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

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

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

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*.[1]

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>."[2] 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."[3]

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."[4] 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."[5]

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,[6] which refers to digital crime as computer-related crime, or cybercrime.[7] 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[8] 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 I3C's website.[9]

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.[10]

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

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.

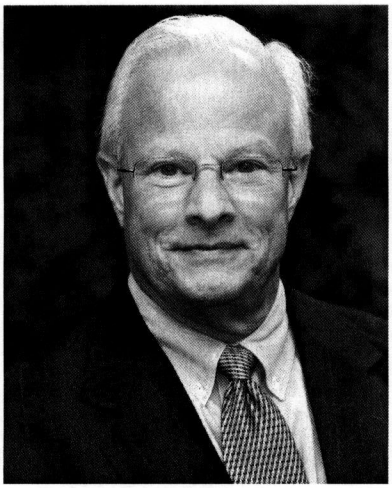
Each numbered chapter includes three additional features: key words and phrases, review problems, and weblinks. Key words and phrases identify topics or items you should be familiar with after reading the chapter and before reading the next chapter. You should be able to define or describe each of those 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.
9. The 2009 IC3 report can be accessed at www.ic3.gov/media/annualreport/2009_IC3Report.pdf.
10. The Sentinel site is www.ftc.gov/sentinel/reports.shtml.
11. Available at www.auscert.org.au.
12. The 2008 Pacific Islands survey is at 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.
14. The 2009 survey is available at 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

Section II

CYBERCRIMES AGAINST INDIVIDUALS

Cybercrimes against the Digital Infrastructure and Computer Systems

I