27] *Id.* at 141.

[28] 233 F.R.D. 363 (S.D.N.Y. 2006).

[29] *Id.* at 372.

[30] In regard to how the moving party might satisfy this factor of the test, the court quoted the *Manual for Complex Litigation*, Fourth, § 11.442 at 73 (2004): "a blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems in their day-to-day operations. In addition, a preservation order will likely be ineffective if it is formulated without reliable information from the responding party regarding what data-management systems are already in place, the volume of data affected, and the costs and technical feasibility of implementation." 233 F.R.D. 363, 372, 2006 U.S. Dist. LEXIS 4407.

[31] 2005 U.S. Dist. LEXIS 36890 (D. Kan. 2005).

[32] *Id.* at *6.

[33] *Id.*

[34] Chapter 7 describes the where or the computing environment model, the data checklist model, the life-cycle model, and the revised refer-or-relate model.

17

Sanctions

Introduction

A court may impose sanctions on a party for breaching the duty to preserve evidence, for spoliation, or for violating a court order or injunction. In Chapter 10 we focused on the contours of the duty to preserve ESI, and in Chapter 16 we examined preservation orders. In this chapter we discuss breach. What result obtains if discoverable ESI has been destroyed or lost, or produced subsequent to discovery deadlines? Under what circumstances do the courts sanction the offending party, and what sanctions are imposed [1]?

These questions have reached particular prominence in the discovery of ESI, or at least the issue of spoliation is more frequently at issue. According to one commentator, there were more reported spoliation cases in the 10 years from 1994 to 2004 than in the 200 years before [2].

One reason for this increase may be that ESI is harder to destroy than paper documents such that the spoliation is more difficult to hide. In *Zubulake v. UBS Warburg, LLC* [3]; for example, Zubulake showed that UBS employees were deleting discoverable e-mail in violation of a litigation hold because e-mail to or from those employees was recovered from backup tapes but not produced from those employees' active files [4]. Parties may be failing in their discovery obligations in regard to ESI, in part, because of a lack of understanding of the ESI environment. Or parties may be seeking sanctions more often simply because of the relative newness of managing ESI in discovery. For example, the requesting party learns that ESI has been deleted—a common phenomenon—and moves for sanctions and a hearing to determine whether the deletion was inadvertent or otherwise [5].

Requests for sanctions may be more common in regard to the discovery of ESI, but an expert in the field, after a thorough review of the reported decisions on ESI discovery sanctions, reports that "courts seem to be 'getting it right'" [6]. That is, the courts are neither more nor less likely to impose sanctions simply because ESI is at issue. Instead, the courts are applying established criteria and imposing sanctions when and as necessary when discoverable ESI has been lost, destroyed, or belatedly produced.

If the courts are getting it right, how are parties getting it wrong? Why have courts increasingly been asked to impose sanctions? In large part, the decisions on sanctions are very fact specific. Thus, a case-by-case analysis would be of little assistance to counsel attempting to oversee a party to ensure that no sanctionable behavior occurs, or to a party considering whether a motion for sanctions is justified. What follows, therefore, is a more general description of how parties are getting it wrong: an overview of the reported decisions on sanctions in the discovery of ESI and the standards the courts apply in determining whether sanctions are appropriate. We then set forth various prescriptions for counsel to follow in managing the discovery process focusing on ESI preservation to avoid sanctions.

Electronic Discovery Sanctions

The following is reprinted with permission from Shira A. Scheindlin, Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. TECH. L. REV. 71 (2004) (citations omitted) [7]:

> Our sample consisted of all the written opinions in the sanctions arena since January 1, 2000: 45 federal cases, and 21 state cases. We included state cases in the sample because spoliation issues are not confined to federal court. We limited the sample to the twenty-first century because we believed recent cases would be the most indicative of whether courts had appropriately adapted to e-discovery issues caused by technological advances. Although we are pleased to report that courts seem to be "getting it right," our analysis is necessarily limited by our small sample and cannot be applied to sanctions cases generally. Because we could only locate and analyze written opinions, the sample is undoubtedly skewed in favor of cases granting sanctions. Many sanctions decisions are issued from the bench, and courts are less likely to issue written opinions when they are denying sanctions than when they are granting them.
>
> . . .
>
> In written opinions, requests for sanctions arose most often in tort (24%) and intellectual property cases (20%), followed by contract (18%), and

employment (15%) cases. The remaining 23% involved various subject matters.

Courts granted sanctions 65% of the time, with defendants being sanctioned four times as often (81%) as plaintiffs (19%). The sanctioned behavior most often involved the nonproduction, (i.e., destruction of electronic documents (84%)), rather than a delay in production (16%). When parties were sanctioned for delay, the late production was sometimes coupled with some form of deception or misrepresentation to the court, such as the fabrication of evidence or falsely claiming that documents did not exist.

Often, the sanctioned party had violated a court order (53%), though not necessarily a specific order to preserve documents (16%). Spoliation also occurred where there were general discovery (30%) or injunctive orders in place (7%). When courts imposed sanctions, they referred to the willfulness or bad faith of the violator (49%), prejudice to the party requesting production (35%), and/or the gross negligence or recklessness of the spoliating party (9%), as the reason(s) for imposing the sanction(s).

Attorney's fees and costs were the most frequently granted sanction (60%). Courts granted evidentiary sanctions, such as preclusion (30%), adverse inference instructions (23%), and dismissal or default judgments (23%) with less frequency. The types of sanctions ordered were not mutually exclusive, with courts imposing more than one sanction 28% of the time. Courts based their authority to impose sanctions on Rule 37 (57% of federal cases), state law (40% of state cases), and their inherent power (28%). In 37% of the cases where sanctions were issued, the court cited no authority whatsoever.

In 35% of all the cases examined, sanctions were not imposed even though a party had destroyed electronic data (87%) or had violated a court order (39%). In some instances, the court declined to impose a sanction because it was too early to determine the extent of the harm involved. Of these cases where sanctions were not imposed, 17% involved appellate courts reversing judgments because the district courts had failed to properly consider the need for e-discovery sanctions. When sanctions were denied, the usual reasons were lack of willfulness or bad faith (35%), and/or lack of prejudice (30%). A small percentage of sanctions motions were held to be premature (17%) or denied for a variety of other reasons (30%).

In short, the results of our survey reveal that the profile of a typical sanctioned party is a defendant that destroys electronic information in violation of a court order, in a manner that is willful or in bad faith, or causes prejudice to the opposing party.

. . .

Appellate courts have made clear that a finding of bad faith is not required to impose discovery sanctions. Indeed, bad faith was not present in most of the cases in our sample, and courts often imposed discovery sanctions where

there was a lesser degree of culpability by the offending party, or cognizable prejudice to the injured party.

In cases where a party has been prejudiced by the spoliation of electronic documents, courts have imposed sanctions aimed at restoring the prejudiced party to the position she would have been in had the documents not been destroyed. Courts often sought to remedy the prejudice through an evidentiary sanction or an adverse inference instruction.

. . .

On the other hand, courts have been less concerned with proof of prejudice when faced with willful or bad faith conduct. In circumstances where the conduct is particularly egregious, courts have granted the ultimate sanction of dismissal or default judgment in order to deter obstructionist behavior. In those cases, however, the courts have sometimes noted that the party requesting the documents had suffered prejudice as well.

. . .

Although our earlier discussion categorizes cases by whether courts emphasized the state of mind of the wrongdoer or the prejudice to the party seeking discovery, sanctions decisions seldom focus solely on one or the other. More often than not, both elements are involved, though one may dominate the court's discussion … In cases where one or the other of these elements is less pronounced, there appears to be a sliding scale between the two. That is, the more willfulness there is, the less prejudice courts require before sanctioning a party for e-discovery violations, and vice versa.

. . .

In our sample, we did not discover a single case where a court sanctioned a party solely for following its document retention and recycling policy; there was always another consideration. Whether documents had been deleted or destroyed was not dispositive of whether courts were likely to impose e-discovery sanctions. Courts tended to focus on the prejudice to the party seeking discovery, as well as on the spoliator's culpable state of mind. Judges did not impose sanctions for the smallest infractions, but rather, exercised their discretion to ensure that cases could be fairly adjudicated on the merits.

The Role of Counsel

Zubulake V. [8] Judge Scheindlin's discourse in *Zubulake V* remains the most frequently cited [9] legal statement on lawyers' responsibilities [10]:

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (*e.g.,* those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (*i.e.,* actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold [10].

A party's discovery obligations do not end with the implementation of a "litigation hold"—to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents. Proper communication between a party and her lawyer will ensure (1) that all relevant information (or at least all sources of relevant information) is discovered, (2) that relevant information is retained on a continuing basis; and (3) that relevant non-privileged material is produced to the opposing party [11].

Once a "litigation hold" is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed "on hold," to the extent required in *Zubulake IV*. To do this, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation, in order to understand how they stored information [12].

To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a system-wide keyword search; counsel could then preserve a copy of each "hit." Although this sounds burdensome, it need not be. Counsel does not have to review these documents, only see that they are retained. For example, counsel could create a broad list of search terms, run a search for a limited time frame, and then segregate responsive documents. When the opposing party propounds its document requests, the parties could negotiate a list of search terms to be used in identifying responsive documents, and counsel would only be obliged to review documents that came up as "hits" on the second, more restrictive search. The initial broad cut merely guarantees that relevant documents are not lost [13].

In short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched. This is not to say that counsel will necessarily succeed in locating all such sources, or that the later discovery of new sources is evidence of a lack of effort. But

> counsel and client must take *some reasonable steps* to see that sources of relevant information are located [14].

Zubulake progeny. Case law subsequent to *Zubulake V* has amplified on counsel's duties. For example, in *Phoenix Four, Inc. v. Strategic Res. Corp* [15], defendants belatedly produced ESI from a company server that had not earlier been searched for potentially responsive information because the system configuration did not allow access to the server from desktop workstations. The court reasoned:

> As to [attorney] Mound Cotton's obligation, Judge Scheindlin has defined the contours of counsel's duty to locate relevant electronic information in Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D. N.Y. 2004)("Zubulake V"). Counsel has the duty to properly communicate with its client to ensure that "all sources of relevant information [are] discovered." *Id.* at 432. To identify all such sources, counsel should "become fully familiar with [its] client's document retention policies, as well as [its] client's data retention architecture." Id. This effort would involve communicating with information technology personnel and the key players in the litigation to understand how electronic information is stored. *See id* [16].
>
> Mound Cotton failed in its obligation to locate and timely produce the evidence stored in the server that the SRC Defendants took with them from Carnegie Hall Towers. Mound Cotton affirms that it engaged in dialogue with the defendants on the need to locate and gather paper and electronic documents. Indeed, when repeatedly questioned at oral argument on what inquiries it had made to discover electronic evidence, Mound Cotton reiterated that it had asked the defendants for all electronic and hard copy documents. *See* Oral Argument Tr. at 36:13-14. But counsel's obligation is not confined to a request for documents; the duty is to search for sources of information [17].
>
> It appears that Mound Cotton never undertook the more methodical survey of the SRC Defendants' sources of information that Judge Scheindlin outlined in Zubulake V. Mound Cotton simply accepted the defendants' representation that, because SRC was no longer in operation, there were no computers or electronic collections to search. Had Mound Cotton been diligent, it might have asked—as it should have—what had happened to the computers SRC used at Carnegie Hall Towers. This question alone would have alerted Mound Cotton to the existence of the server that the defendants had taken with them from their former office. Further, Mound Cotton's obligation under Zubulake V extends to an inquiry as to whether information was stored on that server and, had the defendants been unable to answer that question, directing that a technician examine the server. In the case of a defunct organization such as SRC, this forensic effort would be no more than the equivalent of questioning the information technology personnel of a live enterprise about how information is stored on the organization's

computer system [18].

I emphasize that the duty in such cases is not to retrieve information from a difficult-to-access source, such as the server here, but rather to ascertain whether any information is stored there [19].

I find Mound Cotton's deficiencies here to constitute gross negligence [20].

Electronic Discovery Reference Model [21]. Finally, the highly respected EDRM emphasizes the utility and efficiency of cooperation among counsel, and the trend away from old-school "hide-the-ball" approaches toward collaboration for mutual protection in matters involving discovery of ESI:

> Preservation for electronic discovery has become a complicated, multi-faceted, steadily-changing concept in recent years. Starting with the nebulous determination of when the duty to preserve arises, then continuing into the litigation hold process (often equated to the herding of cats) and the staggering volumes of material which may need to be preserved in multiple global locations, platforms and formats, the task of preservation is an enormous challenge for the modern litigator. Seeking a foundation in reasonableness, wrestling with the scope of preservation is often an exercise in finding an acceptable balance between offsetting the risks of spoliation and sanctions related to the destruction of evidence, against allowing the business client to continue to operate its business in a somewhat normal fashion.
>
> Certain suggested standards and guidelines have been emerging to provide checklists for those preparing (and preserving) to respond to electronic requests for production. However, probably the most important and helpful development which has evolved in preservation is the mandate in FRCP and other state rules for the parties to meet and confer early in the discovery process to attempt to reach agreement on important issues of scope and responsibilities related to discovery. As we continue, the 'old school' adversarial approach to discovery, and its hide-the-ball tactics, is rapidly giving way to a more collaborative common search for reasonableness by counsel and technical resources for both sides of disputes, when it is motivated by avoidance of the staggering potential costs of out-of-control electronic discovery. All of this search for common ground, and fiscal reasonableness for the clients, begins with how good a job the parties do in fleshing out the approach to preservation and the definitions of what may be considered relevant material.
>
> The gargantuan scope and complexity of electronic discovery, and meeting the client's duty to preserve relevant evidence, has dictated some new learning experiences for both the legal and IT communities. It has been noted by one of the pioneers of the burgeoning ED industry that 'the reality of electronic discovery is it starts off as the responsibility of those who don't understand the technology, and ends up the responsibility of those who

don't understand the law.' Expansion of the understanding and cooperation of both the legal and technological disciplines is a critical component of effective preservation, but ultimately, it is the legal counsel protecting the client's interests who must learn the most about the client's IT architecture, policies, personnel and culture. Developing a successful preservation plan will be nearly impossible if legal counsel is not fully aware of all the places in the client's electronic world where relevant material may be stashed. Document retention and destruction policies—and practices—must be defined and under control. The attention and buy-in of key players, underscored by communications from senior management, must be obtained to assure compliance with legal hold orders and the construction of good preservation fences around relevant material.

Assessment of the overall preservation task will, by necessity, involve identification of those groups of potentially relevant materials which will be most critical or most difficult to preserve or collect, and those will be driven by the issues and priorities of the individual case. Some of those thorny areas might dictate an immediate implementation of hard drive mirror imaging for key players, by a forensic expert. Some may involve isolation of access from certain segments of the client's systems until collection can occur. Some may require assistance from the IT department to suspend some operations, or re-route certain tasks to different servers. Whatever these steps are, they will usually be technical, and they will generally require assistance from someone knowledgeable about those technical matters. Don't scrimp on getting the technical assistance you need to offset these key data challenges. Morgan Stanley learned the hard way that failure to engage an expert who understood everything about backup tapes, could be an extremely costly mistake. *Coleman (Parent) Holdings v. Morgan Stanley*, 2005 WL 679071 (Fla. 15th Cir. Mar. 1, 2005).

Endnotes

[1] This chapter does not address criminal sanctions for destroying or altering documents. *See, e.g.*, 18 U.S.C. Sec. 1519 of the Sarbanes-Oxley Act.

[2] David K. Isom, Article*: Electronic Discovery Primer for Judges*, 2005 FED. CTS. L. REV. 1 (2005).

[3] Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (Zubulake V).

[4] *Id.* at 427–428. Zubulake had also shown that certain backup tapes had been destroyed and that one employee's active files—containing discoverable information—had not been timely produced.

[5] *See, e.g.,* Ball v. Versar, Inc., 2005 U.S.Dist. LEXIS 24351 (S.D. Ind. 2005), where Versar argued that plaintiff trustees had destroyed e-mail and asked for sanctions, but the court denied the request because Versar had not shown that the e-mail was irretrievable or that the trustees had not acted in bad faith.

[6] *See* Shira A. Scheindlin, Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century,* 11 MICH. TELECOMM. TECH. L. REV. 71, 73 (2004).

[7] Excerpts (citations omitted); with permission, copyright MICHIGAN TELECOMMUNICATIONS TECHNICAL LAW REVIEW (2004), *available at* http://www.mttlr.org/voleleven/scheindlin.pdf. (last accessed March 21, 2007).

[8] 229 F.R.D. 422 (S.D.N.Y. 2004).

[9] *See also* "The Sedona Conference Working Group Series, Best Practices Recommendations for Addressing Electronic Document Production" (2005), http://www.thesedonaconference.org/content/miscFiles/7_05TSP.pdf.

[10] *Id.* at 431, *citing* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)(Zubulake IV).

[11] *Id.* at 432 (citations omitted).

[12] *Id.* (citations omitted).

[13] *Id.* (citations omitted).

[14] *Id.* (citations omitted).

[15] 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. 2006).

[16] *Id.* at *16, 17.

[17] *Id.* at *17.

[18] *Id.* at *17, 18.

[19] *Id.* at *18, *citing* proposed Fed. R. Civ. P. 26(b)(2)(B).

[20] *Id.* at *18.

[21] Reprinted with permission from edrm.net, Socha Consultants, LLC, and Gelbmann & Associates, copyright http://edrm.net (2006).

18

Transaction Surveillance by the Government*

Introduction

Many important aspects of our lives are inscribed in written and digitized records, housed in private businesses, government agencies and other institutions. These records include all sorts of information about us: reports on our medical status and financial condition; data about our purchases, rentals, real estate holdings, licenses, and memberships; logs listing the destination of our e-mails and our Internet wanderings; and countless other bits of individual descriptors, ranging from salary levels to college grades to driver's license numbers. Whether the information memorializes our own version of personal activities or is created by the record-holder itself, there is often an explicit or implicit understanding that the information will be used or viewed by a limited number of people for circumscribed purposes. In other words, we consider the contents of many of these records private, vis-a-vis most of the world.

Thus, it may be surprising that law enforcement officials can, perfectly legally, gain access to all of this information much more easily than they can search our houses or even our cars. While the latter types of actions require probable cause, government can obtain many of the records just described simply by asking (or paying) for them [1]. And, at most, all the government needs

* Reprinted with permission from Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L. J. 139–166 (2005), copyright *Mississippi Law Journal*, 2005. The text at notes 72–96 has been rewritten by the author to reflect developments since the original article was published.

to show in order get any of these records is that they are "relevant" to a government investigation—a much lower, and much more diffuse, level of justification than probable cause [2].

This state of affairs might make sense when the records sought are truly public in nature. It might also be justifiable when the records involve an entity such as a corporation, professional service provider, or government department and are sought in an effort to investigate the entity and its members. But today, facilitated by the computerization of information and communication, government routinely obtains personal medical, financial and e-mail records, in connection with investigations that have nothing to do with business or governmental corruption [3]. That practice is much more questionable.

The Current Reach of Transaction Surveillance

Transaction surveillance comes in many forms. This section divides it into two types: target-based and event-based. Using these categorizations, the following discussion relies on hypotheticals to flesh out the various ways transaction surveillance can assist law enforcement in investigating street crime.

Target-Based Transaction Surveillance

Assume that I'm a federal agent, and that I'm suspicious of you for some vague reason—perhaps you often pay for your airplane tickets with cash [4], or you have been observed with accessories you shouldn't be able to afford [5], or you are a young, Arab male who goes to the local mosque on a daily basis [6]. Under these types of circumstances, I clearly do not have sufficient suspicion for an arrest [7]. On the other hand, I feel I would be neglecting my obligation as a law enforcement official if I did not investigate you a bit further. So how do I find out more about you?

I could confront you directly, either on the street or through a grand jury [8]. But neither approach is likely to net much information, and both will tip you off that I'm checking you out. Ditto with respect to going to your acquaintances and neighbors; they will probably not be completely forthcoming and they might let you know I've been nosing around. I could try the undercover agent approach—there might be rich payoffs if I or one of my informants can weasel into your good graces. But success at that endeavor is rare, and spending so much effort on someone about whom I'm merely suspicious would usually be a waste of time. I could also surreptitiously follow you around for awhile, but that tactic is unlikely to produce much, especially if you make most of your contacts through technological means—phones, e-mail—rather than physical

travel. Of course, I could tap your phone and intercept your e-mails, but that requires a warrant based on probable cause, which I do not have.

Thankfully there are other, much more efficient ways I can covertly acquire information about you, many of which I can carry out without leaving my desk and most of which, as the next section describes, require no or little legal authorization. The easiest way to get useful data is to contact one of the many companies, usually called commercial data brokers (CDBs), that use computers and the Internet to dig up "dirt" from public and not-so public records [9]. One such company is LexisNexis, the legal research behemoth, which operates Accurint, a program that allows "organizations to quickly and easily extract valuable knowledge from … tens of billions of data records on individuals and businesses," armed with no more than a name, address, phone number, or Social Security number [10]. Through this process, I can obtain information about a wide array of your transactions, including: bankruptcies and corporate filings, criminal convictions and criminal and civil court data (including marriage and divorce information), driver's licenses and motor vehicle information, firearms, hunting, fishing, and professional licenses and permits, Internet domain names, property deeds and assessments, and voter registration information [11]. For some states, the information held in "public records" by government bureaucracies and available via computer is immensely broader: some types of medical records, Social Security numbers, crime victim's names, credit card and account numbers, psychiatric evaluation reports, tax returns, payroll information, and family profiles [12]. For a time, all of this was made even more easily accessible to state law enforcement officials through MATRIX (Multistate Antiterrorist Information Exchange), a multistate consortium that allowed police to use Accurint for investigative purposes until its federal funding was discontinued in 2005 [13].

The FBI and other federal agencies rely on equally powerful commercial data brokers, with perhaps the most popular being Choicepoint [14]. Under its contract with the federal government, Choicepoint can provide me, as a federal agent, with "credit headers" (information at the top of a credit report which includes name, address, previous address, phone number, Social Security number and employer); pre-employment screening information (including financial reports, education verification, reference verification, felony check, motor vehicle record and professional credential verification); "asset location services;" information about neighbors and family members; licenses (driver's, pilot's and professional); business information compiled by state bureaucracies; and "derogatory information" such as arrests, liens, judgments and bankruptcies [15]. If you think I wouldn't bother requesting such a check, think again; between 1999 and 2001, Choicepoint and similar services ran between 14,000 and 40,000 searches per month for the United States Marshall's Service alone [16].

The one drawback to the type of information I get from CDBs is that it is pretty general. I may want to know more about what you do on a daily basis. Fortunately, there are a number of services that can help me out. For instance, advances in data warehousing and data exchange technology in the financial sector allow very easy access to a virtual cornucopia of transaction-related information that can reveal, among other things, "what products or services you buy; what charities, political causes, or religious organizations you contribute to; … where, with whom, and when you travel; how you spend your leisure time; … whether you have unusual or dangerous hobbies; and even whether you participate in certain felonious activities" [17]. If I jump through some *pro forma* legal hoops (detailed below), I can also get records of all the phone numbers you dial and receive calls from [18], and from your Internet service provider (ISP) I can get every Web site address you have visited (so-called "clickstream data") and every e-mail address you have contacted [19].

The latter information can be particularly revealing to the extent you transact your business over the Internet. Recently some ISPs, like America Online, have stopped maintaining clickstream data, precisely so they won't have to answer such law enforcement requests [20]. No worries. All I have to do is invest in something called "snoopware." Bearing names like BackOrifice, Spyagent, and WinWhatWhere [21], snoopware is to be distinguished from adware and spyware. The latter software tells the buyer of the program how to contact people who visit the buyer's Web site. Snoopware, in contrast, allows its buyer to track the target well beyond a single Web site; it accumulates the addresses of all the Internet locations the target visits, as well as the recipients of the target's e-mails. The FBI has developed a similar program, once dubbed Carnivore, now called DCS-1000, that filters all e-mails that pass through a particular server [22]. Although some transaction snoopware requires access to the server or computer to install, other types, called Trojan Horses, can electronically worm their way onto the system disguised as something useful [23].

In short, even if you stay at home and conduct all your business and social life via phone, e-mail and surfing the 'Net, I can construct what one commentator has called "a complete mosaic" of your characteristics [24]. And I can do all of this without you having a clue I'm doing it. It is also possible that I could surreptitiously obtain an even wider array of transactional information—on matters ranging from medical treatment to financial decisions—with very little effort. But further discussion of that possibility, as well as of the huge amount of transactional information that government can obtain if it is willing to proceed overtly, will have to wait for the explanation below of the current legal regime.

Event-Based Transaction Surveillance

Now consider an entirely different type of scenario, one in which government has no suspicion of or even interest in a specific individual, but rather possesses information about a particular crime that has been or will be committed. Government efforts to obtain transactional data in this situation is not target-based, but event-based. Say, for instance, that the police know that a sniper-killer wears a particular type of shoe (thanks to mudprints near a sniper site), that he owns a particular type of sweater (because of threads found at another site), and that he reads Elmore Leonard novels (because of allusions to those books made in his communications to the police). Law enforcement understandably might want to peruse the purchase records of local shoe, clothing, and bookstores as part of their investigation. Once police obtain the credit card numbers of those who bought, say, the type of sweater found at the murder scene, they can trace other purchases made with the same card, to see if the relevant type of shoe or book was bought by any of the same people. Of course, if there is a match on two or three of the items, the surveillance may then turn into a target-based investigation.

Or say that a CIA informant reports that he believes Al Qaeda is considering blowing up a major shopping mall, using skydivers jumping from rental planes [25]. The FBI might want to requisition the records of all companies near major metropolitan areas that teach sky-diving and that rent airplanes, as well as the "cookie" logs (records of cyberspace visitors) of all Web sites that provide information about manufacturing explosives, to see if there are any intersections between these three categories of data, in particular involving men with Arab-sounding names. If there are then, again, further target-based surveillance investigation might take place.

Although the first type of event-based surveillance is backward-looking and the second is forward-looking, both law enforcement efforts are a form of what has been called "data mining" or "profiling," that is, an attempt to look through transaction information to find patterns of behavior that permit police to zero in on possible suspects [26]. If the information sought is not digitized, which is likely with respect to records kept by sky-diving companies, for instance, then law enforcement may have to rely on good old-fashioned human snooping. In this day and age, however, a significant amount of data mining can be carried out using technology. For example, the Defense Department's Total Information Awareness program, before it was severely limited by Congress, would have used software developed by private companies "to sift through virtual mountains of data of everyday transactions, such as credit card purchases, e-mail and travel itineraries, in an attempt to discover patterns predictive of terrorist activity" [27]. Whether it relies on computers or humans, event-based

data mining, like transaction surveillance of particular individuals, can easily be conducted unbeknownst to those whose records are surveilled.

Summary

Technology has made transaction surveillance a particularly powerful law enforcement tool. Given the potential that transaction surveillance provides the government for creating personality mosaics and linking people to crime, it could well be even more useful than visual tracking of person's activities (physical surveillance) and eavesdropping on or hacking into a person's communications (communications surveillance). But the real beauty of transaction surveillance for the government is that, compared to physical surveillance of activities inside the home and communications surveillance, it is so lightly regulated. As Part II explains, under today's regulatory regime it is much easier for government to obtain information about our most intimate transactions, including medical and financial matters, than it is to intercept our communications about those transactions.

Current Legal Regulation of Transaction Surveillance

Under the Fourth Amendment, the government usually cannot conduct a search of houses, persons, papers and effects without probable cause [28], a relatively high level of certainty akin to a more-likely-than-not standard (which, in nonexigent situations, must be found by a magistrate pursuant to an application for a warrant) [29]. For some less invasive actions (a frisk, for instance), police only need reasonable suspicion, which is a lower level of certainty than probable cause but still requires "specific and articulable facts" that "criminal activity may be afoot," to quote from the famous case of *Terry v. Ohio* [30]. Finally, in some "special needs" situations (searches of school children or employees; drug testing; health and safety inspections; roadblocks), the police need only act "reasonably," but that test still usually requires reasonable suspicion [31], or at least a showing that those conducting the government action are pursuing some end other than criminal law enforcement [32].

In contrast, transaction surveillance, whether it is event-based or target-based, never requires probable cause or reasonable suspicion, even when conducted by government agents whose primary goal is criminal investigation. At most, government agents seeking transactional information need a subpoena—either a subpoena *duces tecum* issued by a grand jury, or an "administrative subpoena" issued by a government agency—which is valid as long as the information it seeks is "relevant" to a legitimate (statutorily-authorized) investigation. Relevance, as defined by the Supreme Court, is an extremely low standard. In the grand jury context, a subpoena may be quashed on irrelevancy

grounds only when the court "determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation" [33]. The relevancy standard in the administrative subpoena context is even lower, with the Supreme Court holding that "even if one were to regard the subpoena as caused by nothing more than official curiosity, nevertheless law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest" [34]. In short, the link between the information a subpoena commands and the investigation the government is pursuing can be very tenuous indeed. Although a subpoena may be challenged before it is executed, a successful challenge is exceedingly rare, whether the subpoena is issued by a grand jury or an administrative agency [35].

Furthermore, as we shall see, the law does not require even a traditional subpoena for most types of transaction surveillance. Instead, the government, in particular Congress, has either invented new forms of authorization that are even easier to obtain or has simply permitted unrestrained law enforcement access to transactional information. The following account of this incredibly weak regulatory regime starts with the law regarding transaction surveillance of identifying information, conducted in real-time, then describes regulation of government attempts to obtain public records, and finally describes transaction surveillance of records held by private entities.

Interception of Transaction Information

Real-time government interception of the content of communications (what I am calling communications surveillance) is prohibited unless authorized by a warrant based on probable cause [36]. In contrast, interception of the identifying features of the communication—the names of the communicators, their phone numbers or e-mail addresses, and the addresses of Web sites visited—can take place on a much lesser showing. The Fourth Amendment does not apply at all to this type of transaction surveillance, and statutory law places virtually no restrictions on it.

The Fourth Amendment's justification requirements—probable cause and the like—only apply if government engages in a "search or seizure." Although one might reasonably label government efforts to track down a person's phone and e-mail correspondents a search, the Supreme Court has held that a Fourth Amendment search occurs only when a government action infringes a reasonable expectation of privacy [37]. More importantly for present purposes, the Court has determined, in *Smith v. Maryland* [38], that we do not have a reasonable expectation in the phone numbers we dial because we know or should know that phone companies keep a record of these numbers, and thus "assume the risk" that the phone company will decide to disclose this information to the

government [39]. Because it is generally known that Internet service providers monitor, if only temporarily, our e-mails and Internet surfing, the Court would probably also say that we assume the risk these providers will become government informants. Although Universal Resource Locators (URLs) can be more informative than a mere phone number, both because they are addresses (e.g., www.amazon.com/kidneydisease) and because they allow access to the *Web site* and thus permit government to ascertain what the user has viewed, the lower courts applying *Smith* appear to see no difference between the two types of routing information [40]. Accordingly, the government can probably ignore the Fourth Amendment when intercepting phone numbers and Internet addresses.

Congress has imposed some statutory restraints on this type of surveillance, but nothing approaching the usual Fourth Amendment protections. In the Electronic Communications Privacy Act of 1986 (ECPA), it created a new, streamlined type of authorization process for use of pen registers (technology which intercepts outgoing phone numbers) and trap and trace devices (technology which intercepts incoming numbers), a process that can be initiated by either a federal government attorney or a state law enforcement officer. All the government agent must do is certify to a court facts that show the information is "relevant to an ongoing investigation" and is "likely to be obtained by [the surveillance]" [41]. If that certification is made, the court must issue the order [42].

The USA Patriot Act of 2001 expanded the definition of pen registers and trap and trace devices to include all devices that obtain "dialing, routing, addressing, or signaling information utilized in the processing and transmitting of wire or electronic communications …" [43]. Thus, to use snoopware, DCS-1000, and other means of ascertaining a person's e-mail correspondents and favorite Web sites, the government need only certify the relevance of this information to a current investigation [44]. Again, if this certification is made, the court must issue an order.

Those of us who teach Fourth Amendment law sometimes joke about supposedly "neutral and detached" magistrates rubberstamping warrant applications, but we also assume that judicial independence is theoretically possible [45]. Here, in contrast, Congress has legislatively invented mandatory rubberstamping. It is tempting to call this type of authorization a "rubberstamp order," but I will instead use the more measured term certification order. Whatever one calls the authorization process, it amounts to minimal limitation on interception of transaction information.

Access to Publicly Held Records

Most transaction surveillance does not involve real-time interception of information, but rather contemplates accessing already-existing records, held either by public or private institutions. Information in public records is particularly

easy to secure. Under current law, law enforcement officials do not need even a certification order to use MATRIX, Choicepoint, and similar vehicles for perusing public records. In fact, law enforcement officials need consult no other entity (certainly not a court, and not even a prosecutor) before obtaining such information.

Again, the Fourth Amendment's ban on unreasonable searches and seizures might appear to apply here, because looking for and through records is a search in the usual meaning of the word. But, as already noted, the Supreme Court has made clear that one cannot reasonably expect privacy in connection with information voluntarily given to third parties. Even more important than *Smith* in this regard is *United States v. Miller* [46], decided three year earlier. There the Court held that once a person surrenders information to an agency or institution, he or she assumes the risk the third party will hand it over to the government [47]. The key declaration in *Miller* is worth quoting in full: "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed" [48].

The Privacy Act, enacted by Congress in 1974, does bar or limit access to public records when they are sought by private individuals, and even when most government officials want them [49]. But when law enforcement officials are after the records, the Act merely requires a letter from the head of the agency that is seeking the information, detailing the law enforcement reasons a particular person's records are needed [50]. No court is involved, and neither individualized suspicion nor even a relevance showing is required, just the say-so of the law enforcement department. I will call this kind of authorization an extrajudicial certification.

Not even this level of authorization is necessary for government access to most public records, however. The Privacy Act only applies to federal documents. Unless there is similar legislation at the state level, law enforcement access to state public records is unrestricted [51]. Furthermore, the federal government takes the position that when it obtains information from a commercial data broker like Choicepoint, the Privacy Act does not apply at all, because the Act literally only refers to law enforcement efforts to get records from other government agencies and from private companies that are administering a system of records for the government [52]. Under this interpretation, the only obstacle to complete government access to all the data maintained by commercial brokers is the price of the information [53].

Access to Privately Held Records

Compared to the meager limitations on intercepting transactional information and accessing public records, the restrictions on government access to the contents of records held by nominally private entities, such as hospitals and banks, phone companies and Internet providers, have more teeth, but the teeth are blunt. Again, the Fourth Amendment is pretty much irrelevant here. The notion that one assumes the risk that third parties will be, or turn into, government informants applies to private entities as well as public agencies. The Supreme Court has specifically so held with respect to phone companies (in *Smith*) [54] and banks (in *Miller*) [55]. It has wavered in its willingness to declare private entities untrustworthy confidants only in the medical context, where it has stated, *in dictum*, that the Fourth Amendment or the due process clause might place constitutional limitations on law enforcement access [56]. Although there are also statutory constraints on government accessing of privately held records, they are extremely weak.

Medical records receive the most protection. Even here, however, neither probable cause nor reasonable suspicion is required. Rather, pursuant to rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), the government can obtain medical records from HMOs and hospitals with a simple subpoena. A subpoena, it will be recalled, merely requires a finding that the information sought is relevant to a law enforcement investigation (although the target is entitled to notice and thus has the opportunity to challenge the subpoena on relevance or privilege grounds) [57]. Given the limited scope of the Privacy Act described above, even that obstacle is removed if, as is true in some states, medical and similar information is maintained as a "public record" and the government receives it through a commercial data broker.

Financial records receive similarly minimal protection. To get detailed information from credit agencies, a regular subpoena is required under the Fair Credit Reporting Act [58]. However, analogous to the situation with medical records, no law governs government requests for similar information from database companies and other companies that have obtained it from credit agencies [59]. As a result, the government routinely gets the financial information it wants directly from a commercial data broker, without bothering with a subpoena [60]. Bank records are also easily accessible. The Right to Financial Privacy Act generally requires only a traditional subpoena to obtain financial records from a bank. It also recognizes a significant variation to the traditional subpoena process: notification of the seizure may be delayed for up to 90 days if there is concern that service of the subpoena will tip off a suspect, result in loss of evidence, endanger witnesses or in some other way compromise the government's investigation [61]. In these circumstances, in contrast to the typical subpoena process, the target of a financial investigation will not find out that the

government has the information until well after it is obtained. I will call this type of authorization a delayed-notice subpoena.

Outside of situations covered by the Right to Financial Privacy Act and the Internal Revenue Code, a government agency that is authorized to use administrative subpoenas to obtain financial and business information from third-party entities need not give any notice to the customer whose records are sought [62]. This practice recognizes still another subpoena mutation, which I will call an *ex parte* subpoena. This label is meant to distinguish between third-party subpoenas that allow the target to contest the demand for production and those that don't. The term "*ex parte* subpoena" emphasizes that the customer is outside the process entirely, thus removing, in most cases, the only meaningful inhibition on fishing expedition-by-subpoena.

Transaction surveillance of communications-related information is regulated in a similarly weak fashion. Under ECPA, real-time interception of the content of phone and e-mail communications requires a warrant based on probable cause [63]. But if e-mail has sat on a server for longer than 180 days without being opened, or the recipient of e-mail or voicemail accesses it and stores it on an outside server for any length of time, then a subpoena—delayed if necessary—is all that is needed to obtain the content of the communication [64]. Apparently, the rationale behind permitting easy access to unopened mail that is stored for 180 days is that it is, in effect, abandoned [65]. The rationale for permitting access on less than probable cause to opened e-mail and other communications stored by a third party is that it becomes akin to a business record [66].

ECPA also gives the government easy access to business records held by phone companies and Internet service providers. Under Title II of ECPA, as amended by the Patriot Act of 2001, basic subscriber information—name, address, session times and durations, length and type of service, means and source of payment (including credit card numbers), and the identity of Internet users who use a pseudonym—can be obtained pursuant to an *ex parte* subpoena, the type of authorization that requires no customer notice [67]. If the government seeks additional transactional information—such as account logs and e-mail addresses of other individuals with whom the account holder has corresponded—it still need not alert the subscriber, but must allege "specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought, are relevant and material to an ongoing criminal investigation" [68].

Apparently, this latter standard, found in § 2703(d) of ECPA, is meant to be more demanding than the relevance standard normally required for a subpoena. Yet it is not clear that it is much different. Although the "specific and articulable" language sounds like it requires reasonable suspicion, note that the specific and articulable facts need only support a finding that the information is relevant and material to an ongoing investigation. Even if the latter highlighted

word is meant to augment the former, it does not add much; materiality, in evidence law, merely means that the evidence be logically related to a proposition in the case [69]. Furthermore, whereas *Terry* contemplated that reasonable suspicion exist with respect to the targeted individual, a § 2703(d) order, like a subpoena, allows accessing any records that might be relevant to an investigation, not just the target's. Finally, it is not clear that the "relevant and material" language can be meaningfully enforced. The statute seems to say that the only ground on which an order issued pursuant to § 2703(d) may be challenged is burdensomeness, which eliminates a challenge on relevance grounds [70].

After 9/11, government access to some sorts of privately held records is even easier when a significant purpose of the investigation is to nab terrorists or spies. Two separate subpoena-like mechanisms are important here. The first is an order under Section 215 of the Patriot Act. As originally enacted, that provision authorized the FBI to demand the production of "any tangible things (including books, records, papers, documents, and other items)" if it followed a simple two-step process [71]. First, the Director or his or her designee had to certify to a court that the items sought were "for an investigation to protect against international terrorism or clandestine intelligence activities," and that the investigation did not focus "solely" on activities protected by the First Amendment. Second, the court had to find that the investigation met these conditions; if so, it was required to issue a Section 215 order authorizing the seizure. In other words, a variant of the certification order discussed in connection with use of pen registers and trap and trace devices sufficed in this situation.

In March, 2006, as part of the USA Patriot Improvement and Reauthorization Act, Congress placed a few more restrictions on this process. First, the amendment makes clear that only high-ranking officials can request a Section 215 order when it seeks records regarding library transactions, books sales and educational and medical matters [72]. Second, a mere certification that the items relate to a national security investigation is no longer sufficient. Rather the application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" [73]. Third, procedures must be in place to "minimize" dissemination of any information acquired [74]. Fourth, the amendment clarifies that a 215 order is subject to judicial review upon request by the record-holder and allows the judge to set aside or modify the order [75].

Although in theory the amendments have made a Section 215 order more difficult to obtain, the applicable standard is still "relevance" and the issuing and reviewing judges apparently are still to refrain from inquiring into the basis of the certification, but rather must limit themselves to making sure the relevant statement of facts is provided [76]. Note further that the records that may be obtained in this way are not just those of suspected terrorists, but of anyone whose information might "protect against international terrorism or clandestine

intelligence activities" [77]. Finally, the Section 215 process is *ex parte*, with a twist: A third party served with a Section 215 order is prohibited from telling the target (or, for that matter, anyone else other than a lawyer) about the order [78]. Unlike the delayed-notice subpoena, this gag-order provision operates automatically; no finding that notice might compromise the investigation is required. The 2006 amendments do permit a challenge of this nondisclosure requirement, but only after one year has elapsed since issuance of the order [79].

Paul Rosenzweig has argued that the provision for judicial modification, together with the requirements that the government "swear" the certification is correct and that the Attorney General report to Congress on the use of Section 215 [80], provide more safeguards than those associated with a subpoena reviewable only after challenge [81]. But if the judge is only permitted to modify an order to accommodate First Amendment concerns (a likely limitation, as suggested by the law regarding National Security Letters to be discussed below), and if Congress is only given general data or trivial bits of information about the surveillance program (which is usually the case [82]), then the typical subpoena process—which allows the target to challenge the relevance of the information, either immediately or after delayed notice—is likely to be at least as protective, and is certainly more likely to deter or expose abuses. In any event, neither Section 215 or the typical subpoena process requires probable cause or even reasonable suspicion, if the latter term requires an articulable suspicion that there is a nontrivial (i.e., 30%) chance that the targeted individual is engaged in crime.

Even a Section 215 order is not needed when the FBI is seeking a particular subset of "tangible items" —electronic or communication billing records, financial records or credit records—in connection with a national security investigation. Rather all it must do is issue a form of administrative subpoena, known as a National Security Letter, in which a Special Agent in Charge (in other words, a field agent) certifies that the information sought is relevant to an investigation designed to protect against international terrorism or clandestine intelligence activities [83]. This type of authorization is akin to the extrajudicial certification discussed in connection with law enforcement efforts to seek public documents under the Privacy Act, but with the same gag-order proviso that applies to Section 215 orders [84].

The Patriot Act allowed this extrajudicial process with respect to financial information only when that information was held by banks. However, in December, 2003, that power was expanded by the Intelligence Authorization Act of 2003, which was enacted by Congress as part of an appropriations bill, with no vetting by the Judiciary Committee and no debate on the floor or in the media [85]. The 2003 Act allows the FBI to use extrajudicial certification to obtain statements and records from any financial institution "whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters,"

including banks, stockbrokers, car dealers, casinos, credit card companies, insurance agencies, jewelers, pawn brokers, travel agents, and airlines [86].

At one time, all of this information was the government's simply on its say-so. In 2004, however, a federal district court judge declared the NSL scheme unconstitutional to the extent it immunized NSLs from judicial process and prevented third-party record-holders from challenging an order [87], and in 2005 another court expressed similar concerns [88]. Those decisions, combined with congressional unease about the scope of the program—particularly as it applied to libraries—led to several amendments to the Patriot Act. Libraries are now exempted from its provisions [89], and third parties are permitted to ask a court to set aside or modify NSLs when they are "unreasonable, oppressive, or otherwise unlawful," as well as challenge any accompanying gag order [90].

Again, however, the new judicial review power is relatively toothless. In *Doe v. Ashcroft*, the first decision finding the NSL procedure defective, the court indicated that review of an NSL would be limited to whether "the underlying investigation was not duly 'authorized,' was initiated 'solely on the basis of activities protected by the first amendment to the Constitution of the United States,' or did not involve 'international terrorism or clandestine intelligence activities'" [91]. Indeed, the court stated, "the standard of review for administrative subpoenas similar to NSLs is so minimal that most such NSLs would likely be upheld in court" [92] The gag-order review procedure is similarly illusory, since if the FBI certifies that disclosure would "interfere" with a criminal or national security investigation or endanger someone, the court must abide by that decision [93] In any event, neither review procedure is triggered unless a third party wants to take the trouble to do so. Evidence suggests that virtually no such challenges occur [94].

Section 215 is apparently used relatively sparingly, with the Justice Department stating in late 2005 that it had relied on the provision only 35 times during the previous two years, in aid of efforts to gain access to information about matters such as apartment leases, driver's licenses, and financial dealings [95]. National Security Letters, in contrast, are used quite frequently, under circumstances that do not inspire confidence about the government's willingness to self-regulate. According to one report, the FBI issues roughly 30,000 NSLs a year and maintains all the records thereby obtained (even when not linked to terrorism) [96]. Given the substantial overlap between the kind of information that can be obtained using NSLs and Section 215 orders, it is no surprise that the FBI rarely resorts to the latter.

Summary of Transaction Surveillance Law

Transaction surveillance has spawned a wide array of new regulatory schemes, which are usefully summarized by locating them within the standard Fourth

Amendment hierarchy. As noted earlier, the most protective type of authorization is the warrant, based on probable cause. Although intercepting the content of communications and physical surveillance of the home both require a warrant [97], no type of transaction surveillance requires this most demanding form of authorization. The next type of authorization in the hierarchy, at least in theory, is an order based on reasonable suspicion, or what could be called a Terry order, after *Terry v. Ohio* [98], which required this degree of justification for a stop and frisk. Again, none of the statutory provisions I have described (or any other regulatory regime for that matter) mandates this type of order; I include it both for the sake of comprehensiveness and because it is important to the regulatory scheme I propose below. After a Terry order comes the traditional subpoena, issued upon a judicial finding of relevance and challengeable by the target. This is the first type of authorization that plays a role in transaction surveillance; subpoenas are required to access most medical, financial and stored e-mail records.

Below the traditional subpoena is the delayed-notice subpoena, which authorizes, temporarily, unobstructed access to financial records and stored e-mail when a traditional subpoena might frustrate the investigation. Next is the *ex parte* subpoena (unchallengeable by the target), which allows access to many types of customer records held by third-party entities, including phone and ISP account records [99]. The certification (judicial rubberstamp) order follows in the hierarchy; it authorizes the use of pen registers, trap and trace devices and other forms of transaction-oriented snoopware, as well as tangible items other than financial records thought to be relevant to national security investigations [100]. At the bottom of the authorization totem pole there is the extrajudicial certification, which permits access to public records, and to financial and other records relevant to national security investigations. However, even this type of authorization is not needed to access public records that come from a state with no privacy statute or that are accumulated by a commercial data broker. All of the authorization mechanisms described in this paragraph are statutory inventions, and are particularly punchless given the lack of a remedy in the unlikely event government is found to have abused them [101].

Endnotes

[1] *See generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution,* 86 MINN. L. REV. 1137 (2002).

[2] *See infra* text accompanying notes 35–37.

[3] *See* Solove, *supra* note 1.

[4] *Cf. Florida v. Royer*, 460 U.S. 491, 493 n. 2 (1983) (noting that paying for an airline ticket with cash is often an element of drug courier profiles used by the Drug Enforcement Administration).

[5] *Cf. State v. Cookson*, 361 S.W.2d 683, 684 (Mo. 1962) (informant, who alleged that defendants had robbed a tavern, reported that "they had a large sum of money and were spending freely").

[6] *Cf.* Michael J. Whidden, *Unequal Justice: Arabs in America and United States Antiterrorism Legislation*, 69 FORDHAM L. REV. 2825, 2865 (2001) (recounting FBI surveillance of a Brooklyn mosque).

[7] An arrest or prolonged questioning in the stationhouse requires probable cause. Charles H. Whitebread and Christopher Slobogin, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS 72–76 (4th ed. 2000).

[8] Note further that even questioning in the field that lasts longer than a few minutes requires reasonable suspicion, which exists only if there are specific and articulable facts that the person is or has been engaging in criminal activity. *Id.*

[9] In fact, the Web site for one of these companies can be found at http://digdirt.com. The services are of uneven quality. *See* Preston Gralia, Digital Gumshoes, *available at* http://www.pcmag.com/article2/0,4149,20148,00.asp (Nov. 13, 2001) (recounting efforts to use various services, including digdirt, with mixed results). For present purposes, however, the point is that their potential for transaction surveillance is enormous.

[10] *See* Accurint Web site, *available at* http://www.accurint.com/aoutus.html (last accessed on Sept. 13, 2005). LexisNexis bought Accurint from SeisInt in 2005.

[11] *Id.*

[12] Robert Ellis Smith, *Here's Why People Are Mad*, 29 PRIVACY J. 7, 7 (Jan. 2003) (citing Stephen Grimes, administrator of the Judicial Records Center in Rhode Island), *available at* http://www.privacyjournal.net/.

[13] *See* Fla. Dep't Law Enforcement, *MATRIX Pilot Project Concludes*, April 14, 2005, *available at* http://www.fdle.state.fl.us.pressreleases/20050415matrix project (noting, however, that Florida and several other states may continue funding the program).

[14] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L & COMM. REG. 595, 617–18 (describing the FBI's "secret, classified contract" with Choicepoint).

[15] *Id.* at 601–02. Note also that once a Social Security number and other identifying information is obtained, other personal information might become much more easily accessible. *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 108–14 (2001) (pointing out that schools, financial institutions, and other entities make personal information accessible by anyone with the right Social Security number, address, and mother's maiden name).

[16] *Id.* at 4–6. In 2001, the Immigration and Naturalization Service conducted approximately 23,000 such searches a month. *Id.* at 11.

[17] Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 944–45, 951 (2002).

[18] The Electronic Communications Privacy Act, 18 U.S.C. § 3121 allows prosecutors to obtain this information by certifying to a court that it is relevant to an ongoing investigation. *See infra* text accompanying notes 43–47.

[19] The Electronic Communications Privacy Act at most requires a showing of relevance for this information. *See* 18 U.S.C. § 3121; *infra* notes 69–77 and accompanying text; *see also* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. J. TELECOMM. & TECH. L. REV. 61, 68–69 (2000) detailing the type of information government can obtain through clickstream data).

[20] Conversation with Peter Swire, Professor, Ohio State School of Law, September 20, 2004. The Electronic Frontier Foundation has recommended that ISPs only keep personally identifiable communications from blogs for "so long as it is operationally necessary, and in no event for more than a few weeks." Electronic Frontier Foundation, *Best Data Practices for Online Service Providers*, from the Electronic Frontier Foundation at http://www.eff.org/osp/ 20040819OSPBestPractices. pdf2 (June 29, 2005).

[21] *See* Cade Metz, *Spyware: It's Lurking on Your Machine*, PC MAG., Apr. 22, 2003, at 85, 88.

[22] Jeremy C. Smith, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412, 448–49 (2003). Recently, the FBI announced that it would no longer use DCS-1000, but instead rely on "unspecified commercial software to eavesdrop on computer traffic." *FBI Cuts Carnivore Internet Probe*, at http://www.cnn.com/2005/TECH/internet/01/18/fbi.carnivore.ap/index.html (on file with the *Mississippi Law Journal*).

[23] Metz, *supra* note 23, at 85. Some snoopware, using "key logger" technology, can even tell the user the content of one's computer screen. *Id.* DCS-1000 can also be programmed to access content as well as identifying information. Joseph F. Kampherstein, *Internet Privacy Legislation and the Carnivore System*, 19 TEMP. ENVTL. L. TECH. J. 155, 167 (2001). Both functions are forms of communication surveillance that are beyond the scope of this article.

[24] Anthony Paul Miller, Teleinformatics, *Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age*, 20 COLUM. J. L. & SOC. PROBS. 89, 111 (1986).

[25] This imaginary scenario is borrowed from the second Markle Report. Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force*, app. D at 121–33 (2003), *available at* http://www.markletaskforce.org/.

[26] For a general description of data mining and its prevalence, *see* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 71–88 (2003).

[27] *Id.* at 64; *see also infra* note 122.

[28] *See* U.S. CONST. amend. IV.

[29] *See* WHITEBREAD & SLOBOGIN, *supra* note 9, at 137–42.

[30] 392 U.S. 1, 21, 30 (1968).

[31] *See* O'Connor v. Ortega, 480 U.S. 709, 724 (1987) ("The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest."); New Jersey v. T.L.O., 469 U.S. 325, 341–42, 344 (1985) (holding that "a search of a student by a teacher or other school official will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence" and finding that this standard was met in this case because there was reasonable suspicion).

[32] *See* Bd. of Educ. v. Earls, 536 U.S. 822, 829 (2002) (upholding warrantless, suspicionless school drug testing, noting that "in the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable when 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable'"); City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. Rather, our checkpoint cases have recognized only limited exceptions to the general rule that a seizure must be accompanied by some measure of individualized suspicion.").

[33] United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (emphasis added).

[34] United States v. Morton Salt Co., 338 U.S. 632, 652 (1950); *see also* United States v. Powell, 397 U.S. 48, 57–59 (1964) (holding that administrative subpoenas are valid if the records sought are "relevant" to an investigation conducted for a "legitimate purpose"); United States v. Hunton & Williams, 952 F. Supp. 843, 854 (D.D.C. 1997) (holding that the *Powell* inquiry is more deferential than the arbitrary and capricious standard of review for agency action under the Administrative Procedure Act).

[35] See Wayne R. Lafave, Jerold H. Israel and Nancy J. King, 3 CRIMINAL PROCEDURE 134 (2nd ed. 1999) ("Courts generally give grand juries considerable leeway in judging relevancy."); Jacob A. Stein, Glenn A. Mitchell & Basil J. Mezines, 3 ADMINISTRATIVE LAW 20–59 (2002) ("Subpoenas will be enforced as to any documents that 'are not plainly immaterial or irrelevant to the investigation.'").

[36] 18 U.S.C. § 2518(3). The court must also find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(3)(c).

[37] Kyllo v. United States, 533 U.S. 27, 33 (2001) ("A Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.") (*citing* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[38] 442 U.S. 735 (1979).

[39] *Id.* at 744 ("Petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business … thereby assuming the risk that the company would reveal to police the numbers he dialed.").

[40] *Cf.* Thygeson v. U.S. Bancroft, No. CU-03-467-ST 2004 WL 2066746 (D. Or. Sept. 15, 2004) ("When the information defendants collected was only the website addresses, rather than the actual content of the websites Thygeson visited, [the surveillance] is analogous to

a pen registry search, where in the Fourth Amendment context, courts have held that defendants have no reasonable expectation of privacy in the telephone numbers they dial because the numbers are conveyed to the telephone company."); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("When defendant entered into an agreement with Road Runner for Internet service, he knowingly revealed all information connected to the IP address …."); *see also infra* note 46. Billing records of ISPs may also be unprotected by the Fourth Amendment. United States v. Hambrick, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion) (holding that person does not have a reasonable expectation of privacy "in the account information given to the ISP in order to establish the e-mail account, [because it] is non-content information" disclosure of which "to a third party destroys the privacy expectation that might have existed previously"), available at 2000 U.S. App. LEXIS 18665, at *12. Indeed, some courts have held that the content of e-mail messages, once they are opened, deserve no Fourth Amendment protection because one assumes the risk the recipient will reveal it to others. United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996); United States v. Maxwell, 45 M.J. 406, 417–18 (C.A.A.F. 1996).

[41] 18 U.S.C. § 3123(a)(1)(2000).

[42] United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (the "judicial role in approving use of trap and trace devices is ministerial in nature").

[43] 18 U.S.C. § 3121(c) (2000).

[44] Most courts have held that companies that acquire clickstream data about where an Internet user goes on the Internet do not violate ECPA because the Web sites visited by the user have authorized the companies to access this information. *See* In re DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001); In re Toys R Us, Inc., Privacy Litig., No. C00-2746 2001 U.S. Dist. LEXIS 16947, at *28 (N.D. Cal. Oct. 9, 2001). Thus, government could also obtain routing information from these private companies, without using snoopware. However, some courts might consider that approach to be accessing "stored" information. *See, e.g.,* United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003). If so, government may have to obtain a subpoena. *See infra* text accompanying notes 65–69.

[45] See Richard Van Duizend, L. Paul Sutton & Charlotte A. Carter, *The Search Warrant Process: Preconceptions, Perceptions and Practices*, 47–48 (1985) (describing study of warrant process indicating varying degrees of judicial rubberstamping across jurisdictions).

[46] 425 U.S. 435 (1976).

[47] *Miller*, 425 U.S. at 443.

[48] *Id.* at 443 (emphasis added).

[49] *See* 5 U.S.C. § 552a(b) (2000) ("No agency shall disclose any record which is contained in a system of records … unless [listing 12 exceptions].").

[50] *Id.* § 552a(b)(7) (permitting disclosure "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the

record specifying the particular portion desired and the law enforcement activity for which the record is sought").

[51] *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 605 (1995)(most states lack "omnibus data protection laws," but rather have "scattered laws that provide only limited protections for personal information in the public sector."). One reason Florida is an attractive place to base an operation like MATRIX is that its public records law is quite extensive. *See* FLA. STAT. § 119.01 *et seq.* ("It is the policy of this state that all state, county and municipal records shall be open for personal inspection by any person.") Recognizing this problem, the Florida Supreme Court recently ordered a moratorium on the digitization of Florida's public records. Jason Krause, *Too Much Information? County Clerks Tussle with Nervous State Officials over Posting Court Records Online*, A.B.A. J., April 2004, at 24.

[52] 5 U.S.C. § 552a(m).

[53] *See* Hoofnagle, *supra* note 16, at 623 ("A database of information that originates at a CDB would not trigger the requirements of the Privacy Act [thus allowing CDBs] to amass huge databases that the government is legally prohibited from creating.").

[54] *Smith*, 442 U.S. at 744.

[55] *Miller*, 425 U.S. at 443.

[56] *Cf.* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); Jaffee v. Richmond, 518 U.S. 1, 15 (1996) ("Because we agree with the judgment of the state legislatures and the Advisory Committee that a psychotherapist-patient privilege will serve a public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth, … we hold that confidential communications between a licensed psychotherapist and her patients in the course of diagnosis or treatment are protected from compelled disclosure under Rule 501 of the Federal Rules of Evidence."); Whalen v. Roe, 429 U.S. 589, 605 (1977) (recognizing, in the context of a case involving disclosure of medical information, that a "statutory or regulatory duty to avoid unwarranted disclosures … in some circumstances … arguably has its roots in the Constitution").

[57] 45 C.F.R. § 164.512(f)(1)(ii)(B)(2005) (disclosure of medical records under HIPAA is permissible without permission of their subject if information is sought for law enforcement purposes through a grand jury subpoena). Some courts have required a greater showing to obtain medical records. *See, e.g.,* Doe v. Broderick, 225 F.3d 440, 450–51 (4th Cir. 2000) (finding *Miller* inapplicable to medical records); Haw. Psychiatric Soc., Dist. Branch of American Psychiatric Ass'n v. Ariyoshi, 481 F. Supp. 1028 (D. Haw. 1979); King v. State, 535 S.E.2d 432, 495 (Ga. 2000); Thurman v. State, 861 S.W.2d 96, 98 (Tex. Ct. App. 1993).

[58] 15 U.S.C. § 1681b(a)(1). Name, addresses, and places of employment can be obtained simply upon a request. *Id.* § 1681f.

[59] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Protection*, 75 S. CAL. L. REV. 1083, 1146 (2002).

[60] Chris Hoofnagle has made the argument that this ability to obtain information through a private agency circumvents the Privacy Act, which prohibits government from collecting such information unless there is a specific need for it. Hoofnagle, *supra* note 16, at 18.

[61] 12 U.S.C. § 3409. Furthermore, when subpoena power is not available to the government, it need only submit a formal written request for the information, a process this article calls extrajudicial certification. § 3408. Indeed, apparently banks sometimes still simply hand over information upon request. *See* David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* 106–108 (1989) (describing a number of cases in which banks surrendered account information to law enforcement officers simply upon request and describing a survey finding that 74% of banks did not inform their customers of their routine disclosures to law enforcement).

[62] Ellen S. Podgor & Jerry H. Israel, *White Collar Crime in a Nutshell*, 269 (2004).

[63] 18 U.S.C. § 2518(3)(2000).

[64] 18 U.S.C. § 2703(a) (2000); 2703(b)(1)(B). Further, a subpoena is only required when the information is sought from a "remote computer service" (e.g., a service available to the general public, like AOL). If the information is stored with a service not available to the general public (e.g., one run by an employer), then ECPA does not apply at all and government may obtain the stored information (content or identifying) simply upon a request. *See* 18 U.S.C. § 2703(a)(1–3); *see also* 18 U.S.C. § 2711(2)(2000) (defining remote computing service); U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 89 (July 2002), *available at* http://www.cybercrime.gov/s&s manual2002.htm.

[65] *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1421 (2004). This article is an extremely helpful roadmap and analysis of ECPA, which, unfortunately, I discovered only after wading through the statute myself. *Id.*

[66] *See* Clifford S. Fishman & Anne T. Mckenna, Wiretapping and Eavesdropping, § 26:9 (2nd ed. 1995) (explaining that Congress felt that when an e-mail stays on a server longer than 180 days the service provider is less like a Post Office and more like a storage facility).

[67] 18 U.S.C. § 2703(c)(1)(E)(2001) (describing information that can be obtained); § 2703(c)(3) ("A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.").

[68] § 2703(c) (describing requirements for a court order to obtain "records concerning electronic communication service or remote computing service").

[69] MCCORMICK ON EVIDENCE § 185 at 276–78 (John W. Strong ed., 5th ed. 1999)("Materiality … looks to the relation between the propositions that the evidence is offered … and the issues in the case …. A fact that is 'of consequence' is material …. It is enough if the item could reasonably show that a fact is slightly more probable than it would appear without that evidence.").

[70] § 2703(d) (providing court may quash or modify order if the request is "unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider").

[71] 50 U.S.C. 1861.

[72] *Id.*

[73] *Id.*, (b(2)(A).

[74] *Id.*, (g).

[75] *Id.,* (f)(2)(B).

[76] *Id.* (a judge may grant a petition "only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful").

[77] *Id.*, (a)(1). *See generally* Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEORGE WASHINGTON LAW REVIEW 1, 80–81 (2004). *See also* 18 U.S.C. 2709(b) (wire or electronic service providers); 20 U.S.C. § 1232g(j)(A) (school records).

[78] *Id.*, (d)(1).

[79] *Id.,* (f)(2)(a)(i).

[80] The amendments provide for annual audits of the Section 215 process and require the Department of Justice to provide Congress, on an annual basis, information about "the total number of applications made for orders approving requests for the production of tangible things; and the total number of such orders that were granted, modified, or denied."

[81] Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 694–695 (2004).

[82] Philip B. Heymann, *Terrorism, Freedom, and Security: Winning Without War* 154–56 (2003) (describing complaints from congresstional intelligence committees about the difficulty of obtaining information from the FBI and the CIA).

[83] 12 U.S.C. § 3414(a)(5)(A) ("financial records"); 18 U.S.C. § 2709(b) ("name, address, length of service and local and long distance toll billing records"). Again, the record-holder is prohibited from informing the target of the request. *Id.*, 3414(a)(5)(D).

[84] Section 3414(a)(5)(D); 18 U.S.C. § 2709(c).

[85] Kyle O'Dowd, *Congress Hands FBI "Patriot II" Snooping Power*, 28 *Champion* 18 (Feb. 2004).

[86] 31 U.S.C. § 5312.

[87] Doe v. Ashcroft, 334 F. Supp. 2d 431 (S.D.N.Y. 2004).

[88] Doe v. Gonzales, 386 F. Supp. 2d 66, 67 (D. Conn. 2005). Both *Gonzales* and *Ashcroft* were vacated as a result of the new legislation, described below. *See* Doe v. Gonzales, 2006 WL 1409351 (2nd Cir. 2006).

[89] *See, e.g.*, 18 U.S.C. § 2709(f).

[90] *See, e.g.*, 18 U.S.C. § 3511(a) and (b).

[91] 335 F. Supp. 2d, 496.

[92] *Id.* at 52.

[93] *See, e.g.*, 18 U.S.C. 2709(c)(1).

[94] Barton Gellman, *The FBI's Secret Scrutiny*, WASHINGTON POST, Nov. 6, 2005, A1 (reporting that only 1 out of scores of thousands of NSLs had been challenged by a third party through 2005, although it must be noted that the availability of judicial review during this period was unclear). *See also* Eric Lictblau & Mark Mazzetti, *Military is Expanding Its Intelligence Role in the U.S.*, NEW YORK TIMES, January 14, 2007, *at* A1 (reporting that the CIA and Pentagon have been using "noncompulsory" versions of the NSL to obtain information from banks, credit card companies and other financial institutions, virtually always without resistance.)

[95] Eric Lictblau, *Frustration over Limits on an Antiterror Law*, NEW YORK TIMES, Dec. 11, 2005, A1.

[96] Gellman, *The FBI's Secret Scrutiny*, A1. The Department of Justice later disputed this figure, stating that in 2005, 9,254 NSLs were issued that "related to U.S. persons." *See* 79 BNA CRIMINAL LAW REPORTER 161 (May 10, 2006); Lichblau & Mazzetti, *Military Expanding Its Intelligence Role*, (reporting that the Pentagon had sent NSL letters in roughly 500 investigations from 2002 to 2007).

[97] *See supra* note 5.

[98] 392 U.S. 1 (1968).

[99] Arguably, the "specific and articulable facts" ex parte subpoena required by 18 U.S.C. § 2703(d) is more difficult to obtain than an ordinary subpoena (and apparently Congress so believed), but for the reasons suggested above, *see supra* notes 69–72 and accompanying text, it is classified here as less protective than a regular subpoena, at least one that notifies the target.

[100] People who have worked at the Department of Justice state that, in practice, a certification order may be harder to obtain than a subpoena. Personal conversations with Orin Kerr (Feb. 17, 2005) and Paul Ohm (Jan. 20, 2005). But I rank the certification order lower in the hierarchy of protection because the judge plays such a minimal role; at least with a subpoena the judge is permitted to find a seizure invalid on relevance grounds, although he may rarely do so.

[101] For instance, there is no exclusionary sanction under ECPA, or under the Right to Financial Privacy Act. WHITEBREAD & SLOBOGIN, *supra* note 9, at 344–45; United States v. Kington, 801 F.2d 733, 734 (5th Cir. 1986). Nor are damages actions a significant deterrent, given the intangible nature of the harm involved. *Cf.* Doe v. Chao, 306 F.3d 170, 177 (4th Cir. 2002) (holding that, under ECPA, "a person must sustain actual damages to be entitled to the statutory minimum damages award" of $1,000).

Table of Cases

Capullupo v. FMC Corp., 126 F.R.D. 545 (D. Minn. 1989).

Carefirst of Maryland, Inc. v. Carefirst Pregnancy Centers, 334 F. 3d 390 (4th Cir. 2003).

Carter v. Gibbs, 909 F. 2d 1450 (Fed. Cir. 1990) (en banc), superseded in nonrelevant part, Pub. L. No. 103-424, § 9(c), 108 Stat. 4361 (1994).

Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

Charter Communs., Inc. v. Charter Communs., Inc., 393 F.3d 771 (8th Cir. 2005).

Chemtex, LLC v. St. Anthony Enterprises, Inc., 2004 U.S. Dist. LEXIS 6031 (S.D.N.Y. 2004).

City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

Compaq Corp. v. Packard Bell Elecs., Inc., 163 F.R.D. 329 (N.D. Cal. 1995).

Computer Assoc. Int'l, Inc. v. Am. Fundware, Inc., 133 F.R.D. 166 (D. Colo. 1990).

Connecticut Mut. Life Ins. Co. v. Shields, 18 F.R.D. 448 (S.D.N.Y. 1955).

Convolve v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004).

Costa v. Keppel Singmarine Dockyard PTE, Ltd., 2003 U.S. Dist. LEXIS 16295 (C.D. Cal. 2003).

Crandall v. City & County of Denver, 2006 U.S. Dist. LEXIS 35051 (D. Colo. 2006).

Crown Park Corp. v. Dominican Sisters, 2006 U.S. Dist. LEXIS 19739 (E.D. Mich. 2006).

Cunningham v. Bower, 1989 U.S. Dist. LEXIS 3914 (D. Kan. 1989).

Cuno, Inc. v. Pall Corp., 116 F.R.D. 279 (E.D. N.Y. 1987).

Curto v. Medical World Communs., Inc., 2006 U.S. Dist. LEXIS 29387 (E.D. N.Y. 2006).

Dart Industries Co. v. Westwood Chemical Co., 649 F. 2d 646 (9th Cir. 1980).

Del Campo v. Kennedy, 2006 U.S. Dist. LEXIS 85462 (N.D. Cal. 2005).

Dendrite Int'l v. Doe No. 3, 342 N.J. Super. 1345, 775 A.2d 756 (2001).

DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764 (D. S.C. 2004).

Doe v. Broderick, 225 F.3d 440 (4th Cir. 2000).

Doe v. Chao, 306 F.3d 170 (4th Cir. 2002).

Earthlink, Inc. v. Pope, 2006 U.S. Dist. LEXIS 66596 (N.D. Ga. 2006).

E*Trade Secs. LLC v. Deutsche Bank AG, 230 F.R.D. 582, 592 (D. Minn. 2005).

Eggleston v. Wal-Mart Stores, E., LP, 2006 U.S. Dist. LEXIS 12849 (E.D. Va. 2006).

El-Banna v. Bush, 2005 U.S. Dist. LEXIS 16880 (D. D.C. 2005).

F.C. Cycles Int'l, Inc. v. FILA Sport S.p.A., 184 F.R.D. 64 (D. Md. 1998).

Ferguson v. City of Charleston, 532 U.S. 67 (2001).

First Act, Inc. v. Brook Mays Music Company, 311 F. Supp. 2d 258 (D. Mass. 2004).

Florida v. Royer, 460 U.S. 491 (1983).

In re Horowitz, 482 F.2d 72 (2nd Cir. 1973).

In re Parmalat Secs. Litig., 2006 U.S. Dist. LEXIS 88629 (S.D.N.Y. 2006).

In re Philip Serv. Corp. Secs. Litig., 2005 U.S. Dist. LEXIS 22998 (S.D.N.Y. 2005).

In re Sealed Case, 877 F.2d 976 (D.C. Cir. 1989).

In re Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. 2001).

India Brewing, Inc. v. Miller Brewing Co., 2006 U.S. Dist. LEXIS 50550 (D. Wis. 2006).

Inset Systems, Inc. v. Instruction Set, 937 F. Supp. 161 (D. Conn. 1996).

Inst. for Motivational Living, Inc. v. Doulos Inst. for Strategic Consulting, Inc., 110 Fed. Appx. 283 (3rd Cir. 2004).

Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999).

Intercom, Inc. v. Bell Atlantic Internet Solutions, Inc., 205 F. 3d 1244 (10th Cir. 2000).

International Shoe Co. v. Washington, 326 U.S. 310 (1945).

Internet Doorways, Inc. v. Parks, 138 F. Supp. 2d 773 (S.D. Miss. 2001).

J.C. Associates v. Fid. & Guar. Ins. Co., 2006 U.S. Dist. LEXIS 32919 (D. D.C. 2006).

Jaffe v. Richmond, 518 U.S. 1 (1996).

John Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005).

Katz v. United States, 389 U.S. 347 (1967).

King v. State, 535 S.E.2d 432 (Ga. 2000).

Koch Materials Co. v. Shore Slurry Seal, Inc., 208 F.R.D. 109 (D. N.J. 2002).

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir.), *cert. denied* 537 U.S. 1193 (2003).

Kronisch v. United States, 150 F.3d 112 (2nd Cir. 1998).

Kyllo v. United States, 533 U.S. 27 (2001).

Lakin v. Prudential Securities, Inc., 348 F. 3d 704 (8th Cir. 2003).

Lava Trading, Inc. v. Hartford Fire Ins. Co., 2005 U.S. Dist. LEXIS 466 (S.D.N.Y. 2005).

Leon v. IDX Sys. Corp., 464 F.3d 951 (9th Cir. 2006).

Lilly v. Va., 527 U.S. 116 (1999).

Madden v. Wyeth, 2003 U.S. Dist. LEXIS 6427 (N.D. Tex. 2003).

Malcolm v. Esposito, 63 Va. Cir. 440 (Fairfax 2003).

McGee v. International Life Ins. Co., 355 U.S. 220 (1957).

McPeek v. Ashcroft, 202 F.R.D. 31 (D. D.C. 2001).

Medtronic Sofamor Danek, Inc. v. Sofamor Danek Holdings, Inc,. 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. 2003).

Powers v. Thomas M. Cooley Law Sch., 2006 U.S. Dist. LEXIS 67706 (W.D. Mich. 2006).

Pueblo of Laguna v. United States, 60 Fed. Cl. 133 (2004).

Quinby v. WestLB AG, 2006 U.S. Dist. LEXIS 1178 (S.D.N.Y. 2006).

Rambus, Inc. v. Infineon Technologies, 222 F.R.D. 280 (E.D. Va. 2004).

Recording Indus. Ass'n of Am., Inc. v. Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945 (M.D. N.C. 2005).

Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, 351 F.3d 1229 (D.C. Cir.), *cert. denied* 543 U.S. 924 (2004).

Reno v. ACLU, 521 U.S. 844 (1997).

Rescuecom Corporation v. Hyams, 2006 U.S. Dist. LEXIS 45282 (N.D. N.Y. 2006).

Revel v. Lidov, 317 F. 3d 467 (5th Cir. 2002).

Rice v. Karsch, 154 Fed. Appx. 454 (6th Cir. 2005).

Rowe Entm'l, Inc. v. William Morris Agency, 205 F.R.D. 421 (S.D.N.Y. 2002).

Schnall v. Annuity & Life Re (Holdings), Ltd., 2004 U.S. Dist. LEXIS 209 (D. Conn. 2004).

SEC v. Cassano, 189 F.R.D. 83 (S.D.N.Y. 1999).

Semroth v. City of Wichita, 2006 U.S. Dist. LEXIS 83363 (D. Kan. 2006).

Shaffer v. Heitner, 433 U.S. 186 (1977).

Shoppers Food Warehouse v. Moreno, 746 A.2d 320 (D.C. 2000).

Silvestri v. General Motors Corp., 271 F.3d 583 (4th Cir. 2001).

Simon Property Group, L.P. v. MySimon, Inc., 194 F.R.D. 639 (D. Ind. 2000).

Snowney v. Harrah's Entertainment, Inc., 35 Cal. 4th 1054 (2005).

Sony Music Entm't, Inc. v. Does 1 – 40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004).

St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773 (S.D. Tex. 1999).

State v. Armstead, 432 So. 2d 837 (La. 1983).

State v. Cookson, 361 S.W. 2d 683 (Mo. 1962).

Standard Dyeing & Finishing Co. v. Arma Textile Printers Corp., 1987 U.S. Dist. LEXIS 868 (S.D.N.Y. 1987).

State of North Carolina v. Taylor, 632 S.E. 2d 218 (N.C. App. 2006).

Super Film of Am., Inc. v. UCB Films, Inc., 219 F.R.D. 649 (D. Kan. 2004).

Talbott v. City of O'Fallon, 2006 U.S. Dist. LEXIS 49461 (E.D. Mo. 2006).

Tanne v. Autobytel, Inc., 226 F.R.D. 659 (C.D. Cal. 2005).

Texaco v. P.R., Inc. v. Dep't of Consumer Affairs, 60 F.3d 867 (1st Cir. 1995).

The Cadle Company v. Schlichtmann, 123 Fed. Appx. 675 (6th Cir. 2005).

United States v. Whitaker, 127 F. 3d 595 (7th Cir. 1997).

United States EEOC v. E. I. DuPont de Nemours & Co., 2004 U.S. Dist. LEXIS 20753 (D. La. 2004).

United States ex rel Smith v. Boeing Co., 2005 U.S. Dist. LEXIS 36890 (D. Kan. 2005).

United States ex rel Tyson v. Amerigroup Ill., Inc., 2005 U.S. Dist. LEXIS 24929 (N.D. Ill. 2005).

Visa Int'l Serv. Assoc. v. JSL Corp., 2006 U.S. Dist. LEXIS 77451 (D. Nev. 2006).

Visage Spa v. Salon Visage, Inc., 2006 U.S. Dist. LEXIS 51824 (E.D. Mich. 2006).

Waka v. DCKickball, 2006 U.S. Dist. LEXIS 34501 (E.D. Va. 2006).

Westcoat v. Bayer Cropscience LP, 2006 U.S. Dist. LEXIS 79756 (E.D. Mo. 2006).

Whalen v. Roe, 429 U.S. 589 (1977).

Wiginton v. CB Richard Ellis, Inc., 229 F.R.D. 568 (N.D. Ill. 2004).

Williams v. Mass. Mutual Life Ins. Co., 226 F.R.D. 144 (D. Mass. 2005).

Williams v. Spring/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005).

Winig v. Cingular Wireless LLC, 2006 U.S. Dist. LEXIS 83116 (D. Cal. 2006).

World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980).

Zakre v. Norddeutsche Landesbank Girozentrale, 2004 U.S. Dist. LEXIS 6026 (S.D.N.Y. 2004).

Zippo Manufacturing Company v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).

About the Authors

Marian K. Riedy graduated from Harvard Law School in 1981. She clerked for Chief Judge Harrison L. Winter, U.S. Court of Appeals, Fourth Circuit, and has since practiced as a litigator. She has worked in large and small firms, and litigated a wide range of cases, from complex, international trade disputes to jury trials in local courts. She also has an M.B.A. from Georgetown University's McDonough School of Business. Ms. Riedy is the founding partner of Riedy & Beros, LLC, an e-litigation consulting company.

Suman Beros is the cofounder of Riedy & Beros, LLC, and has been designing, implementing, and operating business solutions in health care and other industries using established and emerging information technologies, since graduating in 1985 from Pace University, where he received an M.B.A. in information systems and marketing management.

Kim Sperduto is the managing director of The Sperduto Law Firm, PLC, a complex commercial litigation boutique in Washington, D.C. Mr. Sperduto received an undergraduate degree from Vanderbilt University and a law degree and a master's degree in public policy from Duke University. After clerking for Federal Judge Thomas C. Platt in New York, he worked at large litigation firms in New York City before starting his own firm 15 years ago.

Index

Recent Titles in the Artech House Telecommunications Library

Vinton G. Cerf, Senior Series Editor

Access Networks: Technology and V5 Interfacing, Alex Gillespie

Achieving Global Information Networking, Eve L. Varma et al.

Advanced High-Frequency Radio Communications, Eric E. Johnson et al.

ATM Interworking in Broadband Wireless Applications, M. Sreetharan and S. Subramaniam

ATM Switches, Edwin R. Coover

ATM Switching Systems, Thomas M. Chen and Stephen S. Liu

Broadband Access Technology, Interfaces, and Management, Alex Gillespie

Broadband Local Loops for High-Speed Internet Access, Maurice Gagnaire

Broadband Networking: ATM, SDH, and SONET, Mike Sexton and Andy Reid

Broadband Telecommunications Technology, Second Edition, Byeong Lee, Minho Kang, and Jonghee Lee

The Business Case for Web-Based Training, Tammy Whalen and David Wright

Centrex or PBX: The Impact of IP, John R. Abrahams and Mauro Lollo

Chinese Telecommunications Policy, Xu Yan and Douglas Pitt

Communication and Computing for Distributed Multimedia Systems, Guojun Lu

Communications Technology Guide for Business, Richard Downey, Seán Boland, and Phillip Walsh

Community Networks: Lessons from Blacksburg, Virginia, Second Edition, Andrew M. Cohill and Andrea Kavanaugh, editors

Component-Based Network System Engineering, Mark Norris, Rob Davis, and Alan Pengelly

Computer Telephony Integration, Second Edition, Rob Walters

Customer-Centered Telecommunications Services Marketing, Karen G. Strouse

Delay- and Disruption-Tolerant Networking, Stephen Farrell and Vinny Cahill

Deploying and Managing IP over WDM Networks, Joan Serrat and Alex Galis, editors

Desktop Encyclopedia of the Internet, Nathan J. Muller

Digital Clocks for Synchronization and Communications, Masami Kihara, Sadayasu Ono, and Pekka Eskelinen

Digital Modulation Techniques, Second Edition, Fuqin Xiong

E-Commerce Systems Architecture and Applications, Wasim E. Rajput

Engineering Internet QoS, Sanjay Jha and Mahbub Hassan

Error-Control Block Codes for Communications Engineers, L. H. Charles Lee

Essentials of Modern Telecommunications Systems, Nihal Kularatna and Dileeka Dias

FAX: Facsimile Technology and Systems, Third Edition, Kenneth R. McConnell, Dennis Bodson, and Stephen Urban

Fundamentals of Network Security, John E. Canavan

Gigabit Ethernet Technology and Applications, Mark Norris

The Great Telecom Meltdown, Fred R. Goldstein

Guide to ATM Systems and Technology, Mohammad A. Rahman

A Guide to the TCP/IP Protocol Suite, Floyd Wilder

Home Networking Technologies and Standards, Theodore B. Zahariadis

Implementing Value-Added Telecom Services, Johan Zuidweg

Information Superhighways Revisited: The Economics of Multimedia, Bruce Egan

Installation and Maintenance of SDH/SONET, ATM, xDSL, and Synchronization Networks, José M. Caballero et al.

Integrated Broadband Networks: TCP/IP, ATM, SDH/SONET, and WDM/Optics, Byeong Gi Lee and Woojune Kim

Internet E-mail: Protocols, Standards, and Implementation, Lawrence Hughes

Introduction to Telecommunications Network Engineering, Second Edition, Tarmo Anttalainen

Introduction to Telephones and Telephone Systems, Third Edition, A. Michael Noll

An Introduction to U.S. Telecommunications Law, Second Edition, Charles H. Kennedy

IP Convergence: The Next Revolution in Telecommunications, Nathan J. Muller

LANs to WANs: The Complete Management Guide, Nathan J. Muller

The Law and Regulation of Telecommunications Carriers, Henk Brands and Evan T. Leo

Litigating with Electronically Stored Information, Marian K. Riedy, Suman Beros, and Kim Sperduto

Managing Internet-Driven Change in International Telecommunications, Rob Frieden

Marketing Telecommunications Services: New Approaches for a Changing Environment, Karen G. Strouse

Mission-Critical Network Planning, Matthew Liotine

Multimedia Communications Networks: Technologies and Services, Mallikarjun Tatipamula and Bhumip Khashnabish, editors

Next Generation Intelligent Networks, Johan Zuidweg

Open Source Software Law, Rod Dixon

Performance Evaluation of Communication Networks, Gary N. Higginbottom

Performance of TCP/IP over ATM Networks, Mahbub Hassan and Mohammed Atiquzzaman

The Physical Layer of Communications Systems, Richard A. Thompson, David Tipper, Prashant Krishnamurthy, and Joseph Kabara

Practical Guide for Implementing Secure Intranets and Extranets, Kaustubh M. Phaltankar

Practical Internet Law for Business, Kurt M. Saunders

Practical Multiservice LANs: ATM and RF Broadband, Ernest O. Tunmann

Principles of Modern Communications Technology, A. Michael Noll

A Professional's Guide to Data Communication in a TCP/IP World, E. Bryan Carne

Programmable Networks for IP Service Deployment, Alex Galis et al., editors

Protocol Management in Computer Networking, Philippe Byrnes

Pulse Code Modulation Systems Design, William N. Waggener

Reorganizing Data and Voice Networks: Communications Resourcing for Corporate Networks, Thomas R. Koehler

Security, Rights, and Liabilities in E-Commerce, Jeffrey H. Matsuura

Service Assurance for Voice over WiFi and 3G Networks, Richard Lau, Ram Khare, and William Y. Chang

Service Level Management for Enterprise Networks, Lundy Lewis

SIP: Understanding the Session Initiation Protocol, Second Edition, Alan B. Johnston

Smart Card Security and Applications, Second Edition, Mike Hendry

SNMP-Based ATM Network Management, Heng Pan

Spectrum Wars: The Policy and Technology Debate, Jennifer A. Manner

Strategic Management in Telecommunications, James K. Shaw

Strategies for Success in the New Telecommunications Marketplace, Karen G. Strouse

Successful Business Strategies Using Telecommunications Services, Martin F. Bartholomew

Telecommunications Cost Management, S. C. Strother

Telecommunications Department Management, Robert A. Gable

Telecommunications Deregulation and the Information Economy, Second Edition, James K. Shaw

Telecommunications Technology Handbook, Second Edition, Daniel Minoli

Telemetry Systems Engineering, Frank Carden, Russell Jedlicka, and Robert Henry

Telephone Switching Systems, Richard A. Thompson

Understanding Modern Telecommunications and the Information Superhighway, John G. Nellist and Elliott M. Gilbert

Understanding Networking Technology: Concepts, Terms, and Trends, Second Edition, Mark Norris

Understanding Voice over IP Security, Alan B. Johnston and David M. Piscitello

Videoconferencing and Videotelephony: Technology and Standards, Second Edition, Richard Schaphorst

Visual Telephony, Edward A. Daly and Kathleen J. Hansell

Wide-Area Data Network Performance Engineering, Robert G. Cole and Ravi Ramaswamy

Winning Telco Customers Using Marketing Databases, Rob Mattison

WLANs and WPANs Towards 4G Wireless, Ramjee Prasad and Luis Muñoz

World-Class Telecommunications Service Development, Ellen P. Ward

For further information on these and other Artech House titles, including previously considered out-of-print books now available through our In-Print-Forever® (IPF®) program, contact:

Artech House
685 Canton Street
Norwood, MA 02062
Phone: 781-769-9750
Fax: 781-769-6334
e-mail: artech@artechhouse.com

Artech House
46 Gillingham Street
London SW1V 1AH UK
Phone: +44 (0)20 7596-8750
Fax: +44 (0)20 7630-0166
e-mail: artech-uk@artechhouse.com

Find us on the World Wide Web at: www.artechhouse.com