

# The Law of Cybercrimes and Their Investigations



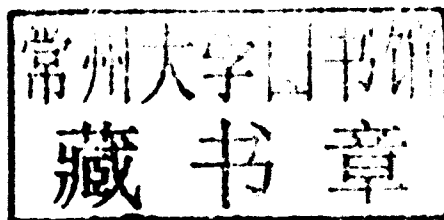
George Curtis

 CRC Press  
Taylor & Francis Group

# The Law of Cybercrimes and Their Investigations

---

George Curtis



**CRC Press**

Taylor & Francis Group

Boca Raton London New York

---

CRC Press is an imprint of the  
Taylor & Francis Group, an **Informa** business

CRC Press  
Taylor & Francis Group  
6000 Broken Sound Parkway NW, Suite 300  
Boca Raton, FL 33487-2742

© 2012 by Taylor & Francis Group, LLC  
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed in Great Britain on acid-free paper  
Version Date: 20110613

International Standard Book Number: 978-1-4398-5831-8 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access [www.copyright.com](http://www.copyright.com) (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

**Trademark Notice:** Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

---

**Library of Congress Cataloging-in-Publication Data**

---

Curtis, George E., 1942-  
The law of cybercrimes and their investigations / George Curtis.  
p. cm.  
Includes bibliographical references and index.  
ISBN 978-1-4398-5831-8 (hardback)  
1. Computer crimes--United States. 2. Computer crimes--Investigation--United States. I. Title.

KF9350.C87 2011  
345.73'0268--dc22

2011005128

---

Visit the Taylor & Francis Web site at  
<http://www.taylorandfrancis.com>

and the CRC Press Web site at  
<http://www.crcpress.com>

# *The* Law of Cybercrimes and Their Investigations

---

# Introduction: The Nature and Scope of Cybercrime

---

## What Is Cybercrime?

---

A cybercrime is any conduct that involves the use of a computer or other digital device in the commission of a crime.

*Cybercrime* is a compound word, meaning that it consists of two distinct words, *cyber* and *crime*. Thus, it is perfectly proper to spell the subject of our focus as *cybercrime*, not *cyber crime*.<sup>1</sup>

*Cyber*, when used in conjunction with *crime*, modifies or restricts the application of crime. The meaning of *cyber* can be drawn from two sources: the compound word *cyberspace* and the dictionary definition of *cyber*. The term *cyberspace* was first used by William Gibson in his book *Neuromancer*, which was published in 1985. It commonly is known to refer to the electronic medium of computer networks where online communication takes place. I refer to cyberspace as the space that encompasses digital devices capable of communication with each other.

Merriam-Webster's Online Dictionary defines *cyber* as "of, relating to, or involving computers or computer networks (as the Internet) <the cyber marketplace>."<sup>2</sup> Thus, cybercrime can be defined as unlawful conduct involving the use of a computer or other digital device in the commission of a crime. For purposes of this text, cybercrimes include crimes committed:

1. By the use of a computer, digital, or electronic device as the instrumentality of the crime
2. Upon a computer, digital, or electronic device, in which case the device is the victim or target of the crime
3. By the use of a computer, digital, or electronic device for the storage of evidence of a crime

The federal laws that prohibit online child pornography provide a good illustration of the application of those three categories of cybercrime. Federal child pornography laws prohibit the distribution, receipt, and possession of child pornography (see 18 USC §§ 2252, 2252A). Clearly, distributing and receiving child pornography involves the use of a computer or digital device as the instrumentality of a crime. Distributors also are utilizing peer-to-peer networks to store child pornography on a person's computer for acquisition by others, many times without the knowledge of person whose computer is used to

store the images. In that circumstance, the computer used for storage is both a victim and a device used for storage. Finally, the person who downloads pornographic images can store those images on someone else's computer, which would then be the category 3 type of cybercrime.

## **Cybercrime Distinguished from Computer Crime, Digital Crime, High-Tech Crime**

---

There is considerable disagreement among scholars and professionals concerning the meaning or scope of the term *cybercrime*. I have utilized a rather broad definition similar to that stated a few years ago by Donn Parker: a "crime in which the perpetrator uses special knowledge of cyberspace."<sup>3</sup>

Notice that my definition does not require a "special knowledge of cyberspace." Parker distinguishes between cybercrime and computer crime by defining computer crime as a "crime in which the perpetrator uses special knowledge about computer technology."<sup>4</sup> I agree with Parker that there is a difference between computer crime and cybercrime. There are those who would, however, disagree. For example, the current edition of *Black's Law Dictionary* defines cybercrime as a "computer crime."<sup>5</sup>

I disagree, however, that cybercrime necessarily involves a "special knowledge of cyberspace." The mere fact that evidence relevant to a crime is stored in a computer or peripheral device also amounts to a crime. As discussed previously, a common example is the storage of images of pornography or child pornography on the hard drive of a person other than the individual who downloaded the images from various locations on the Internet. The storage of those images constitutes the crime commonly referred to as criminal possession of obscene materials or child pornography. Other examples include the unlawful downloading of copyrighted material to a digital device or the recording of illicit transactions on a spreadsheet application. Thus, the storage of digital evidence, by itself, may be a crime.

Our final potential term, *digital crime*, is the subject of an entire text,<sup>6</sup> which refers to digital crime as computer-related crime, or cybercrime.<sup>7</sup> Reading the text, however, one quickly realizes that digital crime and cybercrime, as I have defined it, are the same.

## **Trends Related to Cybercrime**

---

Numerous studies are conducted each year related to cybercrime. The Computer Security Institute conducts an annual survey of computer crime and security. The survey<sup>8</sup> is currently released in the fall of each year. It reveals several important statistics concerning cybercrime that should be reviewed, particularly for analysis of trends.

The Internet Crime Complaint Center (IC3), a joint operation of the FBI and the National White Collar Crime Center, issues an annual report of Internet crime complaints that are filed with the IC3. The annual report is available at the IC3's website.<sup>9</sup>

The Federal Trade Commission publishes an annual report of complaints filed with that agency concerning identity theft and consumer fraud. The national results are available at the FTC's Consumer Sentinel site. The Consumer Sentinel site is accessible by law



enforcement agencies who desire information concerning reported instances of identity theft. The annual report is, however, publicly available at the Sentinel site.<sup>10</sup>

Surveys and reports also are published from an international perspective. The Australian Computer Emergency Response Team (AusCERT) publishes an annual survey,<sup>11</sup> as does the Australian Government<sup>12</sup> and the auditing firms of Ernst and Young<sup>13</sup> and Deloitte Touche.<sup>14</sup>

## About This Book

---

This book is divided into four parts. Part I, which consists of Chapters 1 and 2, focuses on the use of computers and other digital devices to commit traditional computer crimes (Chapter 1) and what is popularly referred to as information warfare and cyberterrorism (Chapter 2).

Part II, “Cybercrimes against Individuals,” consists of Chapters 3 to 5. Chapter 3 considers cybercrimes that implicate morality—obscenity, child pornography, sexual predator conduct, and online gambling. Chapter 4 discusses cyberstalking, cyberharassment, cyberbullying, and other types of unlawful expression. Chapter 5 covers online frauds and other online crimes that do not fit neatly into any other category, including auction fraud, Ponzi and pyramid schemes, access device fraud, identity theft and fraud, securities fraud, bank fraud, money laundering, and electronic fund transfer fraud. Part III, “Crimes against Information Assets, and Data Privacy,” consists of Chapters 6 and 7. Chapter 6 considers identity theft and data privacy crimes, including violations of the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). Chapter 7 covers other online crimes against data, including economic espionage and intellectual property crimes.

Part IV, “Investigation and Enforcement of Cybercrimes,” consists of Chapters 8 through 14. Chapter 8 provides an introduction to general principles applicable to searches and seizures. Chapter 9 discusses laws that apply to the search and seizure of computers, other digital devices, and peripherals. Chapter 10 focuses on those laws governing eavesdropping and the use of wiretaps in connection with electronic communications. Chapter 11 considers the law regulating access to stored communications. Chapter 12 covers the law applicable to other investigatory devices, such as pen registers, trap and trace devices, and global positioning system devices. Chapter 13 considers laws and rules governing the admission of digital evidence and provides an overview of criminal procedure. Chapter 14 discusses international laws and procedures for the investigation of cybercrimes and gathering of evidence beyond the borders of the prosecuting jurisdiction.

Each numbered chapter includes three additional features: key words and phrases, review problems, and weblinks. Key words and phrases identify topics or items you should be familiar with after reading the chapter and before reading the next chapter. You should be able to define or describe each of those items. Review problems have been included to enable the student to determine how much has been learned from the material or for a quick review of the chapter at a later time, perhaps for a quiz or an exam. Weblinks are provided to identify websites that provide additional information concerning the material covered in the chapter or information that can serve as a starting point for a research paper. You may notice missing sections. That was intentional. The statutes and cases were edited.

I hope you enjoy your experience as a student of cybercrime law and investigation.

## Endnotes

1. See Garner, Bryan A. (ed.). (2009). *Black's Law Dictionary* (deluxe 9th ed.). St. Paul, MN: West Publishing, p. 443.
2. Merriam-Webster Online Dictionary. <http://www.merriam-webster.com/dictionary/cyber> (retrieved October 22, 2010).
3. Parker, Donn. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons, p. 72.
4. Id.
5. Garner, op. cit., n. i.
6. See Taylor, Robert W., et al. (2006). *Digital Crime and Digital Terrorism*. Upper Saddle River, NJ: Prentice Hall.
7. Id., at 4–5.
8. The 2009 survey can be obtained online at [www.gocsi.com](http://www.gocsi.com).
9. The 2009 IC3 report can be accessed at [www.ic3.gov/media/annualreport/2009\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf).
10. The Sentinel site is [www.ftc.gov/sentinel/reports.shtml](http://www.ftc.gov/sentinel/reports.shtml).
11. Available at [www.auscert.org.au](http://www.auscert.org.au).
12. The 2008 Pacific Islands survey is at [www.esecurity.net.au/PICCSS08\\_survey.pdf](http://www.esecurity.net.au/PICCSS08_survey.pdf).
13. [www.ey.com/Publication/vwLUAssets/Global\\_Information\\_Security\\_Survey\\_2009/\\$FILE/EY\\_Global\\_Information\\_Security\\_Survey\\_2009.pdf](http://www.ey.com/Publication/vwLUAssets/Global_Information_Security_Survey_2009/$FILE/EY_Global_Information_Security_Survey_2009.pdf).
14. The 2009 survey is available at [www.deloitte.com/assets/Dcom-Shared\\_Assets/Documents/us\\_fsi\\_GlobalSecuritySurvey\\_0209.pdf](http://www.deloitte.com/assets/Dcom-Shared_Assets/Documents/us_fsi_GlobalSecuritySurvey_0209.pdf).



---

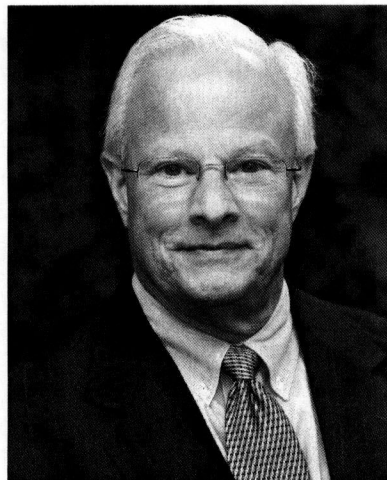
## About the Author

---

**George E. Curtis** is professor of criminal justice at Utica College, Utica, NY. He previously held the positions of dean of the School of Business and Justice Studies and executive director of the Economic Crime Institute of Utica College.

Curtis received a Bachelor of Arts degree from Syracuse University in 1964, and a Juris Doctor degree from Brooklyn Law School in 1967. He is an attorney admitted to the Bar of the State of New York. Curtis served as a confidential law clerk in the New York court system for more than 26 years and currently practices law limited to appellate work. He is a former president of his local bar association and a former delegate to the New York State Bar Association's House of Delegates.

Curtis currently teaches undergraduate and graduate law-related courses in economic crime and cybercrime. He is a Certified Fraud Specialist and a member of the Association of Certified Fraud Specialists, its Board of Regents, and its national faculty. He also is member of the Association of Certified Fraud Examiners and a life member of its Upstate New York Chapter, and the Criminal Justice Educators Association of New York State.



---

# Table of Contents

---

<b>Introduction: The Nature and Scope of Cybercrime</b>	<b>xi</b>
What Is Cybercrime?	xi
Cybercrime Distinguished from Computer Crime, Digital Crime, High-Tech Crime	xii
Trends Related to Cybercrime	xii
About This Book	xiii
Endnotes	xiv
<b>About the Author</b>	<b>xv</b>

## *Section I*

### **CYBERCRIMES AGAINST THE DIGITAL INFRASTRUCTURE AND COMPUTER SYSTEMS**

<b>1</b>	<b>Crimes Involving the Use of Computers</b>	<b>3</b>
	Introduction	3
	Federal Laws Governing Computer Crimes—Historical Development	3
	Federal Laws Governing Computer Crime—18 USC § 1030	5
	Case Applications	6
	New York’s Computer Crime Law	11
	Key Words and Phrases	24
	Review Problems	25
	Weblinks	25
	Endnotes	26
<b>2</b>	<b>Information Warfare and Cyberterrorism</b>	<b>27</b>
	What Is Information Warfare?	27
	Brown Commission	27
	Brian C. Lewis	28
	Martin C. Libicki	28
	Dorothy Denning	28
	What Is Cyberterrorism?	29
	Laws Regulating Information Warfare and Cyberterrorism	29
	Federal Laws	30
	18 USC § 2332b: Acts of Terrorism Transcending National Boundaries	30
	18 USC § 1030: Fraud and Related Activity in Connection with Computers	30
	18 USC § 1831: Economic Espionage	31
	State Laws	31
	Key Words or Phrases	32

Review Problems	32
Weblinks	33
Endnotes	33

## ***Section II***

### **CYBERCRIMES AGAINST INDIVIDUALS**

<b>3</b>	<b>Crimes against Morality</b>	<b>37</b>
	Introduction	37
	Obscenity Crimes	37
	18 USC § 1462	38
	18 USC § 1465	39
	18 USC § 1466	39
	18 USC § 1466A	39
	18 USC § 1470	40
	Case Law Pertaining to Online Obscenity Crimes	41
	Child Pornography Legislation	47
	Legislative History	47
	Current Child Pornography Laws	48
	18 USC § 2251: Sexual Exploitation of Children	53
	18 USC § 2252: Certain Activities Relating to Material Involving the Sexual Exploitation of Minors	54
	18 USC § 2252A: Certain Activities Relating to Material Constituting or Containing Child Pornography	55
	18 USC § 2425: Use of Interstate Facilities to Transmit Information about a Minor	56
	Case Law Pertaining to Online Child Pornography	56
	Online Gambling	69
	Federal Law	69
	The Unlawful Internet Gambling Act—31 USC §§ 5361–5367	69
	The Wire Act—18 USC § 1084	70
	The Travel Act—18 USC § 1952	73
	The Paraphernalia Act—18 USC § 1953	74
	18 USC § 1955	74
	State Gambling Laws	74
	Indiana	74
	New York	74
	Key Words and Phrases	78
	Review Problems	78
	Weblinks	78
	Endnotes	79
<b>4</b>	<b>Crimes Threatening or Resulting in Physical or Mental Harm</b>	<b>81</b>
	Introduction	81
	Sexual Predator Crimes	81

18 USC § 2425: Use of Interstate Facilities to Transmit Information about a Minor	81
Cyberstalking and Cyberharassment Legislation	85
Federal Statutes	85
18 USC § 2261A: Stalking	85
18 USC § 875: Interstate Communications	86
47 USC § 223: Obscene or Harassing Telephone Calls in the District of Columbia or in Interstate or Foreign Communications	86
Cases on Cyberstalking and Cyberharassment	86
Judicial Interpretations of Federal Law	86
Key Words and Phrases	104
Review Problems	104
Weblinks	104

**5 Internet Frauds 105**

Introduction	105
Auction Fraud	105
Ponzi and Pyramid Schemes	106
Access Device Fraud	115
What Is an Access Device?	115
How Is an Access Device Fraud Committed?	115
Electronic Fund Transfer Fraud	116
Identity Theft and Fraud	117
Identity Theft	117
The Federal Identity Theft Crimes	118
18 USC § 1028	118
18 USC § 1028A	119
State Identity Theft Laws	120
Cyberlaundering	122
Other Fraudulent Schemes	127
Key Words and Phrases	128
Review Problems	128
Weblinks	128
Endnotes	128

**Section III**

**CRIMES AGAINST INFORMATION ASSETS, AND DATA PRIVACY**

**6 Data Privacy Crimes 131**

Introduction	131
The Fair Credit Reporting Act (FCRA)	131
The Fair and Accurate Credit Transactions Act (FACTA)	137
The Gramm-Leach-Bliley Act (GLBA)	137

The Health Insurance Portability and Accountability Act (HIPAA)	142
After the Breach: Is There a Duty to Notify the Consumer That the Security of Their Data Has Been Compromised?	143
Key Words and Phrases	145
Review Problems	145
Weblinks	145
Endnotes	146
<b>7 Intellectual Property Fraud</b>	<b>147</b>
Introduction	147
Criminal Copyright Infringement	148
Software Piracy	158
Key Words and Phrases	169
Review Problems	170
Weblinks	170
 <b>Section IV</b>	
<b>INVESTIGATION AND ENFORCEMENT OF CYBERCRIMES</b>	
<b>8 Search and Seizure: Beginning Principles</b>	<b>173</b>
Introduction	173
Constitutional Principles	173
The Fourth Amendment	173
Reasonable Expectation of Privacy	174
Workplace Searches	181
Protection from Government Activity	187
The Mere Evidence Rule	195
Searches with and without a Warrant	195
Consent	196
Plain View	196
Exigent Circumstances	203
Incident to a Lawful Arrest	207
Inventory Search	207
Border Search	208
Administrative Searches	211
Automobile Exception	211
Special Needs Exception	211
Key Words and Phrases	212
Review Problems	212
Weblinks	212
Endnotes	213

<b>9</b>	<b>Search and Seizure: Electronic Evidence</b>	<b>215</b>
	Introduction	215
	Conducting the Search or Seizure	222
	Searches and Seizures without a Warrant	240
	Key Words and Phrases	247
	Review Problems	247
	Weblinks	248
<b>10</b>	<b>Wiretapping and Eavesdropping</b>	<b>249</b>
	Introduction	249
	Statutes and Regulations	249
	Case Law	254
	Key Words and Phrases	291
	Review Problems	291
	Weblinks	291
<b>11</b>	<b>Access to Stored Communications</b>	<b>293</b>
	Introduction	293
	Case Law	295
	Key Words and Phrases	303
	Review Problems	303
	Weblinks	303
<b>12</b>	<b>Pen Register, Trap and Trace, and GPS Devices</b>	<b>305</b>
	Introduction	305
	Pen Register and Trap and Trace Devices	305
	Global Positioning Systems (GPSs)	309
	RFID Technology	322
	Key Words and Phrases	322
	Review Problems	322
	Weblinks	323
<b>13</b>	<b>Digital Evidence and Forensic Analysis</b>	<b>325</b>
	Introduction	325
	Nature of Evidence	325
	Admissibility of Evidence	325
	Preservation of Evidence	327
	Chain of Custody	327
	Admissibility of Digital Evidence	330
	The <i>Frye</i> Test	330
	<i>Frye</i> Plus	333
	<i>Daubert</i> Test	334
	Expert Opinion Evidence	337

Rules Requiring the Exclusion of Evidence	342
Hearsay Rule	342
Exceptions to the Rule	343
Best Evidence Rule	346
Key Words and Phrases	347
Review Problems	347
Weblinks	348
<b>14 International Issues Involving the Investigation and Prosecution of Cybercrime</b>	<b>349</b>
Introduction	349
Jurisdiction	349
Extraterritorial Application of Criminal Laws	353
International Enforcement and Cooperation	363
Letters Rogatory	363
Mutual Legal Assistance Treaty	363
Extradition Treaty	371
Council of Europe Convention on Cybercrime	372
Key Words and Phrases	373
Review Problems	373
Weblinks	373
<b>References</b>	<b>375</b>
<b>Index</b>	<b>377</b>



---

# Cybercrimes against the Digital Infrastructure and Computer Systems

---

I

