

Detailed Contents

ABOUT THE AUTHOR	xv
ACKNOWLEDGMENTS	xvii
CHAPTER 1: Introduction	1
A. Approach	2
B. Structure	2
C. Tempest in a Teapot—What Is Not Covered	3
CHAPTER 2: Basic Investigation	5
A. Follow the Money	6
B. The Most Essential Tool	7
C. Cyberspace Is Smaller than You Think	8
1. The Internet and the World Wide Web Are <i>Not</i> the Same	8
2. A Mere Five Entities Maintain a Directory of the Entire Internet	12
3. Domain Names Are Assigned by a Retailer	15
4. Information Flows in an Orderly Manner	16
D. How to Find a Cybersquatter or Site Owner	17
1. The WHOIS Query and Reverse WHOIS	17
2. Other Clues	19
E. How to Interpret E-mail Headers	20
F. Unmasking the Anonymous E-mailer	21
G. Understanding Affiliate Networks and SPAM Marketing	25
H. An Example of a Simple Investigation Protocol	27
CHAPTER 3: Jurisdictional Quagmire	29
A. What's at Stake: Personal Jurisdiction and the Regulation of the Internet	31
B. Where Have We Been?	34
C. Life Is Complicated	35
D. First Principles	36
1. The Early Cases	36
2. <i>International Shoe</i> and the Rise of Long-Arm Statutes	36
3. Emerging Principles	38
a. General Jurisdiction	39

b. Specific Jurisdiction	39
c. In Rem Jurisdiction	40
E. Enter the Internet	41
F. Consider Functionality	44
G. Internet Activities Plus Business Contacts Equal General Jurisdiction	46
H. Specific Jurisdiction—Defamation	48
I. Recent Case Law: Specific Jurisdiction—Intellectual Property, Contracts, and Commercial Torts	51
1. Trademark Disputes	51
2. Copyright and Patent Disputes	51
3. Other Commercial Cases	53
4. Jurisdiction over Non-U.S. Websites “Importing” Digital Images of Counterfeit Products	55
J. Recent Case Law: Cybersquatting	56
K. Recent Case Law: The Role of Servers and ISPs	58
L. Resolution of the Scenarios	58
M. Long-Arm to Global Reach—International Considerations	60
1. The Complexity of International Jurisdictions	60
2. The European Perspective—First Principles	61
3. The E-Commerce Directive (2001/31)	62
4. The General Rule	62
a. Place of Establishment	62
b. The Coordinated Field	63
5. E-Commerce or Commerce?	64
6. Exceptions to the E-Commerce Directive	64
a. Jurisdiction Regulation	65
b. Rome I Regulation and the Rome Convention	65
7. National Courts versus Country-of-Origin Principle	66
8. Conclusion Regarding E-Commerce Directive	67
9. International Defamation	67
N. Scams and Torts—Unique Jurisdiction Considerations	70
CHAPTER 4: Intellectual Property	75
A. Trademarks and Domain Name Disputes	77
1. Scenarios	77
2. How to Investigate	77
a. The WHOIS Query	78
b. Dun & Bradstreet Reports	81
c. Review and Document How the Domain Is Used	82
d. Collect Ancillary Evidence	82
(i) Prior Use of Domain Name	82
(ii) Document a Registrant’s Previous Instances of Cybersquatting	84
(iii) Document a Registrant’s Ownership of Other Domain Names Incorporating Trademarks	84

e. Hire a Professional Investigator	84
3. The Law	85
a. What Is Cybersquatting?	85
(i) UDRP	86
(ii) ACPA	89
b. Other Types of Claims	91
(i) Traditional Trademark Infringement Claims	91
(ii) State Anticybersquatting Laws	92
c. Effectively Using Cease-and-Desist Letters	92
d. Drafting the UDRP Complaint	95
(i) Quick Recap of ACPA and UDRP Factors	95
(ii) Trademark Rights	96
(iii) Identical or Confusingly Similar	98
(iv) Rights or Legitimate Interests	101
(v) Making Legitimate Noncommercial or Fair Use of Domain Name	105
e. Drafting a Federal Claim	111
(i) Trademark Rights	111
(ii) Registers, Traffics, or Uses	112
(iii) Identical or Confusingly Similar	112
(iv) Bad-Faith Intent to Profit	114
f. UDRP Complaints: To Settle or Not to Settle	118
4. Strategies for Resolving the Scenarios	119
B. Trademark Use in Metatags and Keyword Advertising	123
1. More about the Technical Use of Metatags	124
2. How to Check a Web Page's Metatags	125
3. What Are Keywords and Sponsored or Keyed Ads?	126
4. How to Check for Sponsored Ads	128
5. The Law	128
a. Is This "Use in Commerce"?	129
b. Is Buying or Selling Keywords a "Use in Commerce"?	134
c. Likelihood of Confusion and Initial Interest Confusion	136
d. Fair Use	143
6. Factors That May Affect the Outcome of an Infringement Claim	146
a. Metatags	147
b. Keywords	149
C. Theft of Content—Copyright and Confidential Information	150
1. Scenarios	151
2. How to Investigate	152
3. The Law	155
a. Basic Copyright	155
b. Fair Use of Copyrighted Material	158
c. Copyright, Facts, and "Hot News"	160
d. There Are No Trade Secrets on the Internet	162

D. Counterfeiting	165
1. Scenario	165
2. How to Investigate	166
a. A Model of a Counterfeiting Network—Pharmaceuticals	167
b. Consider Registration and Hosting	169
c. More Tools and Tips	170
CHAPTER 5: Freedom of Expression and the Problem of Anonymity	173
A. Internet Service Provider Liability	174
1. Scenarios	175
2. How to Investigate	176
3. The Law	178
a. History of ISP Liability	178
b. Communication Decency Act, Section 230	180
(i) Broad Immunity for ISPs	180
(ii) Exceptions to Broad ISP Immunity	182
4. Internet Service Providers and Intellectual Property	185
a. Pre-Digital Millennium Copyright Act Liability	185
b. The Digital Millennium Copyright Act	188
c. ISP Liability under the DMCA: Cases	191
5. Internet Service Providers and the Fourth Amendment	195
6. Conclusion	196
B. Defamation	197
1. Scenario	197
2. How to Investigate	198
3. The Law	199
a. Publication versus Distribution	199
b. Expedited Discovery	204
c. Strategy	206
d. Obtaining a Subpoena	209
e. False Light	210
C. Spam	218
1. Scenario	218
2. How to Investigate	219
3. The Law	221
a. Defining Spam	221
b. Private Combat	222
c. Legal Combat	224
(i) State Legislative Efforts	224
(ii) Federal Law	226
(iii) Constitutional Objections to CAN-SPAM	229
(iv) Applying CAN-SPAM in Federal Court	231
4. Prosecution Options Available in the European Union	233
a. Obtaining Information, Help, and/or Directive	233

b. Remedies Available in the European Union	235
c. Implementation of the E-Privacy Directive	236
d. What Can Be Gained by Suing a Spammer in the European Union?	237
e. Conclusion	238
5. Strategies for Resolving the Scenario	238
CHAPTER 6: Electronic Evidence—Special Considerations	241
A. Unique Characteristics of Electronic Evidence	242
B. Authentication of Electronic Evidence	243
1. Authentication of E-Mail Messages	244
2. Authentication of Website Content	245
3. Authentication of Text Messages and Chat Room Content	246
4. Authentication of Electronic Public Records or Reports	247
5. Authentication of Computer-Stored Data and Records Produced in Civil Discovery or Seized in a Criminal Case	248
6. Authentication of Business Records Stored in a Computer	248
C. Hearsay Considerations	249
1. Business Records Exception	250
2. Other Exceptions	251
D. Challenging Authentication	252
E. Stipulated Authentication	252
F. Best Evidence Considerations	253
CHAPTER 7: Forensics and Experts	255
A. Scenario	256
B. Understanding the Expertise	257
C. How to Choose an Expert	257
1. What Credentials Should You Look For?	257
2. How Do You Find Experts?	258
3. How Much Do Expert Services Cost?	258
4. How Many Companies Should You Compare?	258
5. What Should an Expert Concentrate on First?	258
6. Can the Expert Write a Clear Report?	259
D. Computer Forensic Science	259
E. Forensics and the Scenario	260
F. Conclusion	264
APPENDICES	
APPENDIX A: Online Investigative Tools	265
APPENDIX B: Glossary	277
APPENDIX C: Federal Laws	305

APPENDIX D: State Laws	323
APPENDIX E: ICANN Policies & Rules	337
APPENDIX F: Form ICANN Complaints	367
APPENDIX G: Memorandum of Law in Support of Motion for Expedited Discovery (seeking identity of anonymous posters in defamation case)	399
APPENDIX H: Best Practice for the Seizure of Electronic Evidence	417
TABLE OF CASES	419
INDEX	441