

**THE CYBERCRIME HANDBOOK
FOR
COMMUNITY CORRECTIONS**



ABOUT THE AUTHOR

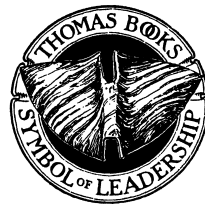
Art Bowker has 26 years experience in law enforcement and corrections. He earned an undergraduate and graduate degree in criminal justice and corrections from Kent State University. Art has completed computer forensic training through the National White Collar Crime Center (NW3C), SEARCH, the Federal Law Enforcement Training Center (FLEC), the Federal Bureau of Investigations (FBI), the American Probation and Parole Association (APPA), and the High Technology Crime Investigation Association (HTCIA). He is a lifetime HTCIA member and served in various positions on its Executive Committee, including International President in 2008. Art is also an APPA member and serves on its Technology Committee. He is an Adjunct Professor at Chancellor University (www.chancelloru.edu/) and writes a blog, the Three C's (Computers, Crime and Corrections), at corrections.com/cybercrime. He can be followed at <http://twitter.com/Computerpo>.

THE CYBERCRIME HANDBOOK FOR COMMUNITY CORRECTIONS

Managing Offender Risk in the 21st Century

By

ART BOWKER, M.A.



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

This book is protected by copyright. No part of
it may be reproduced in any manner without written
permission from the publisher. All rights reserved.

© 2012 by CHARLES C THOMAS • PUBLISHER, LTD.

ISBN 978-0-398-08728-9 (hard)
ISBN 978-0-398-08729-6 (ebook)

Library of Congress Catalog Card Number: 2011039968

*With THOMAS BOOKS careful attention is given to all details of manufacturing
and design. It is the Publisher's desire to present books that are satisfactory as to their
physical qualities and artistic possibilities and appropriate for their particular use.
THOMAS BOOKS will be true to those laws of quality that assure a good name
and good will.*

*Printed in the United States of America
MM-R-3*

Library of Congress Cataloging-in-Publication Data

Bowker, Art.

The cybercrime handbook for community corrections : managing
offender risk in the 21st century / by Art Bowker.

, p. cm.

Includes bibliographical references and index.

ISBN 978-0-398-08728-9 (hard) -- ISBN 978-0-398-08729-6 (ebook)

1. Community-based correction--United States--Management.
2. Probation officers--United States. 3. Parole officers--United States.
4. Computer crimes--United States--Prevention. 5. Criminals--
Rehabilitation--United States. I. Title.

HV9304.B69 2012

364.16'80973--dc23

2011039968

FOREWORD

Digital technology is a part of all of our lives. Our cars record and adjust to our driving habits. We text, tweet, and post our daily lives. We prefer plastic over cash and frequently let the keyboard do the walking when shopping. We choose GPS over maps to get us from point A to point B and our research librarians are being replaced by Google® and Bing®. The spring of 2011 was deemed “The Arab Spring.” The rise of the populous was supported, if not created, by social networks and the Web. Modern politicians are more concerned by their SNS following than mass media coverage. The TSA adjusts its policies in response to You Tube® videos. Blogs and re-tweets have replaced sound bites. Yet, for many years, we acted as if offenders were not part of the wired community. We ignored their digital behavior and failed to monitor it.

I have long held that a computer is a window into the mind of the offender. People look at what they like, they seek out and consume material which supports their beliefs. By examining what an offender seeks and views, we gain an understanding of whom we are trying to manage in the community. Moreover, we gain the ability to assist the offender in learning to appropriately utilize computers in their daily lives. Andrews, Bonta, Latessa et al. focused community corrections on “What Works” and the importance of attitudes, values, and beliefs as well as procriminal associations as factors fostering criminal behavior. Despite understanding these factors, we continued to ignore how the Web isolated offenders and provided support for illicit ideation.

In the 1990s a group of community corrections professionals (Art Bowker among them) began to question how we should address offender computer use while on supervision. Unfortunately, there were few, if any, tools available to assist us. For years we attempted to use tools designed for lab forensics in the far from sterile environment of field forensics within community supervision. In the past 10 years, tools emerged which were developed specifically for triage and field forensics. As these tools were rapidly embraced by many professionals, it became evident there was a second prob-

lem for community corrections. Officers lacked a full understanding of what they could look for, how to look for it, and how to interpret what they found.

This book attempts to resolve this second problem. Written by a man with more than two decades in the trenches of investigations and forensics, Art Bowker provides a clear outline of what we can and should do regarding the management of offender computer use. Not only does this book help community corrections professionals understand how to monitor computer use, but it helps us realize how information gained during monitoring can assist us in overall case management. The technology is now readily available to effectively manage offenders' digital behavior. Bowker's book moves us all toward a more informed use of the technology.

JIM TANNER, PH.D.
Boulder, Colorado

PREFACE

This book will take the reader through paces of managing offender cyber-risk. No advanced technology expertise or background is needed to grasp the discussed concepts or issues. This book is meant specifically for pretrial, probation, parole, and community sanction officers. It hopefully will empower them to meet the supervision challenges of the twenty-first century.

Many probation and parole officers are turning to law enforcement to obtain the technological skills needed for supervising the cyber-offender. This is great for various aspects of managing cyber-risk such as searches. However, proper management frequently requires more than just the ability to do a computer search. One example is installing computer software and reviewing the results. Therefore, community corrections officers need to be trained beyond traditional law enforcement concerns. The material presented in this text will further aid law enforcement trainers when tasked with instructing community correction officers on cybercrime investigation and management.

Many of the techniques discussed in this book obviously require computer use. However, agency computers and systems are not typically controlled or serviced directly by community corrections officers. That function is performed by the correction agency's information technology (IT) staff. This book will provide guidance to IT staff so they can effectively meet the evolving technology needs of those involved in managing cyber-risk.

There is also more to cyber-supervision than just understanding technology. There are also other nuances, such as legal concerns, pro and cons of various techniques, training, equipment needs, and so on. Therefore, anyone charged with managing a community corrections agency (supervisors, chiefs, court administrators, judges, parole commissioners, corrections directors, etc.) will benefit from reading this book. Additionally, both prosecutors and defense attorneys will be in a better position to advocate the various sentencing options, including the imposition of technological conditions, by reviewing this book's material.

This text extensively covers law applicable only in the United States. However, the covered techniques and practices in managing an offender's computer use can be adopted by any foreign jurisdiction involved in community corrections. Many of the tools discussed are openly available outside of the United States. Foreign correctional agencies will therefore gain a better understanding of the technological possibilities for managing cyber-risk by reviewing this book.

The chapters are organized by major areas. The material presented can be read in order or the reader can jump to the topic that he or she is most interested in at the moment. Chapter 1 provides an overview of cyberspace and how it intersects in community corrections. Chapter 2 covers the pros and cons of the various options available for managing cyber-risk. Chapters 3 and 4 cover the legalities of imposing various computer restrictions as well as the enforcement of technological conditions.

Chapter 5 focuses on evaluating cyber-risk. Chapter 6 is a basic primer for understanding computer components and their relevance for supervision officers. Chapter 7 delves into the basic principles of managing an offender's computer use. Chapter 8 discusses computer searches and seizures. Chapter 9 discusses deploying computer monitoring. Chapter 10 covers online investigations by community corrections. Finally, the Appendix contains nine forms mentioned in the text which can be adopted by any community correction agency involved in managing cyber-risk.

A.B.

ACKNOWLEDGMENTS

Almost 25 years ago, when I was first a probation officer at Cuyahoga County (Cleveland, Ohio), I started looking at cybercrime literature. Later, my years as an investigator with the U.S. Department of Labor, Office of Labor Management Standards (OLMS) helped me greatly in becoming comfortable with computers as an investigative tool. Under the tutelage of District Director Jim Gearhart and Supervisor Jack Graczyk, my writing skills also developed. I truly learned the concepts of being concise, accurate, and thorough while working at OLMS.

In 1997, I became a U.S. Probation Officer and transferred those skills again to working with offender supervision. Chief Keith Koenig and later Chief John Peet, III and Supervisor Pete Hoose, encouraged me in developing practices that could be used to manage offender cyber-risk. One result of their encouragement was my seeking out contact with subject matter experts. Two of the first were Lanny L. Newville, Electronic Monitoring Specialist, Texas Western Pretrial Services and Dan Wieser, Jr., Senior U.S. Probation Officer Middle District of Florida, both of whom greatly impacted and improved my cybercrime knowledge base and offender supervision practices.

I also reached out to the High Technology Crime Investigation Association (HTCIA) and the High Tech Crime Consortium (HTCC). These two groups provided much needed information and guidance on best practices. My Ohio HTCIA Chapter friends (Diamond Boggs, Joe Corrigan, Len Drinkard, Barry Gummow, Jim Hawke, and many others) led me many times by the hand in developing some level of comfort handling computer investigations. Additionally, my East and West Coast HTCIA friends, Anthony Reyes and Ron Wilczynski, respectively provided support while I worked on this project and with HTCIA. Much of what I have learned can be tied directly to attending an HTCIA conference or event or speaking with an HTCIA member.

There was also the cybercrime training through the FBI, the Federal Law Enforcement Training Center, National White Collar Crime Center, SEARCH, and the American Probation and Parole Association (APPA). I

want to especially call out Jim Tanner, who teaches the APPA cybercrime course, and thank him for writing this book's Foreword. Finally, there were countless conversations over the years with federal legal experts, such as Bob Kern, Chris Stickan, and Michael Sullivan, which gave me much needed insight into the law and computer crime.

I mention these groups and individuals as they all in a real way contributed to this book's eventual creation. Without their willingness to be supportive and to share their knowledge, this book would not have been written, at least not by me.

There also were some individuals who had a more direct role in helping make this book a reality. They are Scott Brantley, Director of the Chancellor University Criminal Justice Program and former Special Agent and Chief Division Counsel for the FBI in Cleveland, Ohio; Jim Hawke, Partner with Binary Intelligence and former Special Agent with the Ohio Bureau of Criminal Identification and Investigation, Computer Crime Unit; Shawna M. Olachea, Special Offender Specialist, California Central Probation Office, and Debra A. White, Aftercare Specialist, Ohio Northern Probation Office. Their collective comments and suggestions made this book much more readable and understandable. I also want to thank Christopher Brown, Chief Technical Officer of Technology of Technologies Pathway, LLC and Todd Shipley, President at Vere Software for providing screen shots of their software (Figures 28 and 29 respectively). Also I want to thank my son Mark for taking most of the hardware pictures contained in this book. He did a most excellent job. The remaining pictures and screen shots were taken by me.

There are three people who really deserve a special mention. They are my parents, Harry and Martha, and my sister, Bonnie. My parents provided the initial loving and supportive environment to develop the desire to learn new things, including how offenders commit cybercrimes. My smarter sister provided the loving sibling rivalry to push me to do more.

I also want to mention my daughter Stephanie and granddaughter Scarlet; I owe them and my son apologies for diverting my attention to this book. Believe me though, I never diverted my love. This book hopes to provide officers guidance so they all will be better protected as they live and grow in a world ruled by computers and the Internet.

Most importantly, I want to thank my wife Kathy. She provided the needed support for a project like this, as well as the love and encouragement to make me not give up. She also kept at bay the "honey do" list until I finished it. I love you and thank you so much!

Finally, I want to thank Charles C Thomas, Publisher, Ltd. for agreeing to publish this book. Community corrections will never be the same as a result.

CONTENTS

	<i>Page</i>
<i>Foreword—Jim Tanner</i>	v
<i>Preface</i>	vii
<i>List of Illustrations</i>	xvii
 <i>Chapter</i>	
1. DOES COMMUNITY CORRECTIONS COVER CYBERSPACE?	3
Cybercrime Overview	4
Traditional Practices	6
Digital Age’s Advent	6
Cyber-sex Crimes	8
Current Practices	8
Conclusion	11
2. UNDERSTANDING THE OPTIONS	15
Restrictions	16
Functional Restrictions	16
Access Restrictions	17
Total Computer Ban	19
Impact	21
Supervised Person	21
Family/Significant Others	22
Agency	23
Monitoring, Searching, and Other Techniques	26
Monitoring	26
Computer Searches	27
General Searches	28

Online Investigations	29
Polygraph	31
Home Confinement/Location Monitoring	31
Field and Collateral Contacts	32
Interviewing and Records Examination	32
Conclusion	33
3. CONDITION LEGALITY	35
Federal/State Constitutions	36
First Amendment (U.S. Const. Amend. I)	36
Fourth Amendment (U.S. Const. Amend. IV)	36
Fifth Amendment (U.S. Const. Amend. V)	37
Sixth Amendment (U.S. Const. Amend. VI)	37
Eight Amendment (U.S. Const. Amend. VIII)	37
Fourteenth Amendment (U.S. Const. Amend. XIV)	38
State Constitutions	38
Statutes	38
Federal Law	38
State Law	39
Interstate Compact	39
Case Law	40
U.S. v. Paul, 274 F.3d 155 (5th Cir. 2001)	42
U.S. v. Lifshitz, 369 F.3d 173, 175, 190-92 (2d Cir.2004)	43
U.S. v. Zinn, 321 F.3d 1084 (11th Cir. 2003)	44
U.S. v. Sales, 476 F.3d 732 (9th Cir. 2007)	45
U.S. v. Voelker, 489 F.3d 139, 154 (3d Cir.2007)	46
U.S. v. Love, 593 F. 3d 1 (DC Cir. 2010)	47
U.S. v. Tome, 611 F. 3d 1371 (11th Cir. 2010)	48
In Re Hudson, (49 Cal. Rptr. 3d 74 - Cal: Court of Appeals, 1st Appellate Dist., 1st Div. 20, 2006	49
State of New Hampshire vs. Steven Merrill, Case No. 2009-811	50
People v. TR, (Cal: Court of Appeals, 4th Appellate Dist., 1st Div. 2010)	51
Regulations	53
Conclusion	53
4. OPERATIONAL LEGALITY	57
Search Case Law	58

- U.S. v. Tucker, 305 F. 3d 1193, (10th Cir. 2002) 59
- U.S. v. Lifshitz, 369 F.3d 173, 175, 190-92 (2d Cir.2004) 63
- U.S. v. Yuknavich, 419 F. 3d 1302, (11th Cir. 2005) 63
- U.S. v. Herndon, 501 F. 3d 683 (6th Cir. 2007) 68
- Discussion 69
- Statutes 72
 - The Stored Communications Act, 18 U.S.C. §§ 2701-2712 (“SCA”) 73
 - The Wiretap Statute (TITLE III) 18 U.S.C. §§ 2510-2522 75
 - The Privacy Protection Act (“PPA”), 42 U.S.C. § 2000aa 79
- Other Legal Concerns 81
 - Fifth Amendment Issues 81
 - Cyberspace Investigations 83
 - Privileged Materials 85
 - Use of WiFi Detectors 85
 - Use of Ultraviolet Light 87
- Conclusion 88

- 5. ACCESSING CYBER-RISK 91
 - Computers and Criminal Behavior 91
 - Risk Assessment 94
 - Offender’s Motivation 95
 - Criminal Computer Use 96
 - Technical Means 97
 - Technical Ability 99
 - Prior Criminal Behavior 100
 - Evaluating Risk 101
 - Cyber-Sex Offenses 103
 - Files Found 103
 - Equipment and ISP 105
 - Online Activities 106
 - Other Activities 107
 - Risk Level and Monitoring 107
 - Juvenile Texting 109
 - Other Risks 110
 - Substance Abuse 110
 - Gambling 111
 - Suicide 112
 - Conclusion 112

6.	A “BIT” OF COMPUTER EDUCATION	116
	Two Basic Concerns	116
	Computer Basics	123
	Input and Output Devices	125
	Storage	127
	Processing, Communication, and Electrical Supply	134
	Software	136
	Other Concerns	138
	Conclusion	139
7.	PRINCIPLES OF EFFECTIVE COMPUTER MONITORING	140
	Principle 1: Have a Plan	141
	Principle 2: Limit Access	144
	Principle 3: Actively Look for Circumvention	147
	Principle 4: Utilize A Resilient Method	148
	Principle 5: Reliability and Accuracy	149
	Principle 6: Utilize Alerts	150
	Principle 7: Review Notifications/Data	150
	Principle 8: Accessibility	151
	Principle 9: Avoid Negative Impact on Others	151
	Principle 10: Monitoring Can Be Compromised	152
	Conclusion	154
8.	SEARCH AND SEIZURE	155
	Search Types	158
	Boot CD/DVD Software	161
	ImageScan	162
	TUX4N6	163
	Knoppix	164
	NTA Stealth	169
	Discussion	170
	Windows-Based Software	171
	Field Search	172
	Digital Evidence and Forensic Toolkit (DEFT)	174
	FTK Imager®	176
	WinAudit	177
	USBDeview	179
	Triage Tools	180

- Advanced Computer Examination Support for Law
 - Enforcement 182
 - ProDiscover® 182
 - Computercop 183
 - Remote Examination Agents (REA) 184
 - Forensic Software and Hardware 185
 - Seizure 187
 - Mobile Phone and Device Searches and Seizures 189
 - Evidence Storage 190
 - Evidence Disposal 191
 - Conclusion 192
- 9. DEPLOYING MONITORING SOFTWARE 195
 - Evolution of Monitoring Software 196
 - Consumer Monitoring Software 197
 - Original Focus 197
 - Authority 198
 - Familiarity 198
 - Time/Access 199
 - Volume 199
 - Comparison 199
 - Features 200
 - The Company Approach 201
 - Internet Probation and Parole Control (IPPC) 204
 - RemoteCom 205
 - Discussion 207
 - Mobile Phones 208
 - Monitoring Other Systems 209
 - Conclusion 209
- 10. ONLINE INVESTIGATIONS 212
 - Social Networking 212
 - Getting Started 214
 - SNS Profiles 215
 - SNS Monitoring 217
 - Websites 218
 - Documentation 219
 - Training Resources 220
 - Conclusion 222

<i>EPILOGUE</i>	224
APPENDICES	
A. Computer Restriction and Monitoring Program	
Participant Agreement	229
B. Computer Usage Questionnaire	231
C. Hardware/Software Restrictions	244
D. Computer Monitoring Release	245
E. Computer Usage Update Questionnaire	246
F. Authorization to Search/Seize Computer Equipment/ Electronic Data	247
G. Knoppix Evidence Inventory Worksheet	248
H. Preview In Windows	249
I. Property Receipt	250
<i>Index</i>	253

ILLUSTRATIONS

Figures

1. Wrist Watch Containing 2 GB USB Flash Drive
2. Ink Pen Containing 128 MB USB Flash Drive
3. CyberRisk Factors
4. Various Modems
5. Desktop Modem Card
6. Desktop Ethernet Card
7. Various MP3 Players
8. Tamper Tape on Computer
9. Keyghost Logger
10. Inside Computer Case
11. Hard Drives, 30 to 60 GB.
12. External USB Drives
13. Flash Drives
14. Memory Cards
15. Wireless Router
16. WiFi Detection Devices
17. Knoppix 5.1 Desktop View
18. Initial Konqueror Hard Drive View
19. Making Device Writable
20. Konqueror Results for JPG Images
21. Field Search Operation
22. D.E.F.T. Start-Up Menu
23. FTK Imager
24. WinAudit Selections
25. WinAudit Report
26. USBDeview Results
27. D.E.F.T. Log File

28. ProDiscover® Preview
29. Webcase® Control Panel

Tables

1. Cases by Circuit Supporting Technology Conditions
2. Cases by Circuit Limiting Technology Conditions
3. Cybercrime Typology Groups
4. Need for Computer Monitoring in Sex Offense Cases
5. Employer Questions
6. Some Specific File Extensions of Interest
7. Some Folders of Interest
8. Consumer Monitoring Packages

**THE CYBERCRIME HANDBOOK
FOR
COMMUNITY CORRECTIONS**

Chapter 1

DOES COMMUNITY CORRECTIONS COVER CYBERSPACE?

They have computers, and they may have other weapons of
mass destruction.

–Janet Reno, Former U.S. Attorney General

Pretrial officers are responsible for insuring defendants' court appearances, while protecting the community and making rehabilitative efforts. Probation and parole officers likewise are responsible for rehabilitation, reintegration, and community protection. Their combined efforts will hopefully reduce recidivism and provide long-term community protection. Maximizing their effectiveness requires continually addressing risk wherever it may present itself. It is therefore imperative that community correction officers (CCO)¹ effectively manage their caseload's risk, including cyberspace.²

1. Pretrial service officers deal with defendants who have not been convicted and are presumed innocence. They therefore have a slightly different perspective than other supervision officers who deal with offenders after guilt has been established. The term community corrections officers (CCO) in this book will be used to collectively describe pretrial service, probation, parole, and community sanction officers. This text describes concepts and techniques that should be helpful for all officers involved in supervision of defendants and/or offenders. When needed the text will differentiate issues that apply to pretrial service officers as opposed to officers involved in supervision after conviction.

2. Cyberspace in this text describes not only actions taking place online but also any computer activity regardless of whether it has an online aspect.

CYBERCRIME OVERVIEW

Criminal behavior began intersecting with the digital age almost immediately. Early “phreaker,”³ John Draper, aka Captain Crunch, discovered in 1971 that he could obtain free telephone service by blowing a plastic cereal box whistle into a pay phone receiver (Hafner & Markoff, 1991). During the Internet’s infancy, Robert Morris released a worm, a self-replicating program, which shut down thousands of computers (Hafner & Markoff, 1991). Later, the hacker exploits of Kevin Poulsen, aka Dark Dante; Kevin Mitnick, aka Condor; and infamous groups such as the Legion of Doom and the Masters of Deception, influenced the public’s cybercrime perception (Progsystem, 2009). These offenders were generally considered technically sophisticated. The correctional response was incapacitation, namely prohibiting or severely limiting their computer access. This was how community risk was managed.

Unfortunately, corrections has been slow to realize that criminal computer use is no longer limited to the so-called technically sophisticated. Since 2007, MySpace® has reportedly removed 90,000 sex offenders from its social networking site (Wortham, 2009). Youth are now finding ways to commit criminal offenses with computers that in the past only adult offenders could accomplish (Bowker, 1999, 2000). However, computers are not only being misused by sex offenders and wayward youth. Some street gangs are also committing high-tech crimes, such as movie and game piracy. Los Angeles Police Department Senior Lead Officer Randy McCain noted, “They’re making more money selling pirated CDs and DVDs than they would selling narcotics. They make a lot of money and they make the money faster” (Ono, 2010). Parole officers in Multnomah County, Oregon have found parolees with saved electronic data regarding bomb-making instructions, specific plans for a burglary, and how to target elderly for identify theft (Korn, 2011). Additionally, one parole officer found through a mobile phone examination and checking a social networking site that a violent offender was participating in a gang called M.O.B. (Money Over Bitches), which involved individual pimps trad-

3. This is a slang combination of the words phone and freak, denoting someone with an extensive understanding of how telephones function.

ing prostitutes on the West Coast (Korn, 2011). The *2009 National Gang Threat Assessment* reflects:

Gang members often use cell phones and the Internet to communicate and promote their illicit activities. Street gangs typically use the voice and text messaging capabilities of cell phones to conduct drug transactions and prearrange meetings with customers. Members of street gangs use multiple cell phones that they frequently discard while conducting their drug trafficking operations. For example, the leader of an African American street gang operating on the northside of Milwaukee used more than 20 cell phones to coordinate drug-related activities of the gang; most were prepaid phones that the leader routinely discarded and replaced. Internet-based methods such as social networking sites, encrypted e-mail, Internet telephony, and instant messaging are commonly used by gang members to communicate with one another and with drug customers. Gang members use social networking Internet sites such as MySpace®, YouTube®, and Facebook® as well as personal web pages to communicate and boast about their gang membership and related activities. (p. 10)

In 2003, Jennifer Granick, Stanford Center for Internet and Society Director, observed “Without a computer in this day and age, you can’t work, you can’t communicate, you can’t function as people normally do in modern society” (Richtel, 2003). Since 2003, computer and Internet access have only increased as an integral part of law abiding society. According to Nielsen Online, 220 million Americans have Internet access at home and/or work and 73 percent, or 162 million went online in May of 2008 (Nielsen Online, 2008). A 2008 Gallup poll reflected that 31 percent of Americans rely on the Internet for daily news (Morales, 2008). Online banking and shopping are realities. Many community services are located or accessed via the Internet. Taxes and licenses renewals are now done online. Quality Internet educational opportunities are increasing. Online employment searches and posting electronic resumes are also common practice. Additionally, the connectivity between mobile phones and the Internet cannot be ignored. A 2010 Pew Research study noted 75% of teens and 93% of adults ages 18-29 have mobile phones. The study found 58% of 12-year-olds own mobile phones. Additionally, the study noted that 81% of adults between the ages of 18 and 29 are wireless Internet users.