

CYBERCRIME

CYBERCRIME

THE INVESTIGATION, PROSECUTION AND
DEFENSE OF A COMPUTER-RELATED CRIME

Third Edition

EDITED BY

RALPH D. CLIFFORD

PROFESSOR OF LAW
UNIVERSITY OF MASSACHUSETTS
SCHOOL OF LAW

CAROLINA ACADEMIC PRESS

Durham, North Carolina

Copyright © 2011
Ralph D. Clifford
All Rights Reserved

Library of Congress Cataloging-in-Publication Data

Clifford, Ralph D.

Cybercrime : the investigation, prosecution and defense of a computer-related crime / [edited by] Ralph D. Clifford. -- 3rd ed.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-59460-853-7 (alk. paper)

1. Computer crimes--United States. 2. Computers--Law and legislation--United States. 3. Transnational crime. I. Title.

KF390.5.C6C924 2011

345.73'0268--dc23

2011020479

CAROLINA ACADEMIC PRESS

700 Kent Street

Durham, North Carolina 27701

Telephone (919) 489-7486

Fax (919) 493-5668

www.cap-press.com

Printed in the United States of America

CONTENTS

Chapter One • Introduction	3
<i>Ralph D. Clifford</i>	
Chapter Two • Defining Cybercrime: A Review of Federal and State Law	15
<i>Susan W. Brenner</i>	
I. Introduction	15
II. Cybercrimes: New Crimes or Old Wine in New Bottles?	17
III. Federal Cybercrime Legislation	21
A. Cybercrimes Where the Computer Is the Target	22
1. Hacking, Cracking, Fraud, Virus Dissemination and Extortion	22
2. Unauthorized Access to Stored Electronic Communications	38
B. Cybercrimes Involving Improper Communications	40
1. Sending Obscene, Abusive or Harassing Communications	40
2. Online Stalking, Harassment and Threats	41
3. Spam	44
C. Cybercrimes Involving Minors	49
1. Sexual Exploitation of Children	49
2. Sending Offensive Material to Minors	59
3. Transmitting Information about a Minor	61
D. Cybercrimes Involving Fraud and Other Traditional Misconduct	62
1. Mail and Wire Fraud	62
2. Fraud in Connection with Access Devices	65
3. Transporting Stolen Property	68
E. Identity Theft	69
F. Intellectual Property Crimes	72
1. Copyright Infringement	73
2. Trademark Infringement	89

3. Trade Secret Infringement	92
IV. State Cybercrime Legislation	94
A. Cybercrimes where the Computer Is the Target	94
1. Hacking and Cracking	94
2. Denial of Service Attacks	96
B. Cybercrimes Involving Improper Communications	96
1. Cyberstalking	96
2. State Spam Laws	97
C. Cybercrimes Involving Minors	98
D. Cybercrimes Involving Fraud and Other Traditional Misconduct	99
1. Computer Forgery	99
2. Computer Fraud and Theft	99
3. Computer Extortion	100
E. Identity Theft	100
F. Cyberterrorism	101
G. Miscellaneous Cybercrime Offenses	102
V. Conclusion	103
 Chapter Three • The Investigation and Prosecution of a Cybercrime	 105
<i>Ivan Orton</i>	
I. Introduction to the Scenarios	108
A. Case 1—Janet Davis	108
B. Case 2—Mel Howard	109
1. Domain Hijacking	109
2. Massive File Deletions	112
C. Case 3—Allen Worley	113
II. Tracing E-mail	117
III. Obtaining Records from Third Party Record Holders	120
A. Electronic Communications Privacy Act	121
1. What Does the ECPA Cover?	121
2. What Does the ECPA Prohibit?	121
3. When Is a Disclosure to the Government Allowed?	121
4. What Is the Remedy for Violation of This Act?	123
B. Practical Issues	124
1. Limitations of Third Party Records	125
2. How to Obtain the Records	127
3. Contact the ISP and then Serve the Warrant/Subpoena	128
C. The Case Scenarios	129
1. Case 1—Janet Davis	129
2. Case 2—Mel Howard	129
3. Case 3—Allen Worley	132

IV. Search Warrants	132
A. Acquisition of Evidence	137
1. What Crimes?	137
2. What Computers?	137
3. Legal Limits on Searches	138
B. Analysis of Evidence	171
1. At the Search Location	171
2. Offsite/Detailed Analysis	175
3. Can Computers Be Taken Offsite for Examination?	178
4. What Must Be Returned and When	178
C. The Case Scenarios	181
1. Case 1—Janet Davis	181
2. Case 2—Mel Howard	182
3. Case 3—Allen Worley	183
V. The Use of the Seized Material and the Final Results	189
A. Case 1—Janet Davis	189
1. Items Found During the Execution of the Writ	189
2. Davis' Deposition in the Civil Case	190
3. The Criminal Case	191
B. Case 2—Mel Howard	194
1. Comparing the History/Log File Data	194
2. Gaps in the Evidence	197
3. Determining Damages	198
4. Resolution	198
C. Case 3—Allen Worley	199
VI. Conclusion	200
Chapter Four • Defending Cybercrime Cases: Selected Statutes and Defenses	 201
<i>Joseph F. Savage, Jr. and David Goldstone</i>	
I. Introduction	201
II. Category 1: Unauthorized Access	202
A. Computer Fraud and Abuse Act	203
1. Section 1030(a)(5)	205
2. Section 1030(a)(2)	209
3. Section 1030(a)(7)	210
4. Section 1030(a)(6)	211
5. Section 1030(a)(4)	211
6. Section 1030(a)(3)	213
7. Section 1030(a)(1)	213
B. Electronic Communications Privacy Act	214
1. The Wiretap Statute	214

2.	Stored Wire and Electronic Communications Act	216
III.	Category 2: Cyberfraud	217
A.	Identity Theft	217
B.	CAN-SPAM Act	220
IV.	Category 3: Intellectual Property Crimes	221
A.	The Economic Espionage Act	221
1.	Overview of the Statute	221
2.	Constitutional Challenges to the Economic Espionage Act	223
3.	Wide Expansion of Trade Secret Prosecution	224
4.	Defending Against Liability Under the EEA	225
B.	The Copyright Act	229
1.	Criminal Copyright Infringement and the NET Act	229
2.	The PRO-IP Act of 2008	230
3.	Defenses to Criminal Copyright Infringement	231
4.	Pseudo-Copyright Infringement	235
5.	Digital Millennium Copyright Act's Anti-Circumvention Provisions	237
V.	General Defenses to Cybercrime Allegations	239
A.	Search and Seizure Issues	239
1.	Introduction	239
2.	Federal Statutory Protection	239
3.	The Fourth Amendment	243
B.	Other Defenses	253
1.	Identification	253
2.	First Amendment as a Defense to Computer Crime	254
3.	Entrapment	255
VI.	Conclusion	256
 Chapter Five • International Cybercrime: Recent Developments in the Law		 257
<i>Miriam F. Weismann</i>		
I.	Introduction	258
II.	In Search of a Definition	258
III.	Historical Development of International Law	260
IV.	Practical Impediments to International Investigation and Enforcement	263
V.	The Council of Europe Convention on Cybercrime	266
A.	General Principles	266
B.	Summary of Treaty Provisions	268
C.	Application and Analysis of Significant Treaty Provisions	270

1. Four Basic Definitions	270
2. Procedural Safeguards	272
3. Methods of Collecting Evidence	273
4. Crimes	277
5. Jurisdiction and Extradition	278
VI. Mutual Legal Assistance Treaties (MLATs) and Other International Cooperation Agreements	281
VII. The PATRIOT Act and Other Federal Legislation	285
VIII. Continuing Policy Review by the United Nations	287
IX. The Threat of Global Organized Crime	288
X. The Problem of Enforcement Between Differing Legal Systems	292
XI. Conclusion	294
Index	295