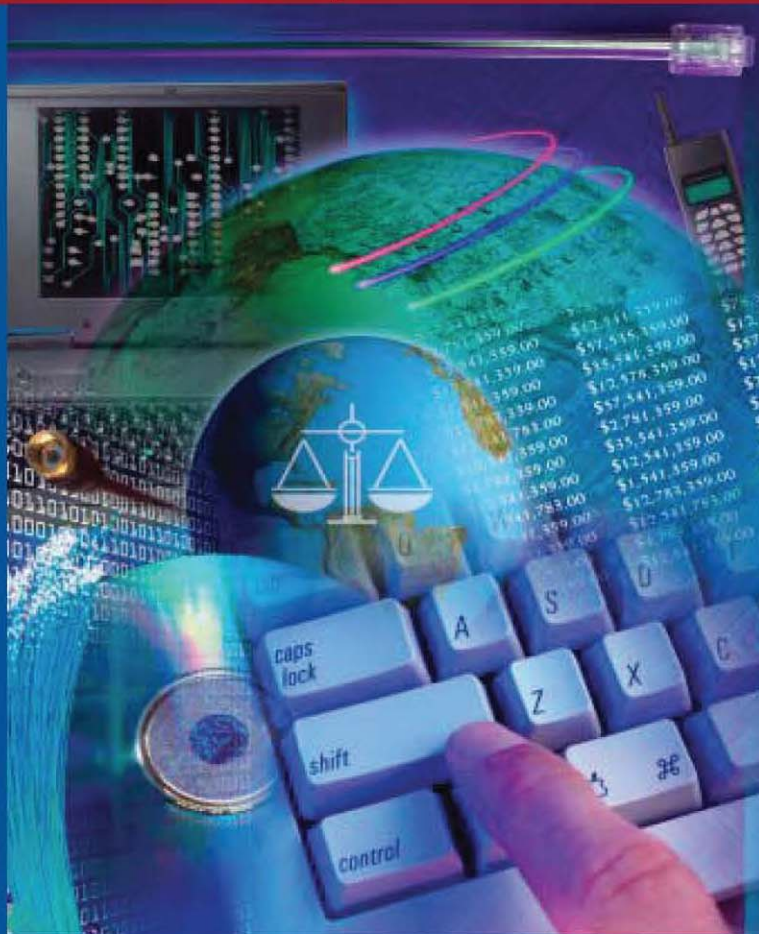


ASPEN PUBLISHERS

# ESI HANDBOOK

SOURCES, TECHNOLOGY, AND PROCESS



ADAM I. COHEN • G. EDWARD KALBAUGH



**Wolters Kluwer**  
Law & Business

ASPEN PUBLISHERS

# ESI HANDBOOK

## Sources, Technology and Process

---

Adam I. Cohen

G. Edward Kalbaugh



Wolters Kluwer

Law & Business

AUSTIN BOSTON CHICAGO NEW YORK THE NETHERLANDS

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought.

—From a *Declaration of Principles* jointly adopted  
by a Committee of the American Bar Association  
and a Committee of Publishers and Associations

© 2009 Aspen Publishers. All Rights Reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher. Requests for permission to reproduce content should be directed to the Aspen Publishers website at [www.aspenpublishers.com](http://www.aspenpublishers.com), or a letter of intent should be faxed to the permissions department at 212-771-0803.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

Library of Congress Cataloging-in-Publication Data

Cohen, Adam I., 1968-

ESI handbook : sources, technology, and process / Adam I. Cohen, G. Edward Kalbaugh.

p. cm.—(Law & business)

Includes bibliographical references and index.

ISBN 978-0-7355-6267-7 (alk. paper)

1. Electronic discovery (Law)—United States. 2. Electronic records. 3. Electronic data processing. I. Kalbaugh, G. Edward. II. Title.

KF8902.E42C65 2008

347.73'72—dc22

2008042041

---

## About Wolters Kluwer Law & Business

Wolters Kluwer Law & Business is a leading provider of research information and workflow solutions in key specialty areas. The strengths of the individual brands of Aspen Publishers, CCH, Kluwer Law International and Loislaw are aligned within Wolters Kluwer Law & Business to provide comprehensive, in-depth solutions and expert-authored content for the legal, professional and education markets.

**CCH** was founded in 1913 and has served more than four generations of business professionals and their clients. The CCH products in the Wolters Kluwer Law & Business group are highly regarded electronic and print resources for legal, securities, antitrust and trade regulation, government contracting, banking, pension, payroll, employment and labor, and healthcare reimbursement and compliance professionals.

**Aspen Publishers** is a leading information provider for attorneys, business professionals and law students. Written by preeminent authorities, Aspen products offer analytical and practical information in a range of specialty practice areas from securities law and intellectual property to mergers and acquisitions and pension/benefits. Aspen's trusted legal education resources provide professors and students with high-quality, up-to-date and effective resources for successful instruction and study in all areas of the law.

**Kluwer Law International** supplies the global business community with comprehensive English-language international legal information. Legal practitioners, corporate counsel and business executives around the world rely on the Kluwer Law International journals, loose-leaves, books and electronic products for authoritative information in many areas of international legal practice.

**Loislaw** is a premier provider of digitized legal content to small law firm practitioners of various specializations. Loislaw provides attorneys with the ability to quickly and efficiently find the necessary legal information they need, when and where they need it, by facilitating access to primary law as well as state-specific law, records, forms and treatises.

Wolters Kluwer Law & Business, a unit of Wolters Kluwer, is headquartered in New York and Riverwoods, Illinois. Wolters Kluwer is a leading multinational publisher and information services company.

---

---

## ASPEN PUBLISHERS SUBSCRIPTION NOTICE

This Aspen Publishers product is updated on a periodic basis with supplements to reflect important changes in the subject matter. If you purchased this product directly from Aspen Publishers, we have already recorded your subscription for the update service.

If, however, you purchased this product from a bookstore and wish to receive future updates and revised or related volumes billed separately with a 30-day examination review, please contact our Customer Service Department at 1-800-234-1660 or send your name, company name (if applicable), address, and the title of the product to:

**ASPEN PUBLISHERS  
7201 McKinney Circle  
Frederick, MD 21704**

---

### **Important Aspen Publishers Contact Information**

- To order any Aspen Publishers title, go to [www.aspenpublishers.com](http://www.aspenpublishers.com) or call 1-800-638-8437.
- To reinstate your manual update service, call 1-800-638-8437.
- To contact Customer Care, e-mail [customer.care@aspenpublishers.com](mailto:customer.care@aspenpublishers.com), call 1-800-234-1660, fax 1-800-901-9075, or mail correspondence to Order Department, Aspen Publishers, PO Box 990, Frederick, MD 21705.
- To review your account history or pay an invoice online, visit [www.aspenpublishers.com/payinvoices](http://www.aspenpublishers.com/payinvoices).



**Wolters Kluwer**

Law & Business

# TABLE OF CONTENTS

---

ABOUT THE AUTHORS.....	xiii
ACKNOWLEDGEMENTS .....	xv
FOREWORD.....	xvii
DISCLAIMER.....	xix

## PART I

### INTRODUCTION AND OVERVIEW

#### Chapter 1

INTRODUCTION.....	1-1
-------------------	-----

#### Chapter 2

OVERVIEW OF THE ELECTRONIC DISCOVERY PROCESS.....	2-1
---	-----

§ 2.01	Introduction.....	2-3
§ 2.02	Forms of ESI.....	2-3
	[A] Native Files.....	2-3
	[B] Metadata.....	2-3
	[C] Image Files .....	2-3
§ 2.03	Electronic Discovery Process Lifecycle .....	2-4
	[A] Phase 1: Preparation .....	2-5
	[B] Phase 2: Search and Collection.....	2-5
	[C] Phase 3: Processing .....	2-5
	[D] Phase 4: Culling.....	2-5
	[E] Phase 5: Review and Analysis .....	2-5
	[F] Phase 6: Production and Presentation .....	2-6
§ 2.04	Issues and Concerns .....	2-6
§ 2.05	Recommendations.....	2-6

#### Chapter 3

OVERVIEW OF THE INFORMATION TECHNOLOGY INFRASTRUCTURE.....	3-1
--	-----

§ 3.01	Introduction.....	3-3
§ 3.02	Networks and Components.....	3-3
	[A] Network Peripherals .....	3-4
	[B] Clients .....	3-4
	[C] Servers.....	3-4
§ 3.03	Types of Networks .....	3-5
	[A] Local Area Networks.....	3-5
	[B] Metropolitan Area Networks.....	3-5
	[C] Wide Area Networks .....	3-5
§ 3.04	Functional Systems.....	3-6
§ 3.05	Information Technology Organization.....	3-6
	[A] Introduction.....	3-6
	[B] Chief Information Officers (CIO) .....	3-6
	[C] Chief Technology Officers (CTO) .....	3-6
	[D] Chief Security Officers (CSO) .....	3-6

[E]	Network Administrators .....	3-6
[F]	Data Administrators.....	3-7
[G]	Email Administrators.....	3-7
[H]	System/Application Administrators and Developers .....	3-7
[I]	Records Administrators .....	3-7
[J]	Business Unit Heads.....	3-7
§ 3.06	Issues and Concerns .....	3-7
§ 3.07	Recommendations.....	3-8

**PART II**  
**SOURCES OF ELECTRONICALLY STORED INFORMATION**

<b>Chapter 4</b>	<b>INTRODUCTION TO SOURCES OF ESI.....</b>	<b>4-1</b>
------------------	--	------------

<b>Chapter 5</b>	<b>OVERVIEW OF FILE AND STORAGE SYSTEMS .....</b>	<b>5-1</b>
------------------	---	------------

§ 5.01	File Systems.....	5-3
[A]	Network File Systems.....	5-3
[B]	Database File Systems.....	5-3
[C]	Transactional File Systems.....	5-3
[D]	Distributed File Systems .....	5-4
§ 5.02	Storage Systems.....	5-4
[A]	Computer Memory .....	5-4
[B]	Secondary Storage .....	5-4
[C]	Removable and Offline Storage Media.....	5-4
[D]	Online Mass Storage.....	5-4
[E]	Storage Virtualization.....	5-6
§ 5.03	Issues and Concerns .....	5-6
§ 5.04	Recommendations.....	5-6

<b>Chapter 6</b>	<b>NATIVE FILES AND METADATA.....</b>	<b>6-1</b>
------------------	---------------------------------------	------------

§ 6.01	Native Files.....	6-3
§ 6.02	Metadata.....	6-3
§ 6.03	Issues and Concerns .....	6-4
§ 6.04	Recommendations.....	6-4
§ 6.05	More Information .....	6-5

<b>Chapter 7</b>	<b>EMAIL AND COLLABORATION SYSTEMS .....</b>	<b>7-1</b>
------------------	--	------------

§ 7.01	Standard Email Systems.....	7-3
§ 7.02	Microsoft Exchange Server .....	7-4
§ 7.03	Lotus Notes.....	7-4
§ 7.04	Instant Messaging.....	7-5
§ 7.05	Issues and Concerns .....	7-5
§ 7.06	Recommendations.....	7-6

<b>Chapter 8</b>	<b>DATABASES.....</b>	<b>8-1</b>
------------------	-----------------------	------------

§ 8.01	Flat Database .....	8-3
§ 8.02	Hierarchical Database.....	8-3

## CONTENTS

---

§ 8.03	Network Database.....	8-3
§ 8.04	Object Database.....	8-3
§ 8.05	Dimensional Database.....	8-3
§ 8.06	Data Warehouse.....	8-4
§ 8.07	Relational Databases.....	8-4
§ 8.08	Issues and Concerns.....	8-4
§ 8.09	Recommendations.....	8-4

### Chapter 9

#### FILE SERVERS..... 9-1

§ 9.01	Description.....	9-3
§ 9.02	Issues and Concerns.....	9-4
§ 9.03	Recommendations.....	9-4

### Chapter 10

#### ENTERPRISE STORAGE SYSTEMS ..... 10-1

§ 10.01	Introduction and Background.....	10-3
§ 10.02	Strategic Issues.....	10-3
§ 10.03	Storage Convergence.....	10-4
	[A] 10 Gigabit Ethernet (10GbE).....	10-4
	[B] Serial Attached SCSI (SAS).....	10-4
	[C] Internet SCSI (iSCSI).....	10-4
	[D] High Capacity Solid State Drive (hSSD).....	10-4
	[E] RAM Hard Disk.....	10-5
§ 10.04	Open Source Storage Products.....	10-5
	[A] Amanda.....	10-5
	[B] FreeNAS.....	10-5
	[C] Areca Backup.....	10-5
	[D] ZFS.....	10-5
	[E] Lustre.....	10-6
	[F] Samba.....	10-6
	[G] OpenAFS.....	10-6
§ 10.05	Hybrid and Bridging Systems.....	10-6
§ 10.06	Deduplication.....	10-6
§ 10.07	Storage Virtualization.....	10-7
§ 10.08	Grid Computing.....	10-7
§ 10.09	Application Fabrics.....	10-8
§ 10.10	Web-Based Storage.....	10-8
§ 10.11	Tape-Based Storage.....	10-9
	[A] Virtual Tape Library (VTL).....	10-9
	[B] Conditions Affecting Tape Cartridge Reliability.....	10-9
	[C] Tape Restoration.....	10-10
§ 10.12	Issues and Concerns.....	10-12
§ 10.13	Recommendations.....	10-12

### Chapter 11

#### DESKTOP AND PORTABLE COMPUTERS..... 11-1

§ 11.01	Introduction and Background.....	11-3
§ 11.02	Issues and Concerns.....	11-3
§ 11.03	Recommendations.....	11-4

**Chapter 12****MOBILE DEVICES ..... 12-1**

§ 12.01	Introduction.....	12-3
§ 12.02	Characteristics of Mobile Devices .....	12-3
§ 12.03	Mobile Device ESI .....	12-3
	[A] Voice Messages .....	12-3
	[B] Email.....	12-3
	[C] Office Applications.....	12-4
	[D] Multimedia.....	12-4
	[E] Instant Messaging .....	12-4
	[F] Text Messaging.....	12-4
	[G] Location-Based ESI.....	12-4
§ 12.04	Issues and Concerns .....	12-5
§ 12.05	Recommendations.....	12-5

**Chapter 13****MULTIMEDIA AND VIDEO ..... 13-1**

§ 13.01	Multimedia.....	13-3
§ 13.02	Video.....	13-3
§ 13.03	Issues and Concerns .....	13-3
§ 13.04	Recommendations.....	13-4

**Chapter 14****REMOVABLE STORAGE DEVICES/MEDIA ..... 14-1**

§ 14.01	Introduction and Background.....	14-3
§ 14.02	Types of Removable Storage Devices .....	14-3
	[A] Magnetic Drives .....	14-3
	[B] Optical Drives.....	14-3
	[C] Solid State Disk (SSD).....	14-4
	[D] Hybrid Devices .....	14-4
§ 14.03	Issues and Concerns .....	14-5
§ 14.04	Recommendations.....	14-5

**Chapter 15****VOICE MAIL ..... 15-1**

§ 15.01	Description.....	15-3
§ 15.02	Issues and Concerns .....	15-3
§ 15.03	Recommendations.....	15-3

**PART III****PERFORMING ELECTRONIC DISCOVERY****Chapter 16****INTRODUCTION..... 16-1**

§ 16.01	e-Discovery Lifecycle.....	16-3
§ 16.02	FRCP 2006 Amendments .....	16-3
	[A] Early Attention to Electronic Discovery: Rules 16(b), 26(a)(1) & 26(f).....	16-3
	[B] Two-Tier Procedure for Discovery of Electronic Information: Rule 26(b)(2)(B).....	16-4
	[C] Privilege Waiver and Inadvertent Disclosure: Rule 26(b)(5).....	16-4
	[D] Production Format for Electronic Information: Rule 34(b) .....	16-4
	[E] Avoidance of Spoliation Sanctions: Rule 37(g) .....	16-4

## CONTENTS

---

	[F] Inspection or Sampling: Rule 34(a) .....	16-5
	[G] Interrogatories: Rule 33(d) .....	16-5
	[H] Electronic Discovery from Non-Parties: Rule 45 .....	16-5
§ 16.03	Chapters in Part 3 .....	16-5
 <b>Chapter 17</b>		
<b>MANAGEMENT AND ADMINISTRATION .....</b>		<b>17-1</b>
§ 17.01	Litigation Response Plan (LRP).....	17-3
	[A] Resources .....	17-3
	[B] IT Infrastructure .....	17-3
	[C] ESI Hold and Preservation .....	17-4
	[D] Control and Oversight .....	17-4
	[E] Reporting .....	17-4
§ 17.02	e-Discovery Project Management .....	17-5
 <b>Chapter 18</b>		
<b>STANDARDS AND BEST PRACTICES .....</b>		<b>18-1</b>
§ 18.01	Auditability .....	18-3
§ 18.02	Chain-of-Custody .....	18-3
§ 18.03	Copying and Fingerprinting Original ESI.....	18-4
§ 18.04	Custodian and Key Person Interviews .....	18-5
§ 18.05	Data Sampling .....	18-6
§ 18.06	Metrics and Measurement .....	18-6
§ 18.07	Quality Control .....	18-7
§ 18.08	Coding Manual .....	18-7
§ 18.09	Security .....	18-8
 <b>Chapter 19</b>		
<b>FORENSIC CONSIDERATIONS .....</b>		<b>19-1</b>
§ 19.01	Introduction and Background.....	19-3
§ 19.02	Issues and Concerns .....	19-3
§ 19.03	Recommendations.....	19-4
 <b>Chapter 20</b>		
<b>SEARCH AND RETRIEVAL CONSIDERATIONS.....</b>		<b>20-1</b>
§ 20.01	Introduction.....	20-3
§ 20.02	Search Techniques.....	20-3
§ 20.03	Issues and Concerns .....	20-4
§ 20.04	Recommendations.....	20-4
 <b>Chapter 21</b>		
<b>PREPARATION AND PRESERVATION .....</b>		<b>21-1</b>
§ 21.01	Identification .....	21-3
§ 21.02	Litigation Hold .....	21-3
	[A] Determination to Trigger Litigation Hold .....	21-3
	[B] Implementation and Compliance of the Hold.....	21-3
	[C] Technology Issues .....	21-4
§ 21.03	Preservation Notices and Letters.....	21-4
	[A] Preservation Notices .....	21-4
	[B] Preservation Letters .....	21-5

§ 21.04	Preservation .....	21-5
§ 21.05	Meet-and-Confer.....	21-6
§ 21.06	Discovery Strategy and Project Plan.....	21-7
§ 21.07	Issues and Concerns .....	21-7
§ 21.08	Recommendations.....	21-7

**Chapter 22**

<b>QUICK WALKTHROUGH OF THE e-Discovery PROCESS.....</b>	<b>22-1</b>
--	-------------

**Chapter 23**

<b>GENERAL ISSUES AND RECOMMENDATIONS .....</b>	<b>23-1</b>
---	-------------

§ 23.01	Management Commitment and Support .....	23-3
§ 23.02	Cultural Issues .....	23-3
§ 23.03	Education and Training .....	23-3
§ 23.04	Planning .....	23-4
§ 23.05	Methodologies .....	23-4
§ 23.06	Standardization .....	23-4
§ 23.07	e-Discovery Technology.....	23-4

**PART IV**

**e-Discovery READINESS PLANNING**

**Chapter 24**

<b>INTRODUCTION.....</b>	<b>24-1</b>
--------------------------	-------------

§ 24.01	Overview.....	24-3
§ 24.02	“State of Readiness of Corporate IT Infrastructure” .....	24-3

**Chapter 25**

<b>GUIDANCE AND GOVERNANCE .....</b>	<b>25-1</b>
--------------------------------------	-------------

§ 25.01	Introduction.....	25-3
§ 25.02	ILM Steering Committee.....	25-3
§ 25.03	ILM Program Office .....	25-4
§ 25.04	ILM Governance and Implementation Methodology .....	25-4
§ 25.05	Third-Party Involvement .....	25-5
§ 25.06	Issues and Concerns .....	25-5
§ 25.07	Recommendations.....	25-5

**Chapter 26**

<b>INFORMATION LIFECYCLE MANAGEMENT .....</b>	<b>26-1</b>
---	-------------

§ 26.01	Introduction.....	26-3
§ 26.02	Background.....	26-3
§ 26.03	Document Lifecycle Model.....	26-4
§ 26.04	Components of ILM .....	26-4
	[A] Information Asset Management .....	26-5
	[B] Content Management.....	26-6
	[C] Compliance Management .....	26-6
	[D] e-Discovery Platform.....	26-7
§ 26.05	Migration to ILM.....	26-7
	[A] Ground Rules .....	26-8
	[B] Moving Through the Process .....	26-8
	[C] Focusing on e-Discovery Readiness .....	26-9

## CONTENTS

---

### Chapter 27

#### **ESTABLISHING THE e-Discovery METHODOLOGY ..... 27-1**

§ 27.01	Methodology Components .....	27-3
§ 27.02	Project Plans .....	27-4

### Chapter 28

#### **IMPLEMENTING AN e-Discovery READINESS PROGRAM ..... 28-1**

§ 28.01	Introduction.....	28-3
§ 28.02	e-Discovery Readiness Program .....	28-3
	[A] Situational Assessment and GIR Analysis.....	28-3
	[B] Strategies and Priorities.....	28-3
	[C] Project Plans and Implementation.....	28-4

### Chapter 29

#### **e-Discovery TECHNOLOGY AND TOOLS ..... 29-1**

§ 29.01	The e-Discovery Marketplace .....	29-3
	[A] Regional/Local Service Bureaus .....	29-3
	[B] Point Solution Vendors.....	29-4
	[C] Integrated Platform Vendors .....	29-4
	[D] Enterprise Solution Vendors .....	29-4
	[E] Consulting Firms .....	29-4
	[F] Law Firms.....	29-4
	[G] End User Entities.....	29-5
§ 29.02	Market Consolidation and Implications .....	29-5
§ 29.03	Solution Categories.....	29-6
	[A] Case Management Suites.....	29-6
	[B] Collection and Preservation.....	29-6
	[C] Search.....	29-6
	[D] Integrated (Processing, Review and Analysis, and Production).....	29-7

### Chapter 30

#### **CHOOSING VENDORS..... 30-1**

§ 30.01	Needs Analysis .....	30-3
§ 30.02	Request for Proposal (RFP).....	30-3
§ 30.03	Due Diligence .....	30-4

## PART V

### APPENDICES

<b>BIBLIOGRAPHY .....</b>	<b>BIB-1</b>
---------------------------	--------------

<b>GLOSSARY .....</b>	<b>G-1</b>
-----------------------	------------

<b>INDEX .....</b>	<b>I-1</b>
--------------------	------------



# ABOUT THE AUTHORS

---

## **Adam I. Cohen**

Adam I. Cohen is a senior managing director in the New York office of FTI's Technology Consulting practice. Mr. Cohen is a nationally recognized expert in electronic discovery and electronic information management policy issues. Mr. Cohen advises on planning and implementation issues associated with every phase of electronic discovery in litigations and investigations as well as electronic information management policies and practices, including, for example, proactive litigation readiness and regulatory compliance, complying with electronic preservation obligations and avoiding spoliation sanctions, crafting and responding to discovery requests targeting electronic information, and cost containment strategies.

Prior to joining FTI, Mr. Cohen was a litigation partner at Weil, Gotshal & Manges, LLP, where he represented major corporate clients in complex litigation involving computer and Internet-related issues. He is co-author (with Weil partner David J. Lender) of the treatise *Electronic Discovery: Law and Practice* (Aspen Publishers), which already has been cited as authority in several landmark electronic discovery opinions by federal courts.

Mr. Cohen is co-chair of the Electronic Discovery committee of the New York State Bar Association's Federal and Commercial Litigation Section, a member of the Advisory Board of the Georgetown Law Center E-Discovery Institute, and a member of the board of Volunteer Lawyers for the Arts. He is admitted to practice in the courts of the State of New York, as well as the United States District Courts for the Southern and Eastern Districts of New York. He holds a B.A. from Wesleyan University and a J.D. from Duke University School of Law.

## **G. Edward Kalbaugh**

G. Edward Kalbaugh is senior managing director of Allegent Consulting Group, a consultancy that advises companies on strategies and application of information technology to achieve business objectives, including governance, risk management, and compliance programs.

Mr. Kalbaugh has led and participated in numerous major national and international engagements involving assessments, strategies, policies and implementation procedures dealing with regulatory compliance, corporate governance, information systems migrations, and enterprise risk management.

Prior to Allegent, Mr. Kalbaugh held senior management positions in banking, where his responsibilities included operations and information systems and membership on the regulatory and risk management steering committees. Mr. Kalbaugh began his career with the Space Division of Rockwell International, where he completed the company's six-year management development program and was director of engineering extended space operations.

Trained as an industrial engineer, Mr. Kalbaugh has been a frequent writer and speaker on business transformation through leverage of information systems. He has formed and sold three technology companies.

**PART I**

# **INTRODUCTION AND OVERVIEW**

---



## CHAPTER 1

# INTRODUCTION

---

Discovery of electronically stored information (ESI), even under optimum circumstances, is a complex, dynamic, and difficult process. It is also a collaborative process requiring a mix of legal, business, and technical knowledge and skills combined with an increasing reliance on technology to facilitate the process.

These imperatives are being positively addressed by the courts through evolving interpretations of the Federal Rules of Civil Procedure and the December 2006 Amended Rules, resulting in several major themes that are important for litigation and discovery practitioners to understand.

Foremost is the requirement for counsel to demonstrate best efforts to achieve a cooperative and efficient approach for accomplishing cost-effective ESI discovery. Inherent in this requirement is the desire of the courts to be unburdened from involvement in resolving capricious discovery issues resulting from lack of diligence and good-faith effort on the part of counsel.

These requirements point to the unquestionable need for counsel to understand ESI sources and information technology, including the software tools that facilitate discovery and litigation. It is also important for counsel to understand how the ESI discovery process works within the framework of corporate governance and technology issues.

These imperatives are made more urgent as the absolute volume of information continues to increase and litigators are obliged to forego “game theory” approaches in favor of strategic cooperation in order to effectively contain discovery costs and protect the client’s position. Seeking all relevant information will give way to seeking the best relevant information.

This will require use of sophisticated discovery tools—concept and contextual searching, artificial intelligence, statistical sampling, and relationship mapping—that help automate the discovery process, reduce costs, and enhance process and information integrity.

As noted, these efforts take place within the framework of law. In that regard, there is considerable detailed material available covering the Federal Rules of Civil Procedure and the December 2006 Amended Rules, including compendia of related case law. Accordingly, this book does not attempt to repeat that body of information.

Instead, this book is designed to provide discovery and litigation practitioners with an easy-to-read introduction and reference source for understanding ESI sources and underlying information technology, the functional components of the discovery process, and the discovery technology that supports that process. The book is organized into five Parts:

- Introduction to the ESI discovery lifecycle and the information technology systems likely to be encountered
- Explanations and discussions of the major sources of ESI
- “Walkthrough” of the e-discovery lifecycle processes
- Information on how to be better prepared for e-discovery in the future
- Additional reference information

Each chapter provides information to educate the reader concerning the various topics covered, and concludes with a summary of issues and concerns that may need attention, as well as recommendations that may be helpful to practitioners in addressing those issues.

In using this book it is important to keep in mind the constant and rapid pace of change that takes place within information systems organizations and in the systems and software tools used by those organizations.

This dynamic aspect of information systems makes it extremely difficult even for specialists in the field to keep current with emerging technology, especially its impact on systems already in place within the organization (legacy systems).

To gain a thorough understanding of any particular information technology would require intensive study of large volumes of information on the subject. Such an effort is impractical and beyond the ordinary scope of most practitioners in the legal profession. However, counsel must understand information technology well enough to meet the intent of the Amended Federal Rules and to adequately represent the best interests of their client.

This book addresses this challenge by focusing on the fundamental characteristics and intent of the applicable technology, not on the arcane details of any particular technology. By taking this approach, the reader is equipped with sufficient information to know what questions to ask, what person in the organization might have the answers, and whether the answers are sufficient to satisfy the particular issue or requirement.

To achieve these objectives, the book is organized to enable easy reading and quick reference to topics, while minimizing dependence on footnotes, endnotes, and other cumbersome annotations.

The Appendix contains sample material that helps make the content of the book more meaningful by illustrating how selected components of the e-Discovery process have, or might be implemented in actual practice.

Finally, the authors recognize that most organizations face budgetary and other resource constraints that impose limitations on their practical ability to implement some of the recommendations set forth in this book. This does not mean that the recommendations should not be considered where resource constraints exist. On the contrary, in all situations, the recommendations should be viewed as incremental objectives that can move the organization forward in terms of achieving effective e-Discovery capabilities. Accordingly, each organization should consider the recommendations, set priorities, and establish plans for selective implementation that optimize that organization's respective capabilities.

## APPENDIX 7

# SELECTED TOPICS FOR DEPOSITIONS OF CORPORATE REPRESENTATIVES REGARDING FACTS IMPACTING ESI AVAILABILITY TO EXAMINING PARTY

---

### TABLE OF CONTENTS

#### INTRODUCTION

- Documentation Re: Sources of ESI
- Electronic Mail – General
  - Public Folders
  - Remote Access
  - Servers
  - Backups
  - E-mail Archiving Systems
  - Hardware
  - Document Management Systems
  - Legacy Systems
  - Databases and Enterprise Systems
  - Voicemail Systems
  - Instant Messaging
  - Third-Party Custodians
  - Intranet and Internet
- General Document Retention Policies and Procedures
- IT Usage Policies
  - Former Employees
  - Litigation Hold Procedures
  - Collection Policies and Procedures
- The Instant Litigation—Chronology of eDiscovery Steps
  - Preservation
  - Collection
  - Post-Collection
- Evidentiary Questions



## INTRODUCTION

- Given the central role of ESI in litigation, the discovery process frequently includes examination into the systems, policies, procedures and practices that influence what ESI is preserved and produced. Authority for depositions on these kinds of facts is often found, for example, in Rule 30(b)(6) of the Federal Rules of Civil Procedure, which permits depositions of corporate representatives on topics identified by the requesting party. We will not attempt to explore the legal parameters of such depositions here, but rather lay out, at a high level, some suggestions as to topics that might be covered by the attorney charged with conducting such an examination before trial.
- As a generic outline, the topics presented here are more general than would be the case in a real deposition, one that would deal with specific facts and most likely some documentation provided in advance of the deposition. Of course, the art of examining a witness is largely in the follow-up—listening to the answer and probing it. Potential witnesses on the ESI topics appearing below should think carefully about the additional questions their answers are likely to raise and how they should answer them.
- By no means are the topics presented below intended to be comprehensive. There are many more topics that could be explored and questions asked depending on the particular situation in which the deposition occurs. Likewise, there are many different ways to ask these questions. Rather, these topics and questions are intended to assist the attorney planning for the deposition by providing some directional guidance, and to assist those preparing for these types of depositions with some insight into what might be covered.
- Note that not included here are the generic topics that are not specific to an examination on ESI sources and discovery issues, such as questions relating to witness background and preparation.

### Documentation Re: Sources of ESI

- Most organizations will have some form of documentation regarding their information systems and related policies and procedures. If discovery of these types of documents has not occurred through written discovery requests or other disclosure mechanisms, the examining attorney may wish to probe what is available and request production. Ideally, such documents would be produced in advance of the deposition and would be available for use as exhibits, but in practice this does not always happen.
- Documentation, especially documents that were not prepared for litigation purposes, can provide insight and understanding into a party's sources of ESI. There are too many possible types of documentation to identify here, but examples could include graphical representations, such as network diagrams or "data maps", lists or inventories of applications, servers and databases, applications inventories, and reports from asset-tracking systems showing what equipment was issued when and to whom.
- The examiner should also find out what personnel are responsible for creating and maintaining any of the documentation, as well as the process for doing so.
- An IT organization chart is a very useful document to have. Without having the kind of information represented in such a chart, the examiner should ask the witness to identify which IT personnel are responsible for each source or system.

### Electronic Mail – General

- Does everyone at the company have a corporate e-mail account or only certain categories of employees?
- If the latter, which categories or personnel?
- What e-mail system does the company use (for example, Microsoft Exchange, Lotus Notes, Other)?
  - What version?
  - When was it installed?

- [Address legacy systems if relevant.]
- What functionality is available to users? Specifically:
  - can they use offline mode (in Exchange) or equivalent?
  - can they store .psts (in Exchange) or otherwise archive locally or elsewhere?
  - can they use automatic forwarding to third-party accounts, e.g., Yahoo!Mail or “gmail”?
  - are they restricted by any policy or technical means from use of the company e-mail system for non-business communications?
  - are they restricted by any policy or technical means from use of non-company e-mail accounts for business communications?
  - [Note that if the answer is “yes” the means of restriction should be probed and, if appropriate, the steps taken to monitor and enforce compliance with any applicable policies]
- Does the company apply a mailbox size limit?
  - What is it?
  - What happens when a user reaches the limit (e.g., are they able to continue to receive or send mail)?
- Does the company deploy spam or antivirus protection?
  - If so, what tools are deployed and how are they configured?
  - What happens to quarantined e-mails? Where are they stored?
- [Note that several other sections below return to e-mail topics in connection with, for example, servers, backups, mobile devices, etc.]

#### Public Folders

- Does the company use public folders? [Public folders are locations on servers set up to facilitate collaborative sharing of information among users granted access to the folder.]
- If the answer is yes, the examiner should probe how the folder is used and access controlled, as well as retention practices, e.g.:
  - Is there a policy governing how public folders are to be used?
  - Can users move e-mail messages to which they want other users to have access to a public folder?
  - Are the folders accessible by multiple employees?
  - What is the process for creating a new public folder?
  - How are permissions and access controlled?
  - What retention rules or practices apply to public folders, if any?
  - [Note applicability of other sections below, e.g., servers and backups.]

#### Remote Access

- Many companies provide means of remote access so that users can work efficiently from outside the office. The nature and use of the access provided can impact the existence and location of ESI, among other things. Accordingly, the examiner should determine how any remote access is handled.
- For example, the examiner should determine whether users can access the company servers via Outlook Web Access (OWA) or some equivalent via a Web browser or by using a Virtual Private Network (VPN).

### Servers

- Servers are one of the fundamental sources of most ESI collections. There may be multiple different types of servers playing various roles, but typically e-mail servers and file servers are a primary focus of electronic discovery.
- Does the company routinely purge or “auto-delete” any information from servers? (Note that this is a fairly common practice for e-mail servers.)
  - If so, what is purged? [Note that very often routine purging is limited to certain folders, such as Inbox, Sent, and Deleted Items; very often e-mails the user moves to personal folders are outside the scope of the purge.]
  - How is the purge implemented technically and procedurally?
  - On what schedule does the purge occur?
  - Are there any exceptions to the regular purge?
  - How is the purge administered by IT personnel?
- What types of files are stored on the company’s file servers? [Note that file servers normally contain “business documents” such as word processing documents, slide presentations, and spreadsheets.]
- Is access restricted or controlled in any way?
- Are there file shares or group shares?
  - How are these organized?
  - Who has access?
- What is the retention schedule for files on file servers?
- How is file server content organized?
- How is it accessed by users?
- [Note backup section below.]

### Backups

- What systems and sources are backed up?
  - Servers?
  - Laptops?
  - Other?
- How are the backups made, i.e., what is or are the backup system(s) in use and how are they configured (hardware and software)?
- What is the schedule for backups?
- Are they full or incremental?
- Are tapes used?
- What type of tapes?
  - Are the tapes recycled?
  - Where and how are they stored?

- How are the tapes labeled, inventoried, and/or organized?
- What information is available about the content of the tapes from reasonably accessible records?
- What is required in terms of tools, resources, and cost to search the tape content?

#### E-mail Archiving Systems

- Does the company use an e-mail archiving system?
  - If so, what system?
  - How is the system configured?
  - What data does it save?
  - What data does it discard?
  - Where does it save data?
  - Who administers the system?
  - How is data extracted from the archive?
  - How long has the archive been in use?
  - Were any e-mails predating the installation of the archive system migrated to the archive?

#### Hardware

- What hardware is issued to users of interest?
  - Desktops?
  - Laptops?
  - Storage devices or media? [Note that some companies prohibit the use of “thumb” drives or other storage devices by policy; if that is the case here, the examiner should probe the monitoring and enforcement of compliance with such policies.]
  - Mobile devices?
    - What are the criteria for issuing mobile devices?
    - Are they completely synchronized with servers?
    - Is SMS or PIN-to-PIN messaging enabled/permitted? [Note that data from such communications may reside on the device itself but not on the servers.]
- Is there an asset-tracking system that reflects this information?

#### Document Management Systems

- Does the company use a document management system to store, manage, and/or search documents on file servers or elsewhere?
  - If so, what system and how is it configured?
  - Where is the data stored?
  - How can relevant ESI be identified and be extracted from the system?
  - What retention rules are applied to the system?

### Legacy Systems

- The examiner should explore what systems were in use prior to the current systems and consider whether the timing may indicate the existence of ESI in legacy systems based on the time period relevant to the lawsuit.
- If any such legacy systems are identified, the examiner should follow the trail of the potentially relevant ESI in such systems—determining whether it is still being stored and if so in what manner.

### Databases and Enterprise Systems

- Organizations of any significant size will have multiple systems using databases to store a variety of ESI. Examples would include customer relationship management systems, financial and accounting systems, human resources systems, engineering systems, etc. The list is endless depending on the particular industry and business in question. At very large companies this list might include hundreds or even thousands of different systems.
- This “structured” data is often overlooked in the excitement to find the smoking gun in the haystack of e-mails. But for many types of cases, such as those involving allegations of accounting fraud, or allegations of patterned employment discrimination to name a few examples, such database systems are critical. They also create unique challenges for electronic discovery on a variety of levels.
- The examining attorney needs to first determine what the corporate landscape looks like for these types of systems. Depending on the number of systems involved, the examiner may need to approach this landscape by exploring categories of systems as opposed to individual systems or instances of systems. Then the examiner can narrow the examination to focus more detailed questions on the systems containing ESI that is potentially relevant to the case.
- The examiner should find out, for example:
  - What types of ESI are stored in the system?
  - How does information enter the system?
  - How does the system process that information?
  - Where does the system store the ESI?
  - In what format is the ESI stored?
  - What database technology may underlie the system (for example, Oracle or SQL)?
  - What reports can the system generate?
  - How is the system backed up?
  - Is the system audited? When? How? What documentation reflects the audits?
  - Who has access to the system and what rights do they have to manipulate or view ESI in the system?

### Voicemail Systems

- Does the company provide the use of a voicemail system?
- If so, what type?
- Which categories of employees have voicemail?
- In what format does the system store voicemails?
- [Note that in many of today’s “unified messaging” systems, the voicemail system is connected with the e-mail system, and voicemails are stored as .wav files which can be transmitted via e-mail; in other cases the system

sends notification to a user that a voicemail has arrived but accessing the voicemail requires using the telephony system.]

- What are the retention rules applied to voicemails?
- Is the voicemail system backed up? [See backup section.]

#### Instant Messaging

- Does the company provide employees use of an instant messaging (“IM”) system?
  - If so, identify and describe the system, who has access, what parameters are in place and functionality enabled, etc.
- Does the IM system allow communications with users external to the company (who are using other IM systems)?
- What data does the IM system generate and what does it retain (e.g., logs, full content of chats, etc.)?
  - Can it be configured to retain additional data?
  - If so, what is involved in doing so?
- Does the company permit employees to use third-party IM applications via the corporate network (for example, Yahoo!Messenger)?
- If such use is restricted, is this done by policy or technical restriction?
  - If by policy, how is compliance with the policy monitored and enforced?
  - If technically, how is the restriction achieved?

#### Third-Party Custodians

- Many companies outsource elements of their IT operations or records management. The result is that relevant ESI may be in the possession of those third parties, thus requiring additional steps to ensure proper preservation and collection. One common example is storage of backup tapes for disaster recovery purposes, but many companies outsource practically their entire IT function. Parties are not free to ignore relevant ESI simply because it is in the hands of a vendor, but it can be easily overlooked until it is too late.
  - Does the company outsource any of its IT or records management functions?
  - If so, what functions?
  - What ESI is retained by the vendor?
  - What retention policies are applied to that ESI?

#### Intranet and Internet

- It is almost hard to imagine a business of any significance without some presence on the Internet. The forms this presence can take are many, including for example, websites, blogs, chat rooms, and bulletin boards. In many cases information from these sources is relevant. Accordingly, in these cases it is critical that the examiner understand the details of the company’s Web presence, including the content as well as the retention policies applied to the resultant ESI.
- Many companies also maintain an Intranet for the use of corporate employees. More often than should be the case, the corporate Intranet is not subject to strong central control and business units are free to set up their

own areas on the Intranet with content that is not reviewed for compliance in advance of or even after posting. The examiner should understand the rules of the road—or lack thereof—for the corporate Intranet, including without limitation the process for the posting of content, the degree of access permitted to various users, and the retention policies applied to Intranet ESI.

#### General Document Retention Policies and Procedures

- Does the company have a document retention policy?
- If so, is it written?
- When was the policy established? [Note that if relevant given the time period of the matter, the examiner will have to track the evolution of the current policy by discovering the prior policy and what changes the retention policies underwent over the time period in question.]
- Is there a retention schedule that accompanies the policy?
- How does the company try to ensure compliance with the policy?
  - Does the company monitor for compliance? How? Is this monitoring documented?
  - What does the company do when it finds non-compliance?
  - Has this ever happened? With what result? Are there records of this or these incidents?
  - Are employees trained on the policy and how to comply?
- What steps does the company take to ensure the confidentiality and security of its data?
- What group or groups and which individuals are responsible for formulating and implementing the document retention policies?

#### IT Usage Policies

- Does the company have a set of policies governing employee use of the company's IT asset? What are they? Are these written?
- Do these policies address permitted storage devices and locations?
- Do they address whether home computers or other non-company-issued devices may be used for business purposes?
  - How does the company monitor and enforce compliance with these policies?
  - Who is responsible for formulating and implementing the policies?

#### Former Employees

- What are the company's policies and procedures with respect to IT assets and ESI held or stored by users who have left the company?
- What happens to their computers when they leave?
- What happens to other devices that may store ESI?
- What happens to ESI they have stored on servers?
- What happens to their access rights and permissions?

Litigation Hold Procedures

- Does the company have policies and procedures governing compliance with legal preservation duties, i.e., “litigation holds”?
- What are they? [Note: the examiner should make sure that all sources are addressed by the procedures. It may be necessary to confirm this for each item on the list. For example, the examiner should find out what procedures have been established for handling e-mail, “business documents” on file servers, computer assets of departed employees, backup tapes, etc.]
- Are these policies written?
- Who decides whether and when a hold should be implemented?
- Are these determinations documented along with the rationale?
- Who determines the scope and parameters of any litigation hold?
- Are these determinations documented along with the rationale?
- How is specific ESI that may be subject to a hold identified?
- Are electronic search methods and technology used?
- If so, what are they?
- What testing is done to ensure correct identification?
- Does the company send hold notices to employees or third parties with ESI that is potentially relevant to reasonably anticipated or pending legal action?
  - Are these based on a standard form that the company uses?
  - How does the company transmit the notices?
  - Does the company transmit notices to each individual custodian with potentially relevant ESI?
  - Are recipients required to acknowledge receipt of and compliance with hold notices? Are there records of such acknowledgements?
- Are employees trained on how to implement litigation holds over ESI?
- Does the company use any specific hardware or software tools to implement litigation holds?
- Does the company monitor and enforce compliance with litigation holds?
  - How?
  - What records does the company keep of such activity?
- Does the company follow up on hold notices issued to individual custodians? How?
- Who was/is involved in formulating and implementing litigation hold policies and procedures, and what are/were their respective roles regarding the same?

Collection Policies and Procedures

- Does the company have policies and procedures governing the collection of ESI?
- What are they? [Note: as above, the examiner should make sure that all sources are addressed by the procedures. It may be necessary to confirm this for each item on the list.]
- Are these policies and procedures written?
- How does the company monitor for and enforce compliance?

- Who formulated these policies and procedures?
- Who carries out collections?
  - What training and/or certification do they have?
- How do they decide what to collect?
- What hardware and software tools do they use and how?
- What testing is done to verify proper collection?
- What elements of the collection process are documented and how?
- How is the chain of custody managed?
- How does the collection process attempt to ensure the integrity of ESI as evidence?
- What safeguards are in place to prevent alteration of metadata?

### The Instant Litigation—Chronology of eDiscovery Steps

#### Preservation

- At this point the examiner may wish to explore what the company did in the case at hand to comply with its various preservation and discovery obligations, in light of the information about sources, systems, personnel, policies, and procedures acquired through the above-outlined avenues of questioning.
- This would include detailed questioning about any actions taken to comply with the duty to preserve ESI relevant to the case, including without limitation who was involved in such actions, when they took such actions, how they identified ESI for preservation, and what documentation exists concerning such actions. For example:
  - When did the company decide that it had an ESI preservation duty in this case?
  - Who was involved in making that decision?
  - Was the decision and the rationale for it documented?
  - When did the company decide on the scope of the duty?
  - What did it decide to preserve?
    - Which custodians?
    - For what time periods?
    - Were keywords used?
    - What sources of ESI were targeted?
  - Who was involved in making that decision?
  - Was the decision and the rationale for it documented?
  - Was a hold notice sent to custodians?
    - To whom?
    - How?
    - What did it say?
    - Were they asked to confirm receipt, understanding, and compliance?
    - Did any of them ask questions about the notice?

- What was done to follow up and ensure compliance?
- Was all of the above documented?
- The examiner should ask about what specifically was done to preserve each source of ESI, including:
  - What steps were taken;
  - Who performed the preservation steps;
  - When they did so;
  - What hardware/software tools were used; and
  - What documentation of the efforts exists.
- Were custodians interviewed to determine what sources of ESI might exist?
  - What were they asked?
  - Who conducted the interviews?
  - When?
  - Is there documentation of these interviews?
- Were electronic searches conducted to identify ESI for preservation?
  - What sources were searched electronically?
  - What types of files did the search target?
  - How was the search executed?
    - Was the protocol documented?
    - Who performed the searches?
    - Were keywords used? If so, what were they?
    - What technology was used to execute the searches?
    - What steps were taken to verify that the search captured results accurately?
    - [Additional probing of the limitations of any search technology might be performed, including how the search addressed problematic files, such as password-protected files.]
    - What records of the searches were kept?

#### Collection

- Was the ESI collected the same ESI as what was preserved?
- If not, why not and what was the discrepancy?
- How was the collection performed? [Note that this may need to be asked for each source of ESI.]
- Was the process documented? How?
- Who performed the collections and what are their qualifications to do so?
- What hardware/software tools did they use?
- Was metadata preserved intact through the collection methods used?
- What documentation was kept regarding the chain of custody?
- Were there sources from which ESI was not collected?

- Which sources?
- Why?
- Were there types of files that were not collected?
- Were any efforts made to recover deleted ESI?

#### Post-Collection

- The examiner should track chronologically the progress of the ESI from the point of collection to production. For example:
  - What was done with the ESI after it was collected?
  - If further “culling” and/or “processing” was performed on the ESI, what was done, what technology was used, and who performed the culling and/or processing?
- Was there a process for handling processing “exceptions” and if so, what was it? If not, what happened to the exception files?
- How was the review for production carried out?
  - Who conducted the review?
    - Were the reviewers attorneys?
    - Was any of the review outsourced to contract attorneys?
    - If so, were any of these attorneys outside the U.S.?
  - What review procedures were followed?
  - What technology was used to conduct the review?
    - How does it work?
    - What checks were done, and what documentation exists to verify completeness and accuracy?
  - Was sampling used as any part of the review process?
- What checks were done, and what documentation exists to ensure that all documents designated for production were copied to the production media?

#### Evidentiary Questions

- The examiner may wish to lay the groundwork for future analysis of evidentiary admissibility issues. For example, questions may be asked to ascertain whether or not it is appropriate to consider certain documents business records under a hearsay exception. The examiner should research the criteria for admissibility under the applicable law and ask questions designed to assist an analysis of whether those criteria have been met.
- The chain of custody questions outlined above would be examples. Another example would be to ask whether the document in question is a record that employees are required to keep as part of their job responsibilities, which is a potentially important factor under the aforementioned business records analysis.