

TABLE OF CONTENTS

CHAPTER 1

Introduction

§ 1.01	Background	1-1
	[1] The Emergence of Modern Discovery Practices	1-1
	[2] Recognition of the Universe of Electronic Records	1-2
	[3] Navigating the Shoals of Electronic Discovery Only by “Dead-Reckoning”	1-4
	[4] The False Concept of “Deleted” Electronic Records	1-8
	[5] Lack of Understanding of Electronic Records Generally, and Bad Habits in the Use of Electronic Communications Methods	1-9
	[6] The Current Electronic Discovery Landscape	1-12
§ 1.02	Electronic Discovery Issues	1-13

CHAPTER 2

The Federal Discovery Rules and Electronic Evidence

§ 2.01	Application of the Federal Rules of Civil Procedure to Electronic Evidence	2-1
	[1] Scope of Discovery	2-7
	[2] Privilege Concerns	2-17
	[3] Third Party Discovery	2-19
§ 2.02	Rule 34 and the Form of Production	2-21

§ 2.03	The Cost of Searching for and Retrieving Electronic Evidence	2-28
	[1] Balancing Test Approach	2-32.3
	[2] The <i>Zubulake</i> Standard	2-33

CHAPTER 3

Planning and Executing Electronic Discovery

§ 3.01	Offensive Discovery	3-3
	[1] The Discovery Plan	3-4
	[a] Identifying Goals and Issues	3-4
	[b] Using Electronic Evidence to Achieve the Client's Goals	3-5
	[2] Electronic Discovery Requests	3-7
	[3] Obtaining Document Preservation Orders from the Court	3-10
	[4] Preparing Document Requests	3-12
	[5] Preparing Interrogatories	3-14
	[6] Taking Depositions	3-14
	[a] Record Custodians	3-14
	[b] Corporate Designees (Rule 30(b)(6))	3-14
	[c] Depositions on Written Questions	3-15
	[7] Compelling Discovery	3-16
§ 3.02	Defending Against and Responding to Electronic Discovery Requests	3-19
	[1] Work Product Databases	3-19
	[2] Failure to Comply with Discovery	3-19
	[3] Avoiding Data Spoliation and Destruction Problems	3-21
	[4] Preparing for Electronic Discovery <i>Before</i> Litigation Is Filed	3-22
	[5] Responding to Document Requests	3-23
	[a] Gauge the Reasonableness of Requests	3-24
	[b] Get a Real Estimate of the Cost and Personnel Burden	3-24
	[c] Remember the Standard Objections	3-25
	[6] The Document Search	3-26

[7] Defending Against Improper or Burdensome Discovery 3-31

CHAPTER 3A

Data Collection, Computer Forensics, and File Processing

§ 3A.01 Introduction 3A-2

§ 3A.02 Scope of the Data Collection Effort 3A-5

[1] Identify the Relevant Subject Matter and Issues 3A-6

[2] Identify the Relevant Custodians 3A-8

[3] Identify the Relevant Time Period 3A-9

[4] Identify the Relevant Data Sources 3A-9

§ 3A.03 Data Collection 3A-17

[1] Forensic Data Collection 3A-19

[a] Types of Data to Collect 3A-19

[b] Minimize Changes to Evidence 3A-21

[c] Methods and Process of Forensic Acquisition 3A-21

[d] Chain of Custody Issues 3A-24

[2] Non-Forensic Data Collection 3A-25

[3] Cost of Data Collection 3A-29

§ 3A.04 Data Analysis and Filtering 3A-30

[1] File Harvesting 3A-30

[2] File Content Analysis 3A-34

[3] Metadata Analysis 3A-48

[4] Deleted Data 3A-50

[5] Temporary Data 3A-51

[6] Web Browser Artifacts 3A-52

[7] Mobile Device Data 3A-53

[8] Anti-Forensics 3A-53

§ 3A.05 The Computer Forensic Expert 3A-56

[1] Education 3A-56

[2] Certification 3A-56

[3] Experience 3A-57

ELECTRONIC DISCOVERY

CHAPTER 4

**Preserving Electronic Documents
Before and After Litigation Ensues**

§ 4.01	Introduction	4-2
§ 4.02	Retention Policies	4-6
§ 4.03	Document Preservation and Demand Letters	4-11
§ 4.04	Document Preservation Orders	4-14.1
	[1] Injunctive Factors	4-16
	[a] Likelihood of Destruction	4-16
	[b] Irreparable Harm	4-16.1
	[c] Burden on the Parties	4-16.1
	[2] Seeking the Least Intrusive Language	4-16.2
§ 4.04A	The Duty to Preserve Backup Tapes	4-17
	[1] Introduction	4-17
	[2] The Nature of Backups and Backup Tapes	4-17
	[a] The Backup Tape	4-18
	[b] Backup Tape Rotation and Overwriting	4-19
	[c] “Point-in-Time” Snapshots	4-20
	[d] Other Forms of Backups	4-21
	[3] The Duty to Preserve Backup Tapes	4-22
	[a] Establishing the Duty to Preserve Tapes and Its Parameters	4-23
	[b] Preserving Existing Tapes vs. Tapes Made in the Future	4-28
	[c] Proportionality and Backup Tape Preservation	4-29
	[d] Consequences of Failing to Preserve Backup Tapes (Sanctions)	4-30
	[4] Practical Advice for Dealing with Backup Tapes	4-31
§ 4.05	Sanctions for Failing to Produce or Preserve Electronic Evidence	4-34
	[1] Sanctions for the Failure to Produce Electronic Evidence	4-38
	[2] Sanctions for Spoliation of Electronic Evidence	4-42
§ 4.06	<i>Form</i> : Sample Electronic Document Retention Policy	4-46.5

TABLE OF CONTENTS

xi

§ 4.07	<i>Form</i> : Sample E-Mail Use and Retention Policy	4-53
§ 4.08	<i>Form</i> : Sample Preservation of Evidence Letter	4-63
§ 4.09	<i>Form</i> : Sample Document Preservation Order	4-67

CHAPTER 5

Drafting Discovery Requests for Electronic Information

§ 5.01	Preparing Electronic Discovery Requests	5-2
	[1] Where to Begin	5-2
	[2] General Considerations	5-3
§ 5.02	Types of Electronic Records Typically Sought in Discovery	5-7
§ 5.03	Sample Document Request	5-14
	[1] Guiding Principles	5-14
	[2] The Definition Section	5-19
	[3] <i>Form</i> : Sample Requests for Production of Documents	5-22
§ 5.04	Interrogatories	5-26
	[1] In General	5-26
	[2] <i>Form</i> : Sample Interrogatories	5-27

CHAPTER 6

Deposing the Records Custodian or Information Technology Manager

§ 6.01	Purpose of Deposing the Electronic Records Custodian or Technology Staff	6-2
§ 6.02	Strategy in Deposing or Defending the Deposition of the Custodian/IT Person	6-5
	[1] Making Use of the Deposition	6-5
	[a] Drafting Document Requests	6-5
	[b] Motions to Compel Discovery	6-5
	[c] Impeaching Credibility	6-6
	[d] Establishing the Documents as Business Records	6-6
	[e] Information to Support Further Discovery	6-7

ELECTRONIC DISCOVERY

	[f] Document Search Efforts	6-7
[2]	Nature and Types of Likely Deponents.	6-7
	[a] The Records or Information Governance Manager	6-8
	[b] The Chief Information Officer.	6-8
	[c] The Information Technology Director or Manager, and the IT Staff	6-8
	[d] The Knowledge Management Officer	6-9
	[e] The Legal Hold Coordinator or Electronic Discovery Manager.	6-9
§ 6.03	The Nuts and Bolts of the Deposition	6-10
	[1] The Timing of the Deposition.	6-10
	[2] Starting the Deposition: The Notice of Deposition	6-10
	[3] The List of Deposition Topics	6-13
§ 6.04	<i>Form</i> : A Sample Outline for Taking the Deposition.	6-20

CHAPTER 7**Special Issues Regarding the Discovery
of Electronic Mail and Messaging**

§ 7.01	Why E-Mail Deserves Special Attention in Electronic Discovery	7-3
§ 7.02	Legal Issues Regarding Discovery of E-Mail.	7-6
	[1] Introduction to and General Law on Discovery of E-Mail Messages.	7-6
	[2] Recovering Deleted E-Mail.	7-7
	[3] A Sound Basis to Recover Deleted Files Is Required	7-8
	[4] Burdens and Costs Relating to Discovery of Deleted E-Mails	7-10
	[5] Oversight of the Process of Retrieving Deleted E-Mails.	7-12
	[6] Federal Statutes Applicable to E-Mail.	7-13
	[a] The Stored Communications Act.	7-13
	[b] The Wiretap Act.	7-16

TABLE OF CONTENTS

xiii

	[c] The Electronic Communications Privacy Act	7-16
§ 7.03	Expectation of Privacy in E-Mail Communications	7-19
	[1] Expectation of Privacy and Confidentiality in E-Mail	7-19
	[2] Court Views on Expectation of Privacy in E-Mail	7-20
	[3] No Expectation of Privacy for Social Media Communications	7-21
	[4] Employee E-Mail Is Sometimes Unprotected	7-23
§ 7.04	Inside the Black Box: How Electronic Mail Works	7-24
	[1] The E-Mail “Client”: The E-Mail Software That Is Used.	7-24
	[2] The E-Mail Server, the Internal Network and the Internet	7-25
§ 7.05	The Components of an Electronic Mail Message and Metadata	7-29
§ 7.06	Finding and Collecting Electronic Mail Messages	7-31
	[1] Where to Search for Stored E-Mail	7-31
	[a] Smartphones and Other Handheld Devices	7-31
	[b] Laptop and Desktop Computers	7-32
	[c] Servers	7-33
	[d] Backup and Other Online and Offline Storage	7-33
	[e] Document Management Systems	7-35
	[f] Web-Based E-Mail Systems	7-35
	[g] E-Mail Archiving Systems	7-36
	[h] Files and Filing Cabinets	7-36
	[2] Obtaining Only Paper Copies of E-Mail is Inadequate for Discovery	7-36
	[3] Obtaining an Immediate Order to Preserve E-Mail	7-39
	[4] Dealing with “Lost” or “Deleted” E-Mail	7-39
§ 7.07	Other Types of Messaging	7-43
§ 7.08	Proactive Planning for E-Mail Discovery	7-47

ELECTRONIC DISCOVERY

CHAPTER 8

The Federal Rules of Evidence
and Electronic Documents

§ 8.01	Introduction	8-2
§ 8.02	Rule 401: Definition of “Relevant Evidence”	8-4
§ 8.03	Rules 901 and 902: Authentication and Self-Authentication	8-5
	[1] Rule 902: Self-Authentication	8-7
	[a] Rule 902(4): Certified Copies of Public Records	8-5
	[b] Rule 902(5): Official Publications	8-6
	[c] Rule 902(7): Trade Inscriptions and the Like	8-6
	[d] Rules 902(11)-(12): Domestic and Foreign Business Records	8-7
	[e] Rules 902(13)-(14): Digital Evidence	8-8
	[2] Rule 901: Authentication and Identification	8-8
	[a] Rule 901(b)(4): Distinctive Characteristics and the Like	8-9
	[b] Rule 901(b)(8): Ancient Documents or Data Compilations	8-10
	[c] Rule 901(b)(9): Process or System	8-10
§ 8.04	Rule 801: The Problem of Hearsay	8-11
	[1] Rule 801(d)(2): Admission of a Party Opponent	8-11
	[2] Rule 803(1): Present Sense Impression	8-12
	[3] Rule 803(6): Business Records	8-13
	[a] The Proper Foundation for Electronic Business Records	8-14
	[b] Regularity Requirement	8-17
	[4] Rule 803(8): Public Records and Reports	8-17
	[5] Rule 803(17): Market Reports, Commercial Publications	8-18
	[6] Rule 807: Residual Exception	8-20

TABLE OF CONTENTS

xv

§ 8.05	Rule 1002: Requirement of Original	8-22
§ 8.06	Rule 1004: Original Not Required	8-25
§ 8.07	Rule 1006: Summaries	8-26
§ 8.08	Rule 502: Attorney-Client Privilege and Work Product; Limitations on Waiver	8-27

CHAPTER 9

The Use of Experts for Electronic Discovery

§ 9.01	Introduction	9-1
§ 9.02	When to Use an Expert	9-3
	[1] The Consulting Expert	9-4
	[2] The Testifying Expert	9-6
	[3] Must an Expert Be Retained?	9-8
	[4] Paying for the Expert/Consultant	9-9
§ 9.03	Independent and Court-Appointed Experts (the Special Master)	9-12
§ 9.04	Guiding the Expert's Work	9-18
TABLE OF CASES		TC-1
INDEX		I-1

