Cybercrime
Cybercrime

The Investigation, Prosecution and Defense of a Computer-Related Crime

Edited by

Ralph D. Clifford
Professor, Southern New England School of Law

Carolina Academic Press
Durham, North Carolina
Chapter One  Introduction
   Ralph D. Clifford

Chapter Two  Defining Cybercrime:  
   A Review of State and Federal Law
   Susan W. Brenner

I. Introduction  11
II. Cybercrimes: New Crimes or Old Wine in New Bottles? 12
III. Federal Cybercrime Legislation 16
   A. Copyright Infringement  18
   B. Trademarks and Trade Secrets  29
   C. Hacking, Cracking, Fraud, Virus Dissemination 
      and Extortion 32
   D. Mail Fraud and Wire Fraud  39
   E. Sexual Exploitation of Children  42
   F. Transporting Stolen Property  49
   G. Unauthorized Access to Stored Electronic 
      Communications 49
   H. Sending Obscene, Abusive or Harassing 
      Communications 50
   I. Sending Offensive Material to Minors 51
   J. Sending Commercial Communications Containing 
      Material Harmful to Minors 53
   K. Transmitting Information about a Minor  55
   L. Online Stalking, Harassment and Threats 55
   M. Fraud in Connection with Access Devices  58
Chapter Three  
The Investigation and Prosecution of a Cybercrime

Ivan Orton

I. Introduction
II. Acquisition of Evidence
   A. What Crimes?
   B. What Computers?
   C. Legal Limits on Searches
      1. Constitutional Limits
         a. Does the Fourth Amendment Apply to the Situation?
            (1) Is There a Reasonable Expectation of Privacy?
            (2) Is Government Action Involved?
               (a) Searches by Non-forum, State Law Enforcement
               (b) Searches by Private Citizens
         b. Is There a Legal Warrant?
            (1) The Application for the Warrant Must Demonstrate Probable Cause to Believe That Evidence of a Crime Will Be Found in the Place to Be Searched
               (a) Evidence of a Crime
               (b) Will Be Found in the Place to Be Searched
            (2) Signed by a Neutral and Detached Magistrate
            (3) Reasonably Precise in Describing the Place to Be Searched and the Items to Be Seized
Contents

(4) Knock and Announce 81

c. Take Items in Plain View 82
d. Good Faith 82
e. Take Computers off Premises to Search 83
f. Prompt Execution 83

2. If There Is Not a Legal Warrant Does the Search Fall Within the Exceptions to the Warrant Requirement? 83
a. Consent 84
   (1) Who May Consent? 84
      (a) Employer 85
      (b) Parent 86
      (c) Spouse 86
      (d) Co-user 86
   (2) Must the Consentor Be Advised of His/Her Right to Withhold Consent 87
   (3) Consent May Be Limited and May Be Withdrawn 88
b. Search Incident to Arrest 88
c. Exigent Circumstances 89
d. Inventory 90
e. Stop and Frisk 90
f. Mobility 90
g. Plain View 91

3. State Constitutional Considerations 92
D. Statutes 92
   1. Privacy Protection Act 92
      a. Suppression 94
      b. Civil liability 95
      c. Good Faith 95
   2. Electronic Communications Privacy Act 96
      a. What Does the ECPA Cover? 96
      b. What Does the ECPA Prohibit? 96
      c. When Is a Disclosure to the Government Allowed? 96
         (1) Subscriber or Customer Records 96
(2) Contents of Electronic Communications 97

d. What Is the Remedy for Violation of this Act? 97
   (1) Criminal Liability 97
   (2) Civil Liability 97
   (3) Suppression 98
   (4) Good Faith 98

E. Court Rules and Magistrate Imposed Restrictions 98
   1. Court Rules — Time Within Which Search Must Be Completed 98
   2. Magistrate Imposed Restrictions 99

III. Analysis of Evidence 100
   A. At the Search Location 100
      1. Who Should Accompany the Officers Executing the Search? 100
         a. Should an Expert Accompany the Officers? 100
         b. Should a Representative of the Victim Accompany the Officers? But What If the Only Expert Is a Representative of the Victim? 101
      2. What Can Be Seized 103
      3. When to Get an Additional Warrant 104
   B. Offsite/Detailed Analysis 105
      1. Accurate Pristine Mirror 105
      2. Analysis Protocol 106
      3. What Must Be Returned and When 107
         a. Stipulation 108
         b. What If the Computer Owner Is Not the Suspect? 108
         c. Contraband on Computer 109
            (1) Obvious Contraband 109
            (2) Suspected Stolen Property — No Irreversible Harm in Returning 109
            (3) Suspected Stolen Property — Irreversible Harm in Returning 109
            (4) Other Types of Contraband — Passwords, Hacking Programs 110

IV. Presentation of Evidence at Trial 110
   A. Computer Printouts and Summaries 110
Chapter Four  Defending Cybercrime Cases:  
Selected Statutes and Defenses  
Joseph F. Savage, Jr. with Amanda J. Metts and Darlene DeMelo  

I. Computer Related Offenses in the New Economy  
A. Introduction  
B. The Computer Fraud and Abuse Act  
1. Substantive Prohibitions  
2. Defenses  
   a. Jurisdiction  
   b. Intent  
   c. “Obtain Anything of Value”  
3. Lack of “Damage” Under the CFAA  
4. Penalties  
C. The Electronic Communications Privacy Act of 1986  
1. The Wiretap Statute — § 2511  
2. SWECTRA — § 2701  
D. The Economic Espionage Act  
1. Overview of the Statute
2. The Wide Expansion of Trade Secret Prosecution 137
3. Defending Against Liability Under the EEA 138
   a. The Prosecutors’ Perspective on Defenses 139
      (1) Parallel Development 139
      (2) Reverse Engineering 139
      (3) General Knowledge 140
      (4) The First Amendment 140
   b. Practical Conclusions 141
E. The Copyright Act 142
   1. Criminal Copyright Infringement and the NET Act 142
   2. Defenses to Criminal Copyright Infringement 144
      a. Invalidate the Copyright 144
      b. No Infringement 144
      c. First Sale Doctrine 145
      d. Fair Use Doctrine 145
      e. Willfulness: The Use Was Authorized 146
      f. Copyright Misuse 147
   3. Pseudo-Copyright Infringement 148
      a. Trafficking in Counterfeit Labels or Computer Program Documentation or Packaging 148
      b. Unauthorized Fixation of and Trafficking in Sound Recordings and Music Videos of Live Performance 149
      c. Digital Millennium Copyright Act 149
      d. Fraudulent Copyright Notice and Removal of Such Notices 150
      e. False Representation in Application to Register Copyright 150
II. General Defenses to Cybercrime Allegations 151
   A. Search and Seizure Issues 151
      1. Introduction 151
      2. Federal Statutory Protection 151
         a. The ECPA — Interception of Electronic Communication 152
         b. SWECTRA — Accessing Stored Electronic Communications 152
## Contents

3. The Fourth Amendment 153  
   a. Scope of Searches 154  
   b. Intermingled Documents 155  
   c. Plain View Doctrine 156  
   d. Consent Searches 157  
   e. Privilege 158  

B. Other Defenses 159  
   1. Anonymity 159  
   2. First Amendment as a Defense to Computer Crime 160  
   3. Entrapment 161  

III. Conclusion 162

---

### Chapter Five  International Aspects of Cybercrime  

*Jessica R. Herrera*  

I. Introduction 165  

II. What is Computer Crime? 167  

III. The Challenges of Cybercrime 169  
   A. Technical Challenges 170  
   B. Meaningfully Enforcing National Laws 173  
      1. Differing Definitions of Cybercrimes 173  
      2. Differing Procedural Hurdles 175  
   C. Operational Challenges 178  

IV. Leadership and Education in the Private Sector 179  

V. International Multilateral Efforts 182  
   A. Organisation for Economic Cooperation and Development 182  
   B. The Group of Eight Nations 182  
   C. Council of Europe 185  
      1. Substantive Laws 186  
      2. Procedural Laws 187  
      3. International Cooperation 187  
   D. United Nations 188  
   E. European Union 189  

VI. Conclusion 189  

Index 191