CYBERCRIME & SECURITY

Cybercrime & Security

Compiled & Edited by
Pauline C. Reich

Volume 1

WEST®
A Thomson Reuters business

For Customer Assistance Call 1-800-328-4880

Mat #41260170

Table of Contents

Volume 1

PART I. CYBERCRIME

CHAPTER 1. INVESTIGATIONS AND FORENSICS

§ 1:1 Hard To Hide on Computer Hard Drives
§ 1:2 Legal Limitations on Cross-border Data Transfers in Cybercrime Investigations

CHAPTER 2. FORENSICS AND ELECTRONIC EVIDENCE

§ 2:1 Knowledge of Computer Forensics is Becoming Essential for Attorneys in the Information Age
§ 2:2 Presenting IT Evidence in the Courtroom
§ 2:3 Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police Officers of England, Wales and Northern Ireland
§ 2:4 Forensic Examination of Digital Evidence: A Guide for Law Enforcement
§ 2:5 Collecting Evidence From a Running Computer: A Technical and Legal Primer for the Justice Community
§ 2:6 Duty Everlasting: The Perils of Applying Traditional Doctrines of Spoliation to Electronic Discovery
§ 2:7 The Admissibility of Electronic Evidence in European Courts: Fighting Technology Crime

CHAPTER 3. ADVANCE FEE FRAUD

§ 3:1 Advance Fee Fraud Scams In-Country and Across Borders
§ 3:2 Advance Fee Fraud Statistics 2009
§ 3:3 Advance Fee Fraud Statistics 2009: Charts

CHAPTER 4. RECENT DEVELOPMENTS AND EMERGING TRENDS IN COMPUTER CRIME

§ 4:1 Cyberbullying, Internet, Suicide, and Legal Responses
§ 4:2 HPM and EMP: The Least-discussed Cyber Threat
§ 4:3 Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare

CHAPTER 4A. ONLINE GAMBLING, CYBERCRIME AND MONEY LAUNDERING ISSUES IN SELECTED JURISDICTIONS

§ 4A:1 Introduction
§ 4A:2 Background—International Perspective
§ 4A:3 U.S. Entities Involved in Regulating/Monitoring Online Gambling
§ 4A:4 Payment Intermediaries and Liability for Processing Online Gambling Transactions
§ 4A:5 2011—UIGEA Indictments—"Black Friday"
§ 4A:6 U.S.—Money Processor Rules—Paypal
§ 4A:7 Non-U.S. Cases
§ 4A:8 Attempts to Amend UIGEA and Theories of Amendments
§ 4A:9 Possible Legalization in District of Columbia
§ 4A:10 United States View of Illegality of Online Gambling and Lack of Clear Definition
§ 4A:11 Legislation in Other Jurisdictions Worldwide Permitting and Prohibiting Various Types of Online Gambling
§ 4A:12 Three Types of Jurisdictions
§ 4A:13 Jurisdictions Permitting Online Gambling
§ 4A:14 Overview of Legality
§ 4A:15 Legal Semantics and Jurisdictional Complexities
§ 4A:16 One Proposed Definition
§ 4A:17 Games of Chance vs. Games of Skill
§ 4A:18 Distinction Between Online Gaming and Online Gambling
§ 4A:19 Jurisdictions Prohibiting Online Gambling
§ 4A:20 Indictments and Convictions in Jurisdictions Where Online Gambling/Gaming Is Illegal
§ 4A:21 Jurisdictions in Which Online Gambling Is Legal
§ 4A:22 Virtual Reality Gambling/Gaming and Conversion of Currency from Virtual World to Real World Form
§ 4A:23 Republic of Korea
§ 4A:24 Conclusion

Appendix 4A-1. United States Federal Legislation Applied to Online Gambling Cases Cited in This Chapter
Appendix 4A-2. Existing United States State Legislation Applied to Online Gambling Cases Cited in this Chapter Either Alone or in Combination with Federal Legislation
Appendix 4A-3. Table of Selected Cases Cited and U.S. Laws Applied to Online Gambling Prosecutions
Appendix 4A-4. Campos—Motion to Dismiss Federal Indictment
Appendix 4A-5. Gold Medal Sports—DOJ Press-Release—Internet Sports Bookmakers Plead Guilty
Appendix 4A-6. E-Gold Ltd.—Federal Seizure Warrant Vacated
Appendix 4A-7. K23Group—Indictment—Online Gambling

Appendix 4A-8. Rennick—Federal Indictment—Online Gambling and Asset Forefeiture

Appendix 4A-9. U.S. v. Scheinberg—DOJ Press Release—Internet Gambling Indictment and Civil Money Laundering and Forfeiture

Appendix 4A-10. U.S. v. Scheinberg—Federal Superseding Indictment—Online Gambling

Appendix 4A-11. U.S. v. Thrillx Systems—Federal Indictment—Online Gambling

Appendix 4A-12. Tzvetkoff—Federal Indictment—Online Gambling, Bank Fraud, Money Laundering, and Asset Forfeiture

Appendix 4A-13. U.S. v. Pokerstars—DOJ Memorandum to Amend Complaint—Civil Money Laundering Claims

Appendix 4A-14. U.S v. Pokerstars—Amended Civil Complaint—Forefeiture and Money Laundering

Appendix 4A-15. Allied Wallet Online Payment Processors—DOJ Press Release

Appendix 4A-16. Kennedy v. Full Tilt Poker—Expedited Discovery Denied

Appendix 4A-17. Interactive Media & Gaming—District Court Dismissal of Challenge to Professional and Amateur Sports Protection Act

Appendix 4A-18. Kennedy v. Full Tilt Poker—Voluntary Dismissal Civil RICO

Appendix 4A-19. Interactive Media & Gaming—Third Circuit Upholds Unlawful Internet Gambling Enforcement Act

Appendix 4A-20. U.S. v. Cohen—Appeal of Conviction for Conspiracy to Transmit Bets in Foreign Commerce

Appendix 4A-21. DOJ US Attorney Hanaway's Congressional Statement re Internet Gambling

Appendix 4A-22. DOJ Memo re Wire Act's Applicability to Internet Sale of State Lottery Tickets Out of State

Appendix 4A-23. People ex rel Vaco v. World Interactive Gaming—Injunction Action Against Online Gambling

Appendix 4A-24. Rousso v. Washington—Online Gambling Ban Upheld

Appendix 4A-25. Internet Community v. Washington State Gambling Commission

Appendix 4A-26. WTO Paypal GATS Challenge to U.S. Measures Affecting Cross-Border Supply of Gambling Materials

Appendix 4A-27. Validity and Construction of Federal Statute (18 U.S.C.A. § 1084(a)) Making Transmission of Wagering Information a Criminal Offense, 5 ALR Fed 166

PART II. CYBER SECURITY

CHAPTER 5. INTERNET SECURITY

§ 5:1 Terrorism and the Internet: A Review of the History, Issues, and Responses
§ 5:2 The U.S. Cyber-security Check List
§ 5:3 Guidelines on Firewalls and Firewall Policy
§ 5:4 2009 Annual Study: U.S. Enterprise Encryption Trends by the Ponemon Institute

CHAPTER 6. INTERNATIONAL AND TRANSNATIONAL APPROACHES TO CYBER SECURITY

A. INTERNATIONAL ORGANIZATIONS

§ 6:1 OECD-1 Guidelines for Cryptography Policy
§ 6:2 OECD-3 Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures
§ 6:3 OECD-4 The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries
§ 6:4 OECD-5 Scoping Paper on Online Identity Theft, Ministerial Background Report
§ 6:5 OECD-6 The Financial Action Task Force: Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems, June 18, 2008
§ 6:6 OECD-7 The Financial Action Task Force: Report on New Payment Methods, October 13, 2006
§ 6:7 UN-1 UN-CTITF, Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes
§ 6:8 WTO-1 Antigua v. United States

B. COUNCIL OF EUROPE; EUROPEAN UNION; EUROPEAN COMMISSION

§ 6:9 Council of Europe-1.5 Convention on Cybercrime (Adopted by the Council of Europe at Budapest on 23 November 2001)
§ 6:10 Council of Europe-2 Additional Protocol to the Convention on Cybercrime concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (Strasbourg, 7 November 2002)
§ 6:11 Council of Europe-8 Council of Europe Additional Protocol to the Convention on Cybercrime Explanatory Report
§ 6:12 Council of Europe-9 Convention on Cybercrime Explanatory Report, 109th Session, 8 November 2001
§ 6:13 Council of Europe-10 The Guidelines for the Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime

§ 6:14 European Union-1 European Network and Information Security Agency: Security Issues and Recommendations for Online Social Networks
§ 6:15 European Union-2 European Network and Information Security Agency: Botnets-The Silent Threat
§ 6:16 European Union-7 Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications
§ 6:17 European Union-11 Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems
§ 6:18 European Union-13 European Network and Information Security Agency (ENISA): A Step-By-Step Approach on How to Set Up a CSIRT

Volume 2

CHAPTER 7. NATIONAL LEGISLATION AND COMMENTARY—AFRICAN COUNTRIES

§ 7:1 Morocco: Council of Europe Project on Cybercrime: Cybercrime Legislation: Morocco Profile

CHAPTER 8. NATIONAL LEGISLATION AND COMMENTARY—ASIA

§ 8:1 Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws
§ 8:2 China: Cybercrime and Relevant Legislation in China
§ 8:3 India: Data Security Council of India Recommendations: Making of Rules Under Sections 43A, 67C and 79 of the Information Technology Act
§ 8:4 India: The Information Technology Act, 2000
§ 8:5 India: The Information Technology (Amendment) Act, 2008
§ 8:6 Indonesia: Indonesia's Cyber Security Environment; VeriSign-iDefense Global Threat Research Report
§ 8:7 Japan: Cybercrime Legislation and Cases in Japan: Update
§ 8:8 Japan: National Information Security 2009
§ 8:9 Japan: Unauthorized Computer Access Law
§ 8:10 Korea: The Present Situation and Legal Countermeasures against Cybercrime in the Republic of Korea
§ 8:11 Korea: Countermeasures to Cyber Attacks in Korea
§ 8:12 Malaysia: Laws Related to Computer Crimes in Malaysia
§ 8:13 Singapore: Cyber Security in Singapore
§ 8:14 Singapore: Singapore Computer Misuse Act
§ 8:15 Singapore: Electronic Transactions Act
§ 8:16 Singapore: Spam Control Act
§ 8:17 Singapore: Evidence Act, excerpt sections 35 and 36
§ 8:18 Singapore: Criminal Procedure Code, excerpt sections 125A and 125B

§ 8:19 Sri Lanka: Computer Crime Act and Implementation Order, 2008
§ 8:20 Taiwan: The Introduction of the Guidelines for Government Agencies Information Outsourcing Security
§ 8:21 Taiwan: Securing Taiwan's Cyberspace: An Overview of the Legal and Regulatory Framework for Countering Cybercrime in Taiwan
§ 8:22 Thailand: Analysis of Computer Crime Act of Thailand
§ 8:23 Thailand: Computer Crime Act, 2007

CHAPTER 9. NATIONAL LEGISLATION AND COMMENTARY—EUROPEAN COUNTRIES

§ 9:1 Austria Council of Europe Project on Cybercrime: Cybercrime Legislation: Austria Profi le
§ 9:2 Estonia: Cyber Security Strategy
§ 9:3 France: Council of Europe Project on Cybercrime: Cybercrime LegislationFrance Profile
§ 9:4 Germany: The Development of Legislation Related to the Criminal Liability of Internet Service Providers in Germany
§ 9:5 Germany: Council of Europe Project on Cybercrime: Cybercrime Legislation: Germany Profile
§ 9:6 Ireland: Cybercrime in Ireland
§ 9:7 Italy: An Overview of the Substantive and Procedural Legal and Regulatory Framework for Countering Cybercrime in Italy after the Council of Europe Cybercrime Convention
§ 9:8 Italy: A-2 Internet Service Providers Liability Cases and Online Gambling Law
§ 9:9 Netherlands: Cybercrime Legislation in the Netherlands
§ 9:10 Russia: State and Trends of the Russian Computer Crime Market in 2010
§ 9:11 United Kingdom Computer Misuse Act 1990 (c.18)
§ 9:12 United Kingdom Computer Misuse Act 1990 (Amendment) Bill
§ 9:13 United Kingdom Police and Justice Bill Excerpt
§ 9:14 United Kingdom: Cybercrime in the United Kingdom

CHAPTER 10. NATIONAL LEGISLATION AND COMMENTARY—LATIN AMERICAN COUNTRIES

§ 10:1 Brazil: Council of Europe Project on Cybercrime: Cybercrime Legislation; Brazil Profile
§ 10:2 Brazil: The Cyber Threat Landscape in Brazil
§ 10:3 Mexico: Cybercrime Legislation and Security Enforcement in Mexico

Volume 3

CHAPTER 11. NATIONAL LEGISLATION AND COMMENTARY—MIDDLE EASTERN COUNTRIES

§ 11:1 Saudi Arabia: The Cyber Threat Landscape of Saudi Arabia; VeriSigniDefense Global Threat Research Report

§ 11:2 Turkey: Council of Europe Project on Cybercrime: Cybercrime Legislation: Turkey Profile

CHAPTER 12. NATIONAL LEGISLATION AND COMMENTARY—AUSTRALIA

§ 12:1 Australia: Cyber Security Strategy

CHAPTER 13. NATIONAL LEGISLATION AND COMMENTARY—NORTH AMERICAN COUNTRIES

I. COMMENTARY

§ 13:1 United States: Nation at Risk: Policy Makers Need Better Information to Protect the Country, March 2009

§ 13:2 United States: Faking It: Calculating Loss in Computer Crime Sentencing

§ 13:3 United States: Cybercrime Law and Policy in the United States

§ 13:4 United States: An Overview of Significant U.S. Data Breach Cases and Enforcement Actions by Susan L. Lyon (issued 3/10)

§ 13:5 United States: Collaboration: The Key To The Privacy and Security Balancing Act

II. REPORTS

§ 13:6 United States: Securing Cyberspace for the 44th Presidency, Center for Strategic and International Studies

§ 13:7 United States: Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure

§ 13:8 United States: Cybersecurity Collaboration Report, May 21, 2009

§ 13:9 Department of Defense Strategy for Operating in Cyberspace

§ 13:10 United States: The Comprehensive National Cybersecurity Initiative

§ 13:11 United States National Strategy for Trusted Identification in Cyberspace-Enhancing Online Choice, Efficiency, Security and Privacy

§ 13:12 United States International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World

III. LEGISLATION

§ 13:13 United States: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)
§ 13:14 United States: Cyber Security Enhancement Act of 2002 [Pub. L. 107-296, Title II, Sec. 225, Jan. 23, 2002]
§ 13:15 United States: Federal Information Security Management Act of 2002 [Pub. L. 107-347, Title III, December 12, 2002]
§ 13:16 United States: Security Breach Notification Chart
§ 13:17 United States: Unlawful Internet Gambling Enforcement Act of 2006 Overview
§ 13:18 White House Cybersecurity Legislative Proposal (May, 2011)

IV. RULES AND REGULATIONS

§ 13:19 United States: Federal Reserve System; Department of the Treasury, Prohibition on Funding of Unlawful Internet Gambling, [31 CFR Part 132, effective January 19, 2009]

CHAPTER 14. INDUSTRY CASE STUDIES

§ 14:1 Technology Risk Management Guidelines for Financial Institutions, Monetary Authority of Singapore
§ 14:2 Internet Banking Technology Risk Management Guidelines, Monetary Authority of Singapore

CHAPTER 15. JUDICIAL CASES AND INDICTMENTS

A. UNITED STATES

1. INTERNET GAMBLING

§ 15:1 Seidl v. American Century Companies, Inc., Dist. Court, SD New York 2010
§ 15:2 United States v. $6,976,934.65, Held in Name of Soulbury, 554 F.3d 123
§ 15:3 Wong v. Partygaming Ltd., Dist. Court, ND Ohio, Eastern Div. 2008
§ 15:4 Cheyenne Sales, Ltd. v. Western Union Financial Services International (E.D. Penn. 1998)
§ 15:5 McBrearty v. The Vanguard Group, Inc., Dist. Court, SD New York 2009
§ 15:6 US v. $734,578.82 in USD; $589,578.82 in USD, American Sports, Ltd.; Intercash Ltd. IOM
§ 15:7 WTO: US v. Ehlermann: Measures Affecting the Cross-border Supply of Gambling and Betting Services

2. CHILD PORNOGRAPHY

§ 15:8 US v. Perez, 247 F. Supp. 2d 459, Dist. Court, SD New York 2003

§ 15:9 US v. Strauser, 247 F. Supp. 2d 1135, Dist. Court, ED Missouri, Eastern Div. 2003
§ 15:10 US v. Paroline, 672 F. Supp. 2d 781, Dist. Court, ED Texas, Tyler Div. 2009
§ 15:11 US v. Robert A. Warren
§ 15:12 Ashcroft, Attorney General, et al. v. Free Speech Coalition et al
§ 15:13 US v. Steiger
§ 15:14 US v. Hall

3. HACKING/NATIONAL SECURITY

§ 15:15 United States of America v. Gary McKinnon (D.N.J., December 11, 2002)
§ 15:16 Creative Computing, dba Internet Truckstop.com v. Getloaded.com LLC, and/or Codified Corporation and Jack C. Martin Dist. Court, Idaho, 2004
§ 15:17 US v. Daniel Spitler criminal complaint
§ 15:18 US v. Auernheimer indictment

4. DOWNLOADING/PEER-TO-PEER

§ 15:19 Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 US 913 Supreme Court 2005
§ 15:20 NinjaVideo.Net indictment

5. SPAM

§ 15:21 Verizon Online Services, Inc. v. Ralsky, 203 F. Supp. 2d 601, Dist. Court, ED Virginia, Alexandria Div. 2002
§ 15:22 Beyond Systems, Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, Dist. Court, D. Maryland 2006
§ 15:23 USSEC v. Meltzer, 440 F. Supp. 2d 179, Dist. Court, ED New York 2006

6. ONLINE PAYMENTS

§ 15:24 Grimm v. First National Bank of Pennsylvania v. Chase Bank USA, NA, 2008
§ 15:25 Grimm v. Discover Financial Services v. Bank of America, Civil Actions Nos. 08-747, 08-832, related (W.D. Mass. 2008)

7. SOLICITATION OF MINORS

§ 15:26 US v. Brian E. Gladish
§ 15:27 US v. John T. Spurlock
§ 15:28 US v. Jeffrey Tucker

8. IDENTITY THEFT; PHISHING

§ 15:29 United States of America v. Andrew Manovani, et al (D.N.J. October 8, 2004)

§ 15:30 SEC v. Marimuthu, 552 F. Supp. 2d 969, Dist. Court, D. Nebraska 2008
§ 15:31 Experi-Metal vs. Comercial Bank

9. INTERCEPTION OF ELECTRONIC COMMUNICATIONS

§ 15:32 US v. Szymuszkiewicz
§ 15:33 US v. Councilman
§ 15:34 US v. Farey-Jones

10. ONLINE PORNOGRAPHY (ADULT)

§ 15:35 US v. Thomas

11. SEARCH AND SEIZURE

§ 15:36 Guest v. Leis
§ 15:37 Steve Jackson Games Inc. v. US Secret Service

12. ANONYMITY; BOTNETS

§ 15:38 Coreflood International Botnet—DOJ Press Release
§ 15:39 Coreflood—DOJ Civil Complaint
§ 15:40 —Summons
§ 15:41 —Order To Show Cause
§ 15:42 —Preliminary Injunction
§ 15:43 —Notice of Proceedings To Modify Preliminary Injunction
§ 15:44 —Order for Default Judgment
§ 15:45 —Default Judgment

Summary of Contents

Volume 1

PART I. CYBERCRIME

Chapter 1. Investigations and Forensics

Chapter 2. Forensics and Electronic Evidence

Chapter 3. Advance Fee Fraud

Chapter 4. Recent Developments and Emerging Trends in Computer Crime

Chapter 4A. Online Gambling, Cybercrime and Money Laundering Issues in Selected Jurisdictions

Appendix 4A-1. United States Federal Legislation Applied to Online Gambling Cases Cited in This Chapter

Appendix 4A-2. Existing United States State Legislation Applied to Online Gambling Cases Cited in this Chapter Either Alone or in Combination with Federal Legislation

Appendix 4A-3. Table of Selected Cases Cited and U.S. Laws Applied to Online Gambling Prosecutions

Appendix 4A-4. Campos—Motion to Dismiss Federal Indictment

Appendix 4A-5. Gold Medal Sports—DOJ Press-Release—Internet Sports Bookmakers Plead Guilty

Appendix 4A-6. E-Gold Ltd.—Federal Seizure Warrant Vacated

Appendix 4A-7. K23Group—Indictment—Online Gambling

Appendix 4A-8. Rennick—Federal Indictment—Online Gambling and Asset Forefeiture

Appendix 4A-9. U.S. v. Scheinberg—DOJ Press Release—Internet Gambling Indictment and Civil Money Laundering and Forfeiture

Appendix 4A-10. U.S. v. Scheinberg—Federal Superseding Indictment—Online Gambling

Appendix 4A-11. U.S. v. Thrillx Systems—Federal Indictment—Online Gambling

Appendix 4A-12. Tzvetkoff—Federal Indictment—Online Gambling, Bank Fraud, Money Laundering, and Asset Forfeiture

Appendix 4A-13. U.S. v. Pokerstars—DOJ Memorandum to Amend Complaint—Civil Money Laundering Claims

Appendix 4A-14. U.S v. Pokerstars—Amended Civil Complaint—Forefeiture and Money Laundering

Appendix 4A-15. Allied Wallet Online Payment Processors—DOJ Press Release

Appendix 4A-16. Kennedy v. Full Tilt Poker—Expedited Discovery Denied

Appendix 4A-17. Interactive Media & Gaming—District Court Dismissal of Challenge to Professional and Amateur Sports Protection Act

Appendix 4A-18. Kennedy v. Full Tilt Poker—Voluntary Dismissal Civil RICO

Appendix 4A-19. Interactive Media & Gaming—Third Circuit Upholds Unlawful Internet Gambling Enforcement Act

Appendix 4A-20. U.S. v. Cohen—Appeal of Conviction for Conspiracy to Transmit Bets in Foreign Commerce

Appendix 4A-21. DOJ US Attorney Hanaway's Congressional Statement re Internet Gambling

Appendix 4A-22. DOJ Memo re Wire Act's Applicability to Internet Sale of State Lottery Tickets Out of State

Appendix 4A-23. People ex rel Vaco v. World Interactive Gaming—Injunction Action Against Online Gambling

Appendix 4A-24. Rousso v. Washington—Online Gambling Ban Upheld

Appendix 4A-25. Internet Community v. Washington State Gambling Commission

Appendix 4A-26. WTO Paypal GATS Challenge to U.S. Measures Affecting Cross-Border Supply of Gambling Materials

Appendix 4A-27. Validity and Construction of Federal Statute (18 U.S.C.A. § 1084(a)) Making Transmission of Wagering Information a Criminal Offense, 5 ALR Fed 166

PART II. CYBER SECURITY

Chapter 5. Internet Security

Chapter 6. International and Transnational Approaches to Cyber Security

Volume 2

PART II. CYBER SECURITY (CONTINUED)

Chapter 7. National Legislation and Commentary—African Countries

Chapter 8. National Legislation and Commentary—Asia

Chapter 9. National Legislation and Commentary—European Countries

Chapter 10. National Legislation and Commentary—Latin American Countries

Volume 3

PART II. CYBER SECURITY (CONTINUED)

Chapter 11. National Legislation and Commentary—Middle Eastern Countries

Chapter 12. National Legislation and Commentary—Australia

Chapter 13. National Legislation and Commentary—North American Countries

Chapter 14. Industry Case Studies

Chapter 15. Judicial Cases and Indictments

Part I

CYBERCRIME

Chapter 1

Investigations & Forensics

§ 1:1 Hard to hide on computer hard drives
§ 1:2 Legal limitations on cross-border data transfers in cybercrime investigations

§ 1:1 Hard to hide on computer hard drives*

The knock on the door interrupted her morning coffee, but annoyance turned to shock when the suburban mom was confronted by two FBI agents. They were there to investigate the trafficking of child pornography by a computer user in the house. The culprit was the fourteen-year old son, who had been exploring erotica online in the privacy of his bedroom. Contained in files he downloaded over a peer-to-peer file sharing network were child pornography images.

Unbeknownst to the teenager, the peer-to-peer file sharing program he had downloaded on his computer to search for and retrieve files for free, had automatically become a "supernode." In effect, his computer had been activated to serve as a network hub, holding part of the massive searchable list of available files for freeloading within the network. As a result, the peering program was beaming around the globe to other network users an invitation to download files stored on

---

[Section 1:1]

*By **Beryl A. Howell** and **Eric Friedberg**.

Beryl A. Howell is the Managing Director of the Washington DC office and Eric Friedberg is the Executive Vice President at Stroz Friedberg, LLC, www.strozllc.com, a consulting and technical services firm with offices in New York City, Washington, D.C., and Minneapolis. Both Ms. Howell and Mr. Friedberg are former Assistant U.S. Attorneys in the U.S. Attorney's Office for the Eastern District of New York. Thanks to Mike McGowan for his assistance.

the computer, with all of the civil and criminal liability that attaches for distributing child pornography. The stunned parents turned to expert computer forensic examiners to help put the teenager's conduct in context and explain to law enforcement investigators how many child porn images were distributed as a result of a direct action by the teenager versus uploading activities by other users on the network.

Whether the conduct being investigated is a network intrusion, denial of service attack, theft of intellectual property, child pornography or other kind of criminal, malicious or tortious activity, electronic data stored on computers, including desktop and laptop machines, servers, personal digital assistants (PDAs), and Blackberries may provide a gold mine of evidence that can shed light on a suspect's past activities, future plans and state of mind. This evidence may be highly probative of guilt or exculpatory.

Given the ubiquitous use of and reliance on computers by companies and individuals to communicate, transact business, find information, and be entertained, investigators and lawyers should have sufficient familiarity with the kinds of evidence that may be found on desktop computers and removable media not only to make use of that evidence, but also to anticipate its defensive use. In the case of the teenage son, forensic examination was able to show that the significant distribution of child pornography from the son's computer was the result of uploading activity by other users—often occurring when the son was not even present—and he avoided prosecution.

The focus here is on the types of information that may be forensically recovered from computer hard drives, but other components of a network, such as the file, e-mail and web servers, printers and other peripherals, and Internet Service Providers used to connect a computer or network to the Internet, also hold information on use of the computer that may be relevant to an investigation or litigation.

The nature of the investigation at hand helps guide the types of electronic data for which the forensic examiner will look. In child pornography cases, investigators will want to look for graphic images on the suspect's computer, determine with whom the suspect was communicating and trading images and which web sites the suspect visited to obtain images. In intellectual property theft cases, investigators may want to compare hash values of the stolen digital property to see if it appears on the suspect's computer and, if so, determine when and how the suspect obtained or transferred the property, whether to or from removable media, such as CDs or floppy disks, or over a network. In cases involving physical violence, stalking or harassment, investigators will want to determine whether the suspect's computer contained addresses or other personal information about the victim and how and when the suspect obtained the information. The victim's computer also may hold clues to the origination point of the perpetrator's e-mail messages.

No matter the type of conduct at issue, the starting point is the