

INTERNET CRIMES, TORTS AND SCAMS

Melise R. Blakeslee

Investigation and Remedies

OXFORD

Internet Crimes, Torts and Scams

Investigation and Remedies

Melise R. Blakeslee



OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press, Inc., publishes works that further Oxford University's objective of excellence in research, scholarship, and education.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi Kuala Lumpur Madrid Melbourne
Mexico City Nairobi New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece Guatemala Hungary Italy
Japan Poland Portugal Singapore South Korea Switzerland Thailand Turkey Ukraine
Vietnam

Copyright © 2010 by Oxford University Press, Inc.

Published by Oxford University Press, Inc.
198 Madison Avenue, New York, New York 10016

Oxford is a registered trademark of Oxford University Press
Oxford University Press is a registered trademark of Oxford University Press, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of Oxford University Press, Inc.

Library of Congress Cataloging-in-Publication Data

Blakeslee, Melise R.

Internet crimes, torts and scams: investigation and remedies / Melise R. Blakeslee.
p. cm.

Includes bibliographical references and index.

ISBN 978-0-19-537351-6 ((pbk.) : alk. paper)

1. Internet—Law and legislation. 2. Computer crimes—Investigation. 3. Evidence, Expert. I. Title.
K564.C6B57 2010
345'.0268—dc22

2009036784

1 2 3 4 5 6 7 8 9

Printed in the United States of America on acid-free paper

Note to Readers

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. 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 expert assistance is required, the services of a competent professional person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

*(Based on the Declaration of Principles jointly adopted by a Committee of the
American Bar Association and a Committee of Publishers and Associations.)*

<p>You may order this or any other Oxford University Press publication by visiting the Oxford University Press website at www.oup.com</p>

About the Author

Melise R. Blakeslee is the founder and president of Ecrimetools.com, the legal professional's Internet partner in fighting cybercrime. Ms. Blakeslee's legal practice is Internet- and litigation-oriented, with an active docket focusing on Internet crimes, complex software and copyright disputes. She has over 23 years of experience protecting and licensing IP in a wide variety of industry sectors, and has represented many famous brands and businesses. She is Managing Partner at Sequel Technology & IP Law, LLP. Previously, Ms. Blakeslee was a partner with McDermott Will & Emery where she served for nine years as the head of the e-Business & Cybercrime group.

Acknowledgments

To the extent I can trace my scholarly bent to any individuals, I owe a special debt to my grandfather, Arthur H. Blakeslee Sr., and to my parents, Ruth and Art Blakeslee, each of whom stewarded my small intellectual ability.

Secondary school teachers do not get many thanks from their pupils so I want to take this opportunity to recognize some teachers. First, to Mr. Giles Slaughter (the then-headmaster of Solihull School, England), thank you for giving me a chance. Second, to Mr. Costard, thank you for opening the door to the fun of debate and critical thinking (also at Solihull School).

Over the years my friends Toby Wyles, Britt Gilder, and Winifred Conkling, and my mentor, Ray Lupo, helped me achieve a degree of intellectual confidence I would not have otherwise possessed.

Thank you to my assistant, Lisa Miller. She has superb skills and patience with me.

Thank you to Norma McCarthy and James Keane for providing an Internet-connected writer's cottage in the wilds of West Wales.

Thank you to various associates and colleagues who have helped: my partner Clare Sellars, Osbourne Shaw, of the Internet Crimes Group; researcher Milton Shook; and creative brand "namer" and lyrics expert, Mark Gunnion; and to all the McDermott associates who supported me: Sarah Brown, Rita Siamas, Whitney Brown, Simone Blakeney, Daniel Powers, and Brendan Cowles.

I would like to particularly acknowledge the substantial contributions of Rohan Massey, Elliot Silverman, and Jeff Bedser.

Rohan Massey has been a partner of mine for many years. Rohan is a delight to work with because he is pragmatic, focused, and has a wicked sense of humour. Rohan contributed the European perspective to the Jurisdiction Quagmire chapter. He is a partner in the London office of McDermott Will & Emery. His practice focuses on media, e-commerce, outsourcing, IT and data protection. In addition to his contributions to this book, Rohan has authored, "Ambush Marketing," *International Chamber of Commerce UK Handbook*; "Transfers of Clinical Research Data from the European Union to the United States," *BNA's Medical Research Law and Policy Report*; "The Growing Concerns of Identity Theft," *Electronic Business Law*; "The Distance Marketing

of Financial Services—A UK Overview,” *Journal of Financial Services Marketing*; “The UK’s Proposed Framework Code of Practice for Sharing Information,” *World Data Protection Report*; and “Sales Promotion in the International Sales and Marketing Practice,” *Practical Law Company*. Rohan also contributes to “Law in Action” on BBC Radio.

Elliot Silverman is a litigation specialist at Jackson DeMarco Tidus & Peckenpaugh located in Irvine, California. The Jurisdiction Quagmire chapter reflects his deep and practical knowledge of this complicated topic. In addition to authoring the U.S. portion of the chapter, he has authored many other works, including: “In Search of Deep Pockets: Secondary Liability Under Federal and California Securities Laws,” *The Recorder*, May 2008; “Be Careful Out There: The IRS Has Lawyers in their Cross-Hairs,” *Orange County Lawyer*, January 2008. He has appeared in dozens of reported litigations.

Jeff Bedser is the president of the Internet Crimes Group, Inc. He coauthored the chapter on Forensics and Experts. Jeff and his team have been deeply helpful to the author in many investigations. Jeff is also a member of the ICANN Security & Stability Advisory Council.

Finally, thank you to Bill Carter, a philosopher, father to our three children, and friend for three decades.

Washington, D.C., London, and Ffynnon-Oer, Wales 2009

Contents

DETAILED CONTENTS	vii
ABOUT THE AUTHOR	xiii
ACKNOWLEDGMENTS	xv
CHAPTER 1: Introduction	1
CHAPTER 2: Basic Investigation	5
CHAPTER 3: Jurisdictional Quagmire	27
CHAPTER 4: Intellectual Property	67
CHAPTER 5: Freedom of Expression and the Problem of Anonymity	157
CHAPTER 6: Electronic Evidence—Special Considerations	215
CHAPTER 7: Forensics and Experts	229
APPENDICES	239
TABLE OF CASES	419
INDEX	437

Detailed Contents

ABOUT THE AUTHOR	xiii
ACKNOWLEDGMENTS	xv
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	15
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. An Example of a Simple Investigation Protocol	25
CHAPTER 3: Jurisdictional Quagmire	27
A. What's at Stake: Personal Jurisdiction and the Regulation of the Internet	29
B. Where Have We Been?	31
C. Life Is Complicated	32
D. First Principles	33
1. The Early Cases	33
2. <i>International Shoe</i> and the Rise of Long-Arm Statutes	34

3. Emerging Principles	35
a. General Jurisdiction	36
b. Specific Jurisdiction	37
c. In Rem Jurisdiction	38
E. Enter the Internet	39
F. Consider Functionality	41
G. Internet Activities Plus Business Contacts Equal General Jurisdiction	44
H. Specific Jurisdiction—Defamation	45
I. Recent Case Law: Specific Jurisdiction—Intellectual Property, Contracts, and Commercial Torts	48
1. Trademark Disputes	48
2. Copyright and Patent Disputes	49
3. Other Commercial Cases	49
J. Recent Case Law: Cybersquatting	50
K. Recent Case Law: The Role of Servers and ISPs	52
L. Resolution of the Scenarios	52
M. Long-Arm to Global Reach—International Considerations	53
1. The Complexity of International Jurisdictions	54
2. The European Perspective—First Principles	55
3. The E-Commerce Directive (2001/31)	55
4. The General Rule	56
a. Place of Establishment	56
b. The Coordinated Field	57
5. E-Commerce or Commerce?	58
6. Exceptions to the E-Commerce Directive	58
a. Jurisdiction Regulation	58
b. Rome I Regulation and the Rome Convention	59
7. National Courts versus Country of Origin Principle	59
8. Conclusion Regarding E-Commerce Directive	61
9. International Defamation	61
N. Scams and Torts—Unique Jurisdiction Considerations	63
CHAPTER 4: Intellectual Property	67
A. Trademarks and Domain Name Disputes	70
1. Scenarios	70
2. How to Investigate	70
a. The WHOIS Query	71
b. Dun & Bradstreet Reports	74
c. Review and Document How the Domain Is Used	74
d. Collect Ancillary Evidence	75
(i) Prior Use of Domain Name	75
(ii) Document a Registrant's Previous Instances of Cybersquatting	76

(iii) Document a Registrant's Ownership of Other Domain Names Incorporating Trademarks	76
e. Hire a Professional Investigator	77
3. The Law	77
a. What Is Cybersquatting?	77
(i) UDRP	79
(ii) ACPA	80
b. Other Types of Claims	83
(i) Traditional Trademark Infringement Claims	83
(ii) State Anticybersquatting Laws	83
c. Effectively Using Cease-and-Desist Letters	83
d. Drafting the UDRP Complaint	86
(i) Quick Recap of ACPA and UDRP Factors	86
(ii) Trademark Rights	87
(iii) Identical or Confusingly Similar	89
(iv) Rights or Legitimate Interests	91
(v) Making Legitimate Noncommercial or Fair Use of Domain Name	95
e. Drafting a Federal Claim	101
(i) Trademark Rights	102
(ii) Registers, Traffics or Uses	102
(iii) Identical or Confusingly Similar	102
(iv) Bad Faith Intent to Profit	104
f. UDRP Complaints: To Settle or Not to Settle	107
4. Strategy for Resolving the Scenarios	108
B. Trademark Use in Metatags and Keyword Advertising	112
1. More about the Technical Use of Metatags	114
2. How to Check a Web Page's Metatags	115
3. What Are Keywords and Sponsored or Keyed Ads?	116
4. How to Check For Sponsored Ads	117
5. The Law	117
a. Is this "Use in Commerce?"	118
b. Is Buying or Selling a Keyword a "Use in Commerce?"	123
c. Likelihood of Confusion and Initial Interest Confusion	125
d. Fair Use	129
6. Factors that May Affect the Outcome of an Infringement Claim	131
a. Metatags	132
b. Keywords	134
C. Theft of Content—Copyright and Confidential Information	135
1. Scenarios	136
2. How to Investigate	137
3. The Law	140
a. Basic Copyright	140
b. Fair Use of Copyrighted Material	143

c. Copyright, Facts and “Hot News”	145
d. There Are No Trade Secrets on the Internet	147
D. Counterfeiting	150
1. Scenario	150
2. How to Investigate	151
a. A Model of a Counterfeiting Network—Pharmaceuticals	151
b. Consider Registration and Hosting	154
c. More Tools and Tips	155
CHAPTER 5: Freedom of Expression and the Problem of Anonymity	157
A. Internet Service Provider Liability	159
1. Scenarios	159
2. How to Investigate	160
3. The Law	162
a. History of ISP Liability	162
b. Communication Decency Act, Section 230	164
(i) Broad Immunity for ISPs	164
(ii) Exceptions to Broad ISP Immunity	166
4. Internet Service Providers and Intellectual Property	168
a. Pre-Digital Millennium Copyright Act Liability	169
b. The Digital Millennium Copyright Act	171
c. ISP Liability under the DMCA: Cases	175
5. Internet Service Providers and the Fourth Amendment	177
6. Conclusion	178
B. Defamation	179
1. Scenario	179
2. How to Investigate	180
3. The Law	181
a. Publication v. Distribution	181
b. Expedited Discovery	186
c. Obtaining a Subpoena	188
4. Strategy	190
C. Spam	193
1. Scenario	193
2. How to Investigate	194
3. The Law	196
a. Defining Spam	196
b. Private Combat	197
c. Legal Combat	199
(i) State Legislative Efforts	199
(ii) Federal Law	201
(iii) Constitutional Objections to CAN-SPAM	204
(iv) Applying CAN-SPAM in Federal Court	206

4. Prosecution Options Available in the European Union	208
a. Obtaining Information, Help, and/or Directive	208
b. Remedies Available in the European Union	209
c. Implementation of the E-Privacy Directive	210
d. What Can Be Gained by Suing a Spammer in the European Union?	212
e. Conclusion	213
5. Strategies for Resolving the Scenario	213
CHAPTER 6: Electronic Evidence—Special Considerations	215
A. Unique Characteristics of Electronic Evidence	216
B. Authentication of Electronic Evidence	217
1. Authentication of E-Mail Messages	218
2. Authentication of Web Site Content	220
3. Authentication of Text Messages and Chat Room Content	221
4. Authentication of Electronic Public Records or Reports	221
5. Authentication of Computer-Stored Data and Records Produced in Civil Discovery or Seized in a Criminal Case	222
6. Authentication of Business Records Stored in a Computer	222
C. Hearsay Considerations	223
1. Business Records Exception	224
2. Other Exceptions	225
D. Challenging Authentication	226
E. Stipulated Authentication	226
F. Best Evidence Considerations	227
CHAPTER 7: Forensics and Experts	229
A. Scenario	230
B. Understanding the Expertise	231
C. How to Choose an Expert	231
1. What Credentials Should You Look For?	231
2. How Do You Find Experts?	232
3. How Much Do Expert Services Cost?	232
4. How Many Companies Should You Compare?	232
5. What Should an Expert Concentrate on First?	232
6. Can the Expert Write a Clear Report?	233
D. Computer Forensic Science	233
E. Forensics and the Scenario	234
F. Conclusion	238
APPENDICES	
APPENDIX A: Online Investigative Tools	239
APPENDIX B: Glossary	251

APPENDIX C: Federal Laws	279
APPENDIX D: State Laws	323
APPENDIX E: ICANN Policies and Rules	337
APPENDIX F: Form ICANN Complaints	365
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	437

CHAPTER 1

Introduction

*Let's start at the very beginning,
A very fine place to start
"Do-Re-Mi"¹
—The Sound of Music*

A. Approach	2
B. Structure	2
C. Tempest in a Teapot—What Is Not Covered	3

Thieves, counterfeiters, name-callers, predators, gamblers, scammers, infringers, pornographers, drug dealers, and spies exist on the Internet just as in any other arena of human activity. However, investigation and prosecution of Internet crimes² fundamentally differs from crimes in the “real” world.

If a thief bursts into a store, bops the owner over the head, and runs off with the till, most legal professionals know how to question a witness, gather potential evidence, and assess other relevant information. At the very least, you as the legal professional will know enough to call the local police!

But who do you call if a client is a victim of Internet fraud? Do you have any idea what type of evidence might exist? Can you thoroughly explain the

1. Lyrics by Oscar Hammerstein.

2. This book uses the phrases *Internet crime* and *Internet criminals* to refer collectively to any type of scoundrel engaged in malicious Internet activity, including those who are, in fact, criminals. It must be recognized, however, that many of the activities described in this book are not criminal per se. The terms *Internet crime* or *criminals* are convenient labels for all those who perpetrate scams, torts, lies, infringements, or actual crimes via the Internet.

problem to someone else? Probably not. There is a startling gap between our ability to deal with scams in the real world and our ability to even understand an Internet scam.

Accordingly, this book is intended to explain the legal implications of the Internet's infrastructure and teach you how to look for and interpret the evidence.

A. Approach

This book is primarily a practical one. The chapters are organized by type of problem instead of by legal topic as the author feels this is the most suitable arrangement. Many legal professionals can identify a problem in a general way (i.e., as defamation or counterfeiting), but may not be able to identify the wide range of interdisciplinary laws needed for resolution to resolve a problem when it occurs on the Internet.

For example, an offer to sell stolen DVD decryption technology is a copyright problem (and possibly more) a mere rehash of copyright law is not what is needed, however. The legal professional needs to understand Internet infrastructure, to recognize the online and other tools needed to identify the infringers, to obtain information about jurisdiction, to be aware of the list of elements necessary to obtain a subpoena, and to have an understanding of criminal and civil computer trespass laws. This book gathers this constellation of information into sections organized by the general type of problem, such as *theft*, *defamation*, and *cybersquatting*.

B. Structure

This book begins with a technology chapter called "Basic Investigation." This chapter is aimed at those who possess only a basic knowledge of Internet infrastructure. You will gain an understanding about the Internet's history, how its layers work, and how information is distributed and traced. The practice tips are based on the author's extensive experience, and provide practical guidance on how to apply the particular information to daily practice.

Jurisdiction is an overarching issue implicated in a growing number of investigations—and certainly, almost always in the more complex ones. The Internet is global. This creates strategic opportunities to use jurisdiction to the best advantage. These subjects are given prime attention in the second chapter, "Jurisdictional Quagmire."

Each subsequent chapter begins with a scenario, which is the jumping-off point for specific step-by-step instructions on how to investigate the particular problem. The scenarios are followed by a subsection discussing the applicable law. Finally, each chapter ends with an analysis of how the investigation and law come together to resolve the scenario.

At the end of the book are important appendices. The two likely to be the most important are the glossary and the list of online investigative tools. The glossary goes beyond standard definitions and provides insight into interpretations in the case law of many of the defined words. The list of investigative tools is a list of Web sites providing access (sometimes via a subscription) to information fundamentally important to all investigations.

The resources listed in this book will change frequently, so updated tools and information are located at www.ecrimetools.com.

C. Tempest in a Teapot—What Is Not Covered

Cyberbullying, denial-of-service attacks, viruses, and theft of an individual's personal information often make headlines, but amount to little more than a "tempest in a teapot" from a legal perspective. These problems simply do not result in case law. The author believes this is true because despite all the press coverage, many of these problems often do not lead to quantifiable damages. This book covers only those problems most likely to arise in civil practice. Updates to this book will report headline-making problems should any result in actual claims and case law. eCrimeTools.com, which offers a database of the cases discussed in this book, will be updated to add developing law.

