

CYBER CRIME AND
DIGITAL EVIDENCE:
MATERIALS AND CASES

Thomas K. Clancy



LexisNexis

CYBER CRIME AND DIGITAL EVIDENCE:

MATERIALS and CASES

Thomas K. Clancy
Director and Research Professor
National Center for Justice and the Rule of Law
University of Mississippi School of Law



ISBN: 978-1-4224-9408-0

Library of Congress Cataloging-in-Publication Data

Clancy, Thomas K.

Cyber crime and digital evidence : materials and cases / Thomas K. Clancy.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-4224-9408-0 (hardbound)

1. Electronic evidence--United States. 2. Evidence, Documentary--United States. 3. Electronic records--Law and legislation--United States. 4. Computer crimes--United States. I. Title.

KF8947.5.C58 2011

345.73'0268--dc23

2011033094

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 expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks and Michie is a trademark of Reed Elsevier Properties Inc., used under license. Matthew Bender and the Matthew Bender Flame Design are registered trademarks of Matthew Bender Properties Inc.

Copyright © 2011 Matthew Bender & Company, Inc., a member of the LexisNexis Group.
All Rights Reserved.

No copyright is claimed in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material exceeding fair use, 17 U.S.C. § 107, may be licensed for a fee of 25¢ per page per copy from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

NOTE TO USERS

To ensure that you are using the latest materials available in this area, please be sure to periodically check the LexisNexis Law School web site for downloadable updates and supplements at www.lexisnexus.com/lawschool.

Editorial Offices

121 Chanlon Rd., New Providence, NJ 07974 (908) 464-6800

201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200

www.lexisnexus.com

MATTHEW  BENDER

PREFACE

This book is designed to be an accessible introduction to Cyber Crime and Digital Evidence. The title is consciously styled: *Cyber Crime and Digital Evidence: Materials and Cases*. The title illuminates two significant aspects of this book. First, cyber crime is only a subset of a much broader trend in the criminal area, which is the use of digital evidence in virtually all criminal cases. Hence, it is important to understand the legal framework that regulates obtaining that increasingly used and important evidence. Second, by listing “materials *and* cases” — in that order — the title signals that this book attempts to provide a broader framework than an endless stream of cases offers. Law students deserve the broader context and, hopefully, will get some of it with this book.

This book is the product of numerous influences, ranging from many years of teaching law students, studying the Fourth Amendment and cyber crime, and witnessing the explosion of the use of digital evidence in criminal cases. Most immediately, I thank those who provided comments and insights on various aspects of the book. Those individuals include Don Mason, Will Wilkins, and Priscilla Grantham. I received invaluable editorial assistance from Andrew Coffman. For the past decade, I have had the privilege of serving as Director of the National Center for Justice and the Rule of Law and Research Professor at the University of Mississippi School of Law, where I created and developed national programs on cyber crime and the Fourth Amendment. Through those programs, the Center offers educational opportunities to judges, prosecutors, and law enforcement on search and seizure, including in emerging areas such as computer searches and seizures, and on broad areas concerning cyber crime. The conferences, lectures, and associations developed at the Center have brought many of the best minds in the country to Oxford, Mississippi to examine the new trends in the criminal law involving new forms of criminal activity and new forms of evidence. The thousands of judges, assistant attorneys general, and other attendees of the Center’s events contributed many insights about actual litigation and law enforcement practices, as well as other challenges involved in adapting criminal law, procedure, and practice to the digital age. From each of those participants I have learned much and I deeply appreciate their contributions.

Thomas K. Clancy
December 1, 2011

A NOTE ON EDITING

The cases and materials in this book are extensively edited and most changes are done without acknowledgment of omissions of text or other material. Footnotes may be omitted or numbering changed. Capitalization and formatting are often changed based on omissions to the text. The reader should always consult the original source before citing or quoting material herein.

TABLE OF CONTENTS

Chapter 1	INTRODUCTION	1
Chapter 2	OBTAINING DIGITAL EVIDENCE: AN INTRODUCTION	7
§ 2.1	ANALYTICAL STRUCTURE OF FOURTH AMENDMENT QUESTIONS	8
1.	Applicability	8
2.	Satisfaction	11
3.	Remedies	11
4.	Independent State Grounds	12
§ 2.2	INTRODUCTION TO THE STATUTORY FRAMEWORK	12
§ 2.3	A CASE STUDY: MAJOR STEPS IN A TYPICAL INTERNET INVESTIGATION	13
	<i>United States v. Steven C. Perrine</i>	13
	Notes	19
Chapter 3	FOURTH AMENDMENT APPLICABILITY: “INSIDE THE BOX”	21
§ 3.1	EXPECTATION OF PRIVACY ANALYSIS	21
1.	In General	21
2.	The Location of the Computer	21
3.	Data on Work Computers — Governmental Employer	22
4.	The Supreme Court Avoids the Issue	23
	Notes	29
5.	Emails on Work Computer	29
	<i>Robin Brown-Criscuolo v. Robert K. Wolfe</i>	29
	<i>State v. Eric M. Young</i>	32
	Notes	34
§ 3.2	PRIVATE SEARCHES AND SEIZURES	35
1.	In General	35
2.	Who is a Government Agent	35
3.	Replication and “Context” Issues: Defining the “Container”	37
	Questions and Comments	41
	<i>People v. Joseph Michael Wilkinson</i>	44
	Notes	47

TABLE OF CONTENTS

Chapter 4	COMPETING VIEWS OF THE NATURE OF DIGITAL EVIDENCE SEARCHES	49
§ 4.1	INTRODUCTION	49
§ 4.2	PLAIN VIEW DOCTRINE	50
1.	Distinguishing Merely Looking	53
	<i>United States v. Artem Bautista David</i>	53
2.	“Immediately Apparent”	54
	<i>United States v. Devin C. Wilson</i>	54
	Notes	56
3.	Opening Closed Files: The Document Approach	57
	<i>United States v. Montgomery Johns Gray</i>	57
	Notes and Questions	60
4.	Opening Closed Files: The Special Approach	61
5.	Independent State Grounds: Inadvertence and File Names	62
	<i>Larry R. Frasier, Jr. v. State</i>	62
	Questions	65
§ 4.3	DOCUMENT SEARCHES	65
1.	Data Are Forms of Records/Container Analogy	66
	<i>United States v. Curtis Robert Williams</i>	69
2.	Rejection of the Document Search and Container Analogy: A “Special Approach”	74
	<i>United States v. Michael Clay Payton</i>	76
	<i>People v. Robert Carratu</i>	81
	Notes and Questions	83
	Notes and Questions	87
	Notes and Questions	89
§ 4.4	LIMITATIONS BASED ON SEARCH EXECUTION PROCEDURES IN WARRANTS	89
1.	Supreme Court Opinions on Execution Procedures	89
2.	Search Protocols — Digital Evidence Cases	90
a.	Rejecting Protocol Requirement	90
	<i>United States v. Brent Ray Brooks</i>	90
b.	Taint Teams and Special Masters	91
	<i>Donald F. Manno v. Christopher J. Christie</i>	91
c.	The Special Approach	94
	<i>United States v. Comprehensive Drug Testing, Inc.</i>	94
	Notes	107

TABLE OF CONTENTS

Chapter 5	WARRANTS FOR DIGITAL EVIDENCE: PARTICULARITY CLAIMS AND BROAD SEIZURES .	109
§ 5.1	IN GENERAL	109
§ 5.2	VARIETIES OF COMPUTER SEARCHES	109
1.	Searches for Computer Equipment	110
	<i>State v. Kenneth Stapleton</i>	111
	Notes	112
2.	Searches for Data	113
§ 5.3	GENERAL PRINCIPLES — PARTICULARITY	113
	<i>United States v. Loretta Otero</i>	113
	Notes	118
1.	Items to be Seized: The Container Approach	118
	<i>People v. Kelli Marie Balint</i>	118
2.	Items to be Seized: The Special Approach	121
§ 5.4	A WARRANT EXERCISE	121
Chapter 6	SEARCH EXECUTION ISSUES	129
§ 6.1	INTERMINGLED DOCUMENTS	129
§ 6.2	ON-SITE VS. OFF-SITE SEARCHES	130
§ 6.3	USE OF EXPERTS	134
§ 6.4	DELETED FILES	134
§ 6.5	TIME PERIODS FOR WARRANTS TO BE VALID	135
	<i>State v. Keith R. Nadeau</i>	138
	Notes	139
Chapter 7	CONSENT SEARCHES; COMPELLING DISCLOSURE OF PASSWORDS	141
§ 7.1	CONSENT — IN GENERAL	141
§ 7.2	CONSENT — SCOPE ISSUES	142
	<i>People v. Robert S. Prinzing</i>	142
	Notes	148
1.	Scope: Does consent to search include forensic exam?	148
	<i>United States v. Jonathan Luken</i>	148
2.	Cell Phones: Scope of Consent	150
	<i>Jermaine L. Smith v. State</i>	150
§ 7.3	THIRD PARTY CONSENT	151
1.	Passwords and Encryption	152
	<i>United States v. Ray Andrus</i>	153
	<i>United States v. Frank Gary Buckner</i>	159
	Notes	161

TABLE OF CONTENTS

§ 7.4	FIFTH AMENDMENT PRIVILEGE: REQUIRING THE DISCLOSURE OF PASSWORDS, DECRYPTED FILES	161
	<i>In Re Grand Jury Subpoena To Sebastien Boucher</i>	162
	Notes	165
Chapter 8	CELL PHONES, OTHER MOBILE DIGITAL DEVICES, AND TRADITIONAL FOURTH AMENDMENT DOCTRINE PERMITTING WARRANTLESS SEARCHES	167
§ 8.1	SEARCH INCIDENT TO ARREST	167
1.	Basic Principles	167
2.	Permissible Objects Sought	168
3.	Cell Phone Searches Incident to Arrest	169
	<i>State v. Antwaun Smith</i>	169
4.	Location of the Search	173
	<i>People v. Gregory Diaz</i>	175
	Questions	177
5.	Scope: Areas Within the Arrestee's "Control"	178
6.	Scope: Vehicle Searches Incident to Arrest	179
	<i>Arizona v. Rodney Joseph Gant</i>	179
	Questions	181
§ 8.2	ADDITIONAL THEORIES TO JUSTIFY A SEARCH AND THE SCOPE OF A PERMISSIBLE SEARCH OF CELL PHONES: VIEWING IMAGES DISPLAYED, BROWSING, ANSWERING CALLS	182
	<i>State v. Jermichael James Carroll</i>	182
	Notes	187
Chapter 9	SEIZURES OF DIGITAL EVIDENCE	189
§ 9.1	INTANGIBLE PROPERTY AND DIGITAL EVIDENCE	189
§ 9.2	SEIZURES OF DIGITAL EVIDENCE	196
	<i>United States v. Howard Wesley Cotterman</i>	197
1.	Revocation of Consent After the Mirror Image is Made	198
	<i>United States v. Youssef Samir Megahed</i>	198
	Notes	199
2.	Digital Seizures: Seeking a Workable Definition	199
3.	Is There a Need for Special Rules for Digital Evidence?	200
	Notes and Questions	202
§ 9.3	THE REASONABLENESS OF WARRANTLESS SEIZURES OF DIGITAL DEVICES	204
1.	Warrantless Seizures	204
	<i>Commonwealth v. Charles Hinds, Jr.</i>	204
	<i>Commonwealth v. Harold Kaupp</i>	205

TABLE OF CONTENTS

2.	Delays to Obtain a Warrant after a Warrantless Seizure	206
	<i>United States v. Peter J. Mitchell</i>	206
	<i>People v. Yoshiaki Shinohara</i>	209
	Notes	210
Chapter 10	SEARCHES AT THE INTERNATIONAL BORDER	213
§ 10.1	OVERVIEW OF THE INTERNATIONAL BORDER DOCTRINE	213
§ 10.2	LETTERS AS TARGETS	216
§ 10.3	DATA AS TARGETS	218
	<i>United States v. Michael Timothy Arnold</i>	219
	Notes and Questions	221
§ 10.4	DEFINING THE BORDER	222
Chapter 11	FOURTH AMENDMENT APPLICABILITY TO NETWORKS AND THE INTERNET	225
§ 11.1	INTRODUCTION — “OUTSIDE THE BOX”	225
§ 11.2	VOLUNTARY EXPOSURE/ASSUMPTION OF RISK	225
1.	Peer-to-Peer Distribution Schemes	225
	<i>United States v. Charles A. Borowy</i>	226
	Notes	228
2.	Email Received and Chatroom Communications	229
	<i>Commonwealth v. Robert D. Proetto</i>	229
	Notes	231
	<i>People v. David Gariano</i>	231
	Notes	233
§ 11.3	INTERNET SURVEILLANCE: TYPES OF INFORMATION SOUGHT	233
1.	Background Principles	233
	<i>Michael Lee Smith v. State</i>	233
2.	Types of Information Available: Content vs. Non-Content	239
	<i>United States v. Mark Stephen Forrester</i>	246
3.	An Alternative View — Independent State Grounds	248
	<i>State v. Shirley Reid</i>	248
	Notes	253
§ 11.4	INFORMATION OBTAINED FROM THIRD PARTIES AND FROM THE CLOUD	253
	Notes and Questions	255
Chapter 12	STATUTORY REGULATION OF OBTAINING DATA .	257
§ 12.1	INTRODUCTION	257
§ 12.2	THE PEN/TRAP STATUTE, 18 U.S.C. §§ 3121-3127	258

TABLE OF CONTENTS

1.	Application for Internet Communications	259
	<i>In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Trap & Trace Device on E-mail Account</i>	259
2.	“Post-Cut-Through Dialed Digits”	260
	<i>In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices</i>	260
3.	Content Related to Internet Activity	261
	<i>In Re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap On [xxx] Internet Service Account/user Name</i>	261
4.	Remedies under the Pen Register Statute	262
	<i>United States v. Mark Stephen Forrester</i>	262
	Notes	263
§ 12.3	THE WIRETAP STATUTE, 18 U.S.C. §§ 2510-22	264
1.	Definitions	264
2.	Wiretap Orders 18 U.S.C. § 2518	266
	Notes	267
3.	Remedies for Violations of the Wiretap Statute	267
4.	Exceptions to the general prohibition against wiretapping include:	268
§ 12.4	STORED COMMUNICATIONS ACT 18 U.S.C. §§ 2701-12	269
1.	Overview	270
	<i>In the Matter of the Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to Not Disclose the Existence of the Search Warrant</i>	270
2.	Framework to analyze the SCA	272
	<i>Andersen Consulting LLP v. UOP and Bickel & Brewer</i>	273
	<i>Jerilyn Quon v. Arch Wireless Operating Co.</i>	275
	<i>George Theofel v. Alwyn Farey-Jones</i>	279
	<i>Ernest Flagg v. City of Detroit</i>	282
	<i>Michael Aaron Jayne v. Sprint PCS</i>	289
3.	Compelling Disclosure § 2703	291
4.	SCA Process for Compelled Disclosure: Uncertain Status under the Fourth Amendment	293
	<i>Steven Warshak v. United States</i>	293
	<i>United States v. Steven Warshak</i>	298
5.	Miscellaneous SCA Provisions	304
	Notes	305

TABLE OF CONTENTS

Chapter 13	OBSCENITY AND CHILD PORNOGRAPHY	307
§ 13.1	OBSCENITY	307
1.	The <i>Miller</i> Standard	307
	<i>Marvin Miller v. California</i>	307
2.	Community Standards	310
	<i>United States v. Robert Alan Thomas</i>	310
	<i>United States v. Jeffrey A. Kilbride</i>	313
§ 13.2	EVOLUTION OF CHILD PORNOGRAPHY REGULATION AS A SEPARATE CATEGORY OF PROHIBITED SPEECH	319
	<i>New York v. Paul Ira Ferber</i>	321
1.	Possession of Child Pornography	325
	<i>Clyde Osborne v. Ohio</i>	325
2.	Virtual Child Pornography	327
	<i>John D. Ashcroft v. The Free Speech Coalition</i>	327
3.	Pandering	336
	<i>United States v. Michael Williams</i>	336
	Notes	340
4.	Morphed Images	340
	<i>United States v. Dale Robert Bach</i>	340
	Notes	342
5.	Obscene Cartoons Featuring Children	343
	<i>United States v. Christopher S. Handley</i>	343
	<i>United States v. Dwight Edwin Whorley</i>	345
§ 13.3	ELEMENTS OF CHILD PORNOGRAPHY OFFENSES	347
1.	Distribution	347
	<i>United States v. Joshua P. Navrestad</i>	347
	<i>United States v. William Ralph Dodd</i>	352
	Notes	354
2.	Possession; Access with Intent to View	354
	<i>United States v. Stuart Romm</i>	355
	<i>United States v. Brian Bass</i>	359
	<i>State v. Benjamin W. Mercer</i>	362
	Notes	368
§ 13.4	PROVING AT TRIAL THAT THE IMAGE DEPICTS A REAL CHILD	368
	<i>United States v. Tom Vig</i>	368
	<i>United States v. Anthony Marchand</i>	370
	Notes	376
§ 13.5	COMMON SEARCH AND SEIZURE ISSUES IN CHILD PORNOGRAPHY CASES	377
1.	Probable Cause to Believe a Person Possesses Child Pornography	378

TABLE OF CONTENTS

a.	Subscribers of Child Pornography Web Sites	379
	Notes	380
b.	Retention Habits of Collectors	380
c.	Pedophile Profiles	381
	<i>United States v. Edward S. Macomber</i>	381
	Notes	384
d.	Staleness	384
	<i>United States v. William David Burkhart</i>	386
	Notes	389
e.	Locating the Computer: IP Addresses; Screen Names; Nexus	
	Questions	389
	<i>United States v. Javier Perez</i>	390
	Notes	391
2.	Sufficiency of the Descriptions of Sexual Activity in the Affidavit	393
	<i>United States v. Justin Barrett Hill</i>	393
	<i>United States v. Richard Genin</i>	394
	Notes	400
§ 13.6	SELF-PRODUCED CHILD PORNOGRAPHY AND SEXTING	400
	Mary Graw Leary, <i>Self-Produced Child Pornography: The Appropriate</i>	
	<i>Societal Response to Juvenile Self-Sexual Exploitation</i>	400
	<i>Maryjo Miller v. Jeff Mitchell in His Official Capacity as District Attorney</i>	
	<i>of Wyoming County, Pennsylvania</i>	404
	Notes	409
Chapter 14	POLICING THE INTERNET FOR CRIMES INVOLVING	
	EXPLOITATION OF CHILDREN	411
§ 14.1	TRAVELER CASES	411
	<i>United States v. Erik D. Zahursky</i>	412
§ 14.2	USING A COMPUTER TO ENTICE A CHILD; ENTRAPMENT	418
	<i>State v. James R. Pischel</i>	418
	<i>United States v. Mark Douglas Poehlman</i>	423
	Notes	430
§ 14.3	LIABILITY OF SOCIAL NETWORKING SITES	431
	<i>Julie Doe II, A Minor v. Myspace Incorporated</i>	431
Chapter 15	PROPERTY CRIMES AND COMPUTER MISUSE	439
§ 15.1	INTRODUCTION	439
§ 15.2	TRADITIONAL PROPERTY CRIMES	440
1.	Larceny and Theft	441
2.	Applying Traditional Views	442
	<i>Charles Walter Lund v. Commonwealth</i>	442

TABLE OF CONTENTS

	<i>State v. Michael McGraw</i>	445
3.	Expanding the Concepts of “Property” and “Taking”	447
	<i>State v. Randal Lee Schwartz</i>	447
	<i>United States v. Bertram E. Seidlitz</i>	450
	Notes	452
Chapter 16	COMPUTER SPECIFIC CRIMES: OBTAINING CONFIDENTIAL INFORMATION, UNAUTHORIZED ACCESS, FRAUD, AND DAMAGE	453
§ 16.1	OVERVIEW: COMPUTER FRAUD AND ABUSE ACT — 18 U.S.C. § 1030	453
§ 16.2	KEY DEFINITIONS OF THE CFAA	455
1.	Protected Computer	455
a.	Current Version of “Protected Computer”	455
	<i>United States v. Chad A. Powers</i>	456
b.	Evolution of the Types of Computers Protected	457
	<i>Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.</i>	457
2.	Intentional Access	459
a.	How to Restrict Access: Code-Based and Contract-Based Restrictions	459
	<i>Ef Cultural Travel BV v. Zefer Corporation</i>	460
	<i>United States v. Lori Drew</i>	462
	<i>United States v. Lori Drew</i>	462
	<i>State v. Anthony A. Allen</i>	463
	<i>State v. Joseph N. Riley</i>	466
3.	Without or in Excess of Authorization	467
a.	Agency Theory To Find Lack of Authorization	469
	<i>Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.</i>	469
b.	Rejection of Employee Breach of Duty as Basis	470
	<i>Bell Aerospace Services, Inc. v. U.S. Aero Services, Inc.</i>	471
c.	Non-Intended Use as Basis	473
	<i>United States v. Dimetriace Eva-Lavon John</i>	473
d.	Websites: Terms of Use and Technical Barriers	475
	<i>Facebook, Inc. v. Power Ventures, Inc.</i>	475
	<i>United States v. Lori Drew</i>	478
	Notes	486
§ 16.3	SPECIFIC SUB-SECTIONS OF § 1030	486
1.	Obtaining Confidential Information.	486
	<i>Brenda Czech v. Wall Street on Demand, Inc.</i>	487
2.	Trespassing into a Government Computer 18 U.S.C. § 1030(a)(3). . . .	489
3.	Accessing to Defraud and Obtain Value 18 U.S.C. § 1030(a)(4). . . .	490

TABLE OF CONTENTS

	<i>United States v. Richard W. Czubinski</i>	492
4.	Damaging a Computer or Information 18 U.S.C. § 1030(a)(5)	494
	<i>United States v. Robert Tappan Morris</i>	498
	Notes	501
	<i>International Airport Centers v. Jacob Citrin</i>	501
	<i>United States v. Allan Carlson</i>	503
	<i>United States v. Nicholas Middleton</i>	505
	Notes	509
Chapter 17	INTELLECTUAL PROPERTY THEFT	511
§ 17.1	COPYRIGHT	511
1.	17 U.S.C. § 506(a) provides:	513
2.	Evolution of File Sharing	515
	<i>A&M Records, Inc. v. Napster, Inc.</i>	515
	<i>Sandra Leigh King, While You Were Sleeping</i>	524
	Notes	531
3.	Illegal “Warez” Organizations and Internet Piracy	531
	Notes	534
§ 17.2	THE DIGITAL MILLENIUM COPYRIGHT ACT, 17 U.S.C.	
	§§ 1201-05	534
	<i>United States v. Elcom Ltd.</i>	536
1.	Example of Circumventing Access Controls	537
2.	Example of Trafficking	537
	<i>Universal City Studios, Inc. v. Eric Corley</i>	537
	Notes	543
3.	DMCA meets Video Gaming	543
	<i>Sandra Leigh King, While You Were Sleeping</i>	543
Chapter 18	SPYWARE, ADWARE, MALWARE; PHISHING; SPAM; AND IDENTITY-RELATED CRIME	547
§ 18.1	SPYWARE, ADWARE, MALWARE	547
	<i>People v. Direct Revenue</i>	549
	Notes	552
§ 18.2	PHISHING	555
	<i>Facebook, Inc. v. Jeremi Fisher</i>	555
	Notes	558
§ 18.3	SPAM	558
	<i>United States v. Jeffrey A. Kilbride</i>	563
	<i>United States v. Michael Steven Twombly</i>	567
	Notes	569
§ 18.4	IDENTITY-RELATED CRIME	570

TABLE OF CONTENTS

	<i>United States v. Vladimir Cabrera</i>	572
	Notes	576
Chapter 19	OTHER CRIMES AGAINST PERSONS: CYBERBULLYING, THREATS, STALKING, HARASSMENT, AND DEFAMATION	577
§ 19.1	CYBERBULLYING	578
	Questions	579
	Notes	583
§ 19.2	THREATS	584
	<i>People v. Alan Munn</i>	584
	<i>United States v. Abraham Jacob Alkhabaz</i>	586
	Notes	595
§ 19.3	STALKING AND HARASSMENT	596
1.	The Impact of Technology	596
2.	Criminalization of Harassment	601
	Susan W. Brenner & Megan Rehberg, “Kiddie Crime”? <i>The Utility of Criminal Law in Controlling Cyberbullying</i>	601
	<i>State v. Ellison</i>	603
	<i>A.B. v. State</i>	605
	Susan W. Brenner & Megan Rehberg, “Kiddie Crime”? <i>The Utility of Criminal Law in Controlling Cyberbullying</i>	608
	<i>People v. Darren S. Kochanowski</i>	611
	Notes	612
§ 19.4	DEFAMATION	613
	Susan W. Brenner & Megan Rehberg, “Kiddie Crime”? <i>The Utility of Criminal Law in Controlling Cyberbullying</i>	613
	<i>Thomas Mink v. Susan Knox</i>	614
	Notes	620
Chapter 20	SENTENCING	623
§ 20.1	FEDERAL SENTENCING GUIDELINES — ENHANCEMENTS	623
1.	Use of Computer	624
	<i>United States v. Todd Franklin Lewis</i>	624
2.	Special Skills	626
	<i>United States v. Kent Aoki Lee</i>	626
	Notes	631
§ 20.2	SENTENCING IN CHILD PORNOGRAPHY CASES	631
	<i>United States v. Jerry Paull</i>	631
	<i>United States v. Justin K. Dorvee</i>	635
§ 20.3	RESTRICTIONS ON INTERNET USE OR USING COMPUTERS	639

TABLE OF CONTENTS

<i>United States v. Ronald Scott Paul</i>	639
<i>United States v. Mark Wayne Russell</i>	640
<i>United States v. Arthur William Heckman</i>	643
Notes	646
TABLE OF CASES	TC-1
INDEX	I-1