

Cyber-Enabled Financial Abuse of Older Americans: A Public Policy Problem

An interpretative framework investigating the social, economic, and policy characteristics  
of cyber-enabled older American financial abuse

Christine Lyons

A dissertation submitted in partial fulfillment of the requirements for the degree of  
Doctor of Public Administration

College of Public Affairs  
University of Baltimore  
Baltimore, Maryland  
December, 2019

Cyber-enabled Financial Abuse of Older Americans: A Public Policy Problem

A Dissertation

Submitted to

College of Public Affairs

University of Baltimore

in partial fulfillment of the requirements for the degree

of

Doctor of Public Administration

By

Christine Lyons

  
Chair

  
Committee Member

  
Committee Member

University of Baltimore  
College of Public Affairs  
Baltimore, Maryland  
November, 2019

This dissertation is dedicated to those who bravely shared their story with me in confidence. I am truly honored to be entrusted by you with the details of your financial and emotional trauma stemming from a time in your life so vividly painful.

## **ACKNOWLEDGMENTS**

No one writes a dissertation without significant help from others and this is so very true with this endeavor. I would like to give a special thanks to three strong, admiralty intelligent, and hard-working women, my committee: Dr. Heather Wyatt-Nichol (chair), Dr. Lorenda Naylor, and Dr. Shelly Bumphus. Thank you for not giving up on me and encouraging me to continue to research a much under-studied public administration topic. Without your support, this dissertation would not be finished.

I wish to express my thanks to Ms. Nina Helwig; the Adult Protective Services of Montgomery County, MD; and the Fraud Department of the Montgomery County, MD Police. I am also thankful for the time and assistance from Dr. Richard Mestas, as well as two of the best research librarians – Ms. Elizabeth Ventura and Mr. Andrew Wheeler,

I am unable to adequately express my gratitude for the unwavering and unconditional support from my life partner of almost forty years, Clint Lyons; our son Clinton, his wife Annie, and our grandchildren CJ, Gabby, Natalie, and Alex; and our daughter Mary-Michael. I love you all beyond words.

## **ABSTRACT**

Cyber-Enabled Financial Abuse of Older Americans: A Public Policy Problem

Christine Lyons

Global cybercrime and cyber-enabled crime costs more than \$400 billion annually with an estimated cost to the US of over \$120 billion dollars annually. With the spread of cyber-enabled crime, a troubling trend has evolved in which the victim is unknowingly complicit in the offence. These incidents have arisen as an evolving public policy challenge at all levels of government, including municipal, county, state, federal, and global. This dissertation examines the social, economic, and policy characteristics of cyber-enabled elder financial abuse. Elder financial abuse perpetrated over the Internet straddles two challenging areas of public policy: cybercrime and elder abuse. In the context of cyber-enabled crime, this study first explains the mechanisms whereby individuals fall prey to abuse and second; conducts an older American cyber-safety needs assessment, which collects information to identify the extent to which regulatory policies either mitigate or contribute to the financial abuse of older citizens.

## TABLE OF CONTENTS

LIST OF TABLES.....	xii
LIST OF FIGURES .....	xiii
Introduction .....	1
Exposed Consumer Data Leads to Consumer Losses .....	9
Applicability to Public Administration.....	11
Statement of the Problem .....	14
Why Study Cyber-Enabled Abuse of Older Americans? .....	15
Finances in Retirement .....	16
Active Use of Technology by Older Americans .....	18
Background of Cyber-Enabled Financial Abuse .....	19
Unwitting Self-Victimization .....	19
Public Service Delivery and Information Communication Technology .....	20
Cyberattack-Gleaned Data.....	21
Organizational Responses to Data Theft .....	21
Privacy and Data Brokers .....	22
Big Data .....	24
Data Brokers' Use of Consumers' Data .....	26
Legal Consequences .....	29
Behavioral Economics.....	31

Reanonymizing Data .....	35
Purpose of the Study.....	36
Conceptual Framework of Cyber-Enabled Elder Financial Abuse Theory.....	36
Theoretical Framework.....	38
Grooming of the Victim .....	40
Review of the Literature .....	44
Information and Communication Technologies.....	45
The Perpetrator .....	56
Classifications of Cybercrime and Cybercriminals .....	56
Limitations of Law Enforcement.....	77
The Victim.....	80
Persuasion and Trustworthiness .....	84
Older Americans as a Cohort.....	101
Financial Exploitation.....	103
Cognitive Function and Grooming .....	106
Victim Services.....	112
The Internet and Law.....	<b>Error! Bookmark not defined.</b>
The Historical Framework.....	118
Statement of the Research Problem and Significance of the Research .....	125
Methodology.....	126
The Survey: Justification for Narratives and Case Studies .....	127
Law and Document Analysis.....	130
Process Tracing.....	130

Conceptual Framework.....	135
Types of Data.....	137
Data Collection.....	138
Data Sources .....	139
Data Collection Methods .....	139
Data Analysis.....	140
Assumptions and Strengths and Limitations of the Study.....	140
Assumptions .....	140
Strengths and Limitations.....	141
Results .....	142
Internet Crime Complaint Center Results .....	143
Survey Results .....	147
Characteristics of Respondents.....	148
Sentiment from the Survey .....	158
Interviews and Case Study Analyses.....	158
Characteristics of the Victims.....	160
Section One Interviews.....	162
N1 .....	163
Victim Interview.....	164
Relative Interview.....	166
Sister Interview.....	167
O1 .....	168
Victim Interview.....	170

Husband Interview.....	172
Other Information .....	173
F1 .....	173
P1 .....	176
E1.....	179
A2 .....	181
Victim's Letter.....	183
First Adult Child Interview.....	184
Second Adult Child Interview .....	188
H1 .....	191
G1 .....	193
C2.....	196
Section Two Interviews.....	199
J1.....	199
Section Three Interviews .....	201
A1 .....	201
A3 .....	201
B1.....	202
B2.....	203
B3.....	205
B4.....	205
B5.....	205
C1.....	206

D1 .....	207
I1 .....	208
I2 .....	209
K1 .....	209
L1 .....	210
M1.....	211
Existing Law and Selected Criminal Cases.....	212
Cybercrime Law Review .....	221
Law and Characteristics of the Criminal Cases.....	244
Romance and Dating Website Scam .....	246
Romance, Inheritance, and Lottery Scams .....	247
Grandparent Scam .....	250
Investment Scam.....	250
Romance and Inheritance Scams .....	251
Internal Revenue Service (IRS) Impersonation Scam.....	253
Romance, Advance Fee, Counterfeit Checks, Computer Hacking, Email Spoofing, and Check Forgery .....	253
Investment Fraud.....	255
Discussion.....	257
Overview of the Study .....	257
Friends, Family, and Services as Capable Guardians.....	260
Laws as Capable Guardian .....	262

Recommendations for Future Research; Recommendations and Implications for Public Administration.....	267
Recommendations for Future Research.....	267
The Enigmatic Impact: Implications for Public Administration .....	268
Appendix A Consent Form.....	271
Appendix B Survey Summary .....	274
Appendix C Survey Results.....	278
Appendix D Definitions of Terms .....	291
References .....	301

## **LIST OF TABLES**

Table 1. Classification of transnational crimes .....	60
Table 2. Best and Luckenbill's (1982) characteristics of social organization of deviants .....	61
Table 3. Cybercrime typology of Holt (2013).....	62
Table 4. Loss of funds reported to the Internet Crime Complaint Center in 2012 and 2014–2018 .....	144
Table 5. Moniker, type, and loss for each case.....	161

## LIST OF FIGURES

Figure 1. Conceptual framework .....	37
Figure 2. Theoretical framework .....	39
Figure 3. The scammers persuasive technique model developed by Monica Whitty .....	42
Figure 4. Integration of the ontology of financial abuse grooming into the scammers persuasive technique model.....	43
Figure 5. Median amount lost per referred complaint for Florida, Maryland, and Virginia.....	145
Figure 6. Total number of complaints regardless of age for Florida, Maryland, Virginia, and the United States.....	146
Figure 7. Dollar values in millions for all age groups across 50 states. ....	147
Figure 8. Age groups of survey participants.....	149
Figure 9. Age groups of survey participants.....	149
Figure 10. Percentage of different age groups responding yes to questions .....	151
Figure 11. Perceived vulnerability by age group.....	152
Figure 12. Not being part of the workforce by age group .....	153
Figure 13. Victims who may require public assistance by age group .....	154
Figure 14. Three-point rating scale by age group.....	155
Figure 15. Vulnerability .....	156
Figure 16. Vulnerability by age range .....	157

Figure 17. Word cloud.....	158
Figure 18. Application of the theoretical framework to case N1 .....	164
Figure 19. Application of the theoretical framework to case O1 .....	170
Figure 20. Application of the theoretical framework to case F1 .....	174
Figure 21. Application of the theoretical framework to case P1 .....	177
Figure 22. Application of the theoretical framework to case E1 .....	180
Figure 23. Application of the theoretical framework to case A2 .....	182
Figure 24. Application of the theoretical framework to case H1 .....	192
Figure 25. Application of the theoretical framework to case G1 .....	194
Figure 26. Application of the theoretical framework to case C2.....	197

## **Introduction**

US digital dependence continues to grow as American society adopts and uses new varieties of digitally interconnected technology in everyday life—from smart phones to medical wearables, fitness trackers, the global positioning system (GPS), laptops, tablets, credit cards, cable or smart television, and loyalty cards. The internet has created a revolutionary means of product and service delivery, changing whole industries as well as the interaction between providers and clients. Many of these businesses run solely on the internet have developed in the last 10–20 years, which has helped drive consumers to the digital world. As an example, Airbnb, a different way to rent a temporary livable space, challenges the traditional hotel chains just as Uber and Lyft, taxi and ride-sharing services, challenges the established taxicab business (Parker, Van Alstyne, and Choudary 2016). Some brick and mortar businesses, like Borders and Blockbuster, fell victim to the success of companies such as Amazon and Netflix. Examples of finance companies that use the internet are Bitcoin sellers, Lending Club, and Kickstarter (Parker, Van Alstyne, and Choudary 2016). Yelp, Foursquare, and Angie’s List are illustrations of nationwide businesses customized to provide a service in the customer’s location. Aside from business benefits, internet technologies offer social benefits, such as the opportunity for friends and families to reconnect or the chance to meet new friends with mutual interests.

Many of these connections are made through social media<sup>1</sup> platforms, such as social networking sites (Facebook, Google Plus, Gather, eHarmony, Match, and OurTime), micro blogging sites (Twitter, Tumbler, and Posterous), publishing tools (Blogger and Word Press), publishing platforms (Amazon Kindle publishing), rating review (Amazon Home Services, Angie's List, and TripAdvisor), photo sharing sites (Instagram, and Pinterest), video sharing sites (YouTube), online markets (Amazon Marketplace, Etsy, and eBay), and group buying sites (Groupon and Living Social). Online, people discuss work and hobbies, make purchases, socialize, find new friends, and sometimes start friendships, which may progress into romantic relationships (Peris, Gimeno, Pinazo, Ortet-Fabregat, Carrero, Sanchiz, and Ibanez. 2002).

Yet there is a disadvantage to these internet interconnections. Criminal hackers,<sup>2</sup> like their counterparts in the physical world, break in to steal financial assets. However, a thief does not need to hack or break into a computer if he or she can convince or manipulate someone with access to the desired object to provide the password or other vitally important information. In his February 2016 statement for the record on the Worldwide Threat Assessment, Director of National Intelligence James Clapper made the point that privacy, data integrity, and services are threatened by the ubiquitous connection among “smart” devices—from household appliances to the electric grid—through an ever-growing complexity of interconnections.<sup>3</sup> In 2017, the new director, Daniel Coats,

---

<sup>1</sup> Social media is composed of technological and social means by which individuals create and share information and content online. Blogs, message boards, podcasts, file-sharing sites, wikis, and social networking sites are some of the tools used in social media.

<sup>2</sup> A *computer hacker* is an individual associated with the computer underground who specializes in obtaining unauthorized access to computer systems (Meyer 1989).

<sup>3</sup> *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, before the Senate Armed Services Comm.*, 114th Cong. (2016) (statement of James Clapper, Director of National Intelligence).

said in his testimony before the Senate Select Committee on Intelligence that “cyber threats also pose an increasing risk to public health, safety, and prosperity” and that “criminals are also developing and using sophisticated cyber tools for a variety purposes including theft, extortion, and facilitation of other criminal activities.”<sup>4</sup> In 2018, Director Coats testified that “transnational criminals will continue to conduct for-profit cyber-enabled crimes,”<sup>5</sup> and in 2019 he claimed that “financially motivated cyber criminals very likely will expand their targets in the United States in the next few years.”<sup>6</sup>

Cyber-enabled crime, in which the victim is unknowingly influenced by the criminal and becomes unwittingly complicit in the offence, is an emerging public policy challenge that reaches all levels of bureaucracy: municipal, county, state, federal, and global. Cyber-enabled crime against youth is well known and well documented in the information age, with sexual exploitation, cyberbullying, and blackmail causing indescribable misery to victims and their families (United Nations Office on Drugs and Crime 2015; Goodman 2015). The various levels of government legislatures and the judiciary, in conjunction with local and national law enforcement, have thus developed a myriad of efforts to combat these criminal activities against youth, including norms, standards, laws, task forces, sting operations, educational programs, and crime-prevention measures to protect juvenile predation through mediums like the internet (Department of

---

<sup>4</sup> *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, before the Senate Select Comm. on Intelligence*, 115th Cong. 1–2 (2017) (statement of Daniel Coats, Director of National Intelligence).

<sup>5</sup> *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, before the Senate Select Comm. on Intelligence*, 115th Cong. 6 (2018) (statement of Daniel Coats, Director of National Intelligence).

<sup>6</sup> *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, before the Senate Select Comm. on Intelligence*, 116th Cong. 6 (2019) (statement of Daniel Coats, Director of National Intelligence).

Homeland Security 2017). Unlike the youth, there are minimal efforts to combat nefarious activities committed against older Americans.<sup>7</sup>

Every American is impacted by technological developments—from seemingly mundane machinery to complex technologies such as electricity, automotive transportation, air travel, medical advancements, and information and communication technologies (ICT). In fact, Bruce Mazlish, professor of history at the Massachusetts Institute of Technology and American Academy of Arts and Sciences fellow, proffered in his 1993 book *The Fourth Discontinuity: The Co-evolution of Humans and Machines* that it is unrealistic to consider humans without machines. From hearing aids and pacemakers to genetic engineering and artificial intelligence, humans and machines have a symbiotic relationship (Mazlish 1993).

On balance, the technological impact on society has been positive; however, as Mazlish (1993) writes, advances in technology and the inability to control it cause unending strife with devastating consequences, such as electrocution, car mishaps, medical malfunctions, and airplane crashes. The causes of these outcomes may be technical glitches or human error. The advances made in the telecommunications industry however, proved to have a relatively positive impact on American society for generations (Paglin 1990). Only in the last decade have the negative aspects of telecommunications, particularly the internet, come under scrutiny. It is the successful criminal's manipulation of people in the cyber environment that is of interest to this research. More specifically,

---

<sup>7</sup> While the terms *elder* or *elderly* will be used when referring to a government-recognized type of abuse, the terms *older American* or *older citizen* will be used throughout the study to refer to citizens aged 60 years or older. This is in an attempt to avoid the terms *elderly* and *senior*, which may be considered by some as pejorative (Applewhite 2016).

the interest is in the application of strategies of social engineering<sup>8</sup> to influence older Americans to assist in their own victimization<sup>9</sup> (Muscanell, Guadagno, and Murphy 2014).

The internet, whose roots lie in the evolutionary improvement of the telegraph, telephone, radio, and computer, revolutionized the telecommunications industry. Today the internet is more than a distribution channel: it acts as a coordination mechanism and provides the infrastructure for innovative product and service creation (Parker, Van Alstyne, and Choudary 2016). The internet consists of interconnected networks<sup>10</sup> that disseminate information worldwide and provide both individuals and computers the ability to interact seamlessly and simultaneously without any consideration of physical location. These interconnected networks link electronic, telephonic, and other ever-evolving technologies together and enable over \$8 trillion of global e-commerce and trade annually (United Nations Interregional Crime and Justice Research Institute 2012; Pelissic du Rausas et al. 2011). The impact on both society and the economy are enormous. For every job lost due to the advances brought by the internet, 2.4 jobs are created (Pelissic du Rausas et al. 2011). During the 15-year period from 1996 to 2011, the standard of living also advanced. There was average growth of \$500 per capita, which for

---

<sup>8</sup> Social engineering is the practice of deceiving a target, who may never realize they have been victimized, using nontechnical means through personal interaction with the express intent of tricking the victim into revealing personal information, giving up something of value, or breaching normal security practices (Long 2008). Social engineering occurs when a criminal influences a victim or exploits the victim's cognitive bias (Bullee, Montoya, Junger, and Hartel 2017).

<sup>9</sup> A cyber-enabled fraud victim is a person who responded to an internet-based invitation, request, or offer by providing either personal information or a monetary asset, which led to suffering a financial or nonfinancial loss (Cross, Smith, and Richards 2014).

<sup>10</sup> A network is the physical domain of cyberspace (Anderson and Rainie 2017); cyberspace is used to develop, store, change, or exploit information through interdependent and interconnected networks using ICT (Kuehl 2009, 30).

the corresponding increase in quality of life took the Industrial Revolution 50 years (Pelissic du Rausas et al. 2011).

Concomitantly, the downside cost to the global economy from cybercrime and cyber-enabled crime<sup>11</sup> is estimated to be more than \$400 billion annually (Center for Strategic and International Studies 2014). For perspective, these crimes' monetary value is roughly equal to 15%–20% of the world's gross domestic product, much of which is absorbed by the most digitally connected countries: the United States, China, Japan, and Germany (Glenny 2009; Center for Strategic and International Studies 2014). The cost to the United States is estimated to be as high as \$120 billion annually, with a direct impact to over 500,000 US jobs every year (Demirdjian and Mokatsian 2015). In 2015 Juniper Research claimed that by 2019 businesses globally would lose more than \$2 trillion from crime committed in cyberspace. Cyberspace was defined by the Bush administration in "National Security Presidential Directive 54/Homeland Security Presidential Directive 23" (2008) as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (6). Cyber is a man-made domain, an ecosystem unto itself, and the governance of this system is dispersed internationally. The complexity cannot be overstated, with the biggest internet businesses approaching member populations and control over economic systems that rival those of nation-states (Parker, Van Alstyne, and Choudary 2016). The lack of an internationally recognized set

---

<sup>11</sup> A cybercrime is a crime committed via telecommunications networks in which computers or computer networks are used for criminal activity. Activities may include financial exploitation, pedophilia, denial of service, credit card fraud, identity theft, blackmail, harassment, stalking, software piracy, and child pornography (IC3 2012). Cyber-enabled crimes are traditional crimes that are perpetrated with ICT (McGuire and Dowling 2013). Theft through deception and fraud are examples.

of laws to govern the internet or a comprehensive approach to address cybercrime or cyber-enabled crime led President Obama's White House cybersecurity coordinator,<sup>12</sup> Michael Daniel (2017), to assert that "the United States' digital dependency makes cyber the number one policy challenge for the 21<sup>st</sup> Century."

The US government's focus on this challenge has been primarily on cyber's impact to the US government's infrastructure, financial institutions, and other critical industries, which overshadows the effect of cyber-enabled crime on the individual citizen. This concern and focus are understandable, as the cyber problem facing the government is more sophisticated and dangerous than ever before (Daniel 2017). Worse, it is years before almost 60% of the government's security breaches are discovered (SecurityScoreCard 2018). In 2007 the problem was malware such as worms,<sup>13</sup> by 2012 it was denial of service attacks, and in 2017 concern turned toward the security of the power grid (Daniel 2017). Today, the internet underpins every aspect of American citizens's lives and serves as the foundation for much of the country's critical infrastructure. As an example of the government's infrastructure concern, a successful digital attack on a western-US electric utility's critical infrastructure occurred on March 5, 2019 (Sobczak 2019). While this interfered with the electrical grid operations and serves as a significant warning, it was not sophisticated enough to affect service to customers (Sobczak 2019). However, a 2015 joint Lloyd's and University of

---

<sup>12</sup> Sometimes referred to as the *cyber czar*.

<sup>13</sup> The three most prevalent types of malware are

- viruses, which delete or collect information using an executable file that remains dormant until opened;
- worms, which are capable of spreading across the internet without assistance from other files; and
- trojans, which appear to be like other programs but are malicious and capable of performing unauthorized tasks.

Cambridge's Centre for Risk Studies report claimed that the impact of a large-scale sophisticated attack could cost hundreds of millions of dollars, hence the federal government's focus on national-level cybersecurity (Sobczak 2019; Maynard and Beecroft 2015). The power grid, financial systems, communication networks, supply chain management tools, water treatment, and controls of transportation modes all connect through key digital systems supported by the internet.

However, since 90% of Americans use the internet for personal reasons, the potential for crime against the individual is substantial (Lebo 2016). In fact, the Internet Crime Complaint Center (IC3)<sup>14</sup> received 3,463,620 complaints between May 2000 and December 2015 from individual citizens, which—according to the estimates from the US Department of Justice (IC3 2014)—represents approximately 15% of the victims (US Department of Justice 2015; IC3 2016). The loss to individuals during this timeframe is over \$4 billion, with over \$3 billion of that during five reporting years (IC3 2012, 2013, 2014, 2015, 2016). Between 2013 and 2017, the loss to 1,420,555 complaints was \$5.52 billion, with seniors making up approximately 17% of the victims but over 20% of the losses (IC3 2014, 2015, 2016, 2017, 2018). The total financial loss to Americans rose from \$1.418 billion in 2017 to \$1.7816 billion in 2018, with seniors making up approximately 24% of the victims and 34% of the losses (IC3 2019). The inability of government and businesses to manage privacy and cybersecurity continues to

---

<sup>14</sup> The IC3, sponsored by the Federal Bureau of Investigation, the Bureau of Justice Assistance, and the National White Collar Crime Center, is a multiagency task force whose mission is to provide a public reporting vehicle for internet-facilitated crimes (IC3 2016). The IC3 maintains a database of complaints to assist all levels of government and law enforcement and publishes an annual report of complaints submitted the previous year. In addition, the IC3 conducts analysis on ostensibly disparate incidents, referring many to law enforcement for investigation and possible prosecution (IC3 2013).

significantly impact the consumer and creates an environment where individuals are at risk of experiencing significant losses.

### **Exposed Consumer Data Leads to Consumer Losses**

News outlets are replete with stories of compromised data from hacked computers, but little reporting has focused on the fraud inflicted on individuals following these hacks, as it is difficult to attribute harm that resulted from inadequate cybersecurity. Companies from all sectors of business, including entertainment, investment, and health care, and the federal government have had their data and their customers' data compromised. Well-known corporations with millions of customers—such as Home Depot (56 million customers), Target (40 million), Sony (47,000), Premera Blue Cross (11 million), Ashley Madison (unknown), Anthem (80 million), and JPMorgan (76 million), Equifax (over 145 million), and the Marriot hotel chain (as many as 500 million)—and their patrons have suffered from cyberattacks (Krebs 2015; Money 2014; Equifax 2017; Marriott 2018). Then there are surprising sectors that are potentially lucrative for the criminal. For example, TruShield, a cybersecurity company, reported that the legal profession is the most targeted industry after retail and finance (Babazadeh 2018). Lawyers have sensitive client information, which significantly reduces the hackers' time and efforts to obtain a significant treasure trove of personal data and potentially embarrassing information (Babazadeh 2018). The lawyer or law firm is often unaware of any breach; therefore, clients are not notified of the danger from their exposed personal information (Babazadeh 2018).

While all states and the District of Columbia require notification of affected parties, there is no federal regulation requiring notification.<sup>15</sup> The timing of notification, how notification is made, and under what circumstances the notification is made is determined by a maze of laws. According to Daniel (2017), these industry security failures were not due to the sophisticated capabilities of criminals: criminals exploit software patch negligence, design flaws, policy implementation failures, or other elements of security failure. The senate report on Equifax's 2015 data breach found there were over 8,500 vulnerabilities that the company failed to address for more than 90 days beyond the recommended patching timeframe; more than 1,000 of them were externally facing vulnerabilities that were rated medium to critical. Over 145 million citizens had their personal information compromised through the Equifax security failure (Kanell 2018).

In her testimony before the Senate Committee on the Judiciary in October 2017, Jamie Winterton, director of strategy at the Global Security Initiative at Arizona State University, stated that cyber threats are making greater headway than the ability to defend against the criminal's onslaught:

Companies collect and store vast amounts of personal data, yet cannot adequately protect them. One reason we can't sufficiently secure online systems is because we fail to understand their complexity—from a computer science perspective, a social science perspective, or a legal perspective, much less the overlap of all three . . . [t]ime to implement a forward-looking research agenda. It's clear that

---

<sup>15</sup> Senate Comm. on Homeland Security and Governmental Affairs, Permanent Subcomm. on Investigations, *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach*, S. (2019).

we need some revolutionary approaches to the problem if we want things to change.<sup>16</sup>

This dissertation investigates the social, economic, and policy characteristics of cyber-enabled financial abuse to advance the body of knowledge of the field of public administration and inform policies on cybercrime and older citizens. Financial abuse<sup>17</sup> against older Americans perpetrated over the internet straddles two challenging public policy areas: cybercrime and older-citizen (elder) abuse.<sup>18</sup> In the context of cyber-enabled crime, this study seeks, first, to explain the mechanisms whereby individuals fall prey to fraud<sup>19</sup> and, second, to understand how policies either mitigate or contribute to the financial abuse of older citizens.

### **Applicability to Public Administration**

For some Americans, cybercrime is a personal problem, but the quantity and severity of the crimes as well as their impact to society as a whole makes cybercrime a public policy problem. The US government is struggling to protect the country's vital

---

<sup>16</sup> *Equifax: Continuing to Monitor Data-Broker Cybersecurity: Hearings before the Senate Comm. on the Judiciary, Subcomm. on Privacy, Technology, and the Law*, 115th Cong. P.3 (2017) (statement of Jamie Winterton, director of strategy at the Global Security Initiative at Arizona State University).

<sup>17</sup> Financial or material exploitation is the illegal or improper use of an older person's funds, property, or assets. Examples include, but are not limited to, cashing checks without authorization or permission, forging another person's signature, misusing or stealing an older person's money or possessions, coercing or deceiving an older person into signing a document (e.g. a contract or a will), and improper use of conservatorship, guardianship, or power of attorney (AoA 2011).

<sup>18</sup> Abuse is "the knowing infliction of physical or psychological harm or the knowing deprivation of goods or services that are necessary to meet essential needs or to avoid physical or psychological harm" (42 U.S. Code §1397j). Elder financial abuse or exploitation is the illegal or improper use of an older adult's funds, property, or assets (GAO 2011). *Elder* is the commonly used legal term to describe the demographic of the victim. For the purposes of this paper, and to avoid using what some consider a pejorative word, *older American* or *older citizen* will be used.

<sup>19</sup> Fraud and financial exploitation are both crimes, and these terms are often used interchangeably. Strictly speaking, however, the perpetrator of financial exploitation takes advantage of the victim's psychological vulnerability and impaired ability to effectively make reasoned decisions, while fraud involves deceiving or tricking a victim who has the capacity to make an informed decision based on the available information (Hill 1994; Roubick 2009).

cyber-dependent infrastructure (e.g., financial, transportation, power, and supply chain), which overshadows serving the citizen's need for protection against cyber-enabled financial abuse. In addition, the failure of the US government and corporations to secure personally identifiable information increases an individual's susceptibility to financial abuse.

Even though the IC3 collects data and works with law enforcement entities to resolve problems, the sheer magnitude and nature of the cybercrimes overwhelms law enforcement. Gaus (1947) proffered that one of the reasons society has an inability to address a given problem, in this case cyber-enabled fraud, lies in the rate of invention and the capacity to adjust to the effects of invention. This is a critical issue, as cyber-related technology increases exponentially every year concomitantly with the threat from criminals, yet Gaus (1947) claims the inability to adjust makes even the catastrophic effects of a disaster such as Pearl Harbor (or 9/11) induce only moderate institutional changes. Consequential policy change begins with a diagnosis of the problem, inquiry into the existing public policy, and analysis to provide insight into the instruments of government (Gaus 1947).

For Herbert Simon (1997, 118), "the central concern of administrative theory is with the boundary between rational and nonrational aspects of human social behavior. Administrative theory is peculiarly the theory of intended and bounded rationality—of the behavior of human beings who satisfice because they have not the wits to maximize." In actuality, all decisions are a matter of compromise, since no one person has the ability to identify all possible alternatives, determine the consequences from each of the alternatives, and then compare the accuracy and efficiency of each of these consequences.

Even large corporations are fallible when it comes to predicting outcomes with a high degree of certainty. In other words, while “rationality requires a choice among all possible alternative behaviors,” Simon (1997, 79) acknowledged that humans had restricted information and developed what they would consider rational techniques in order to overcome limited knowledge or arrive at a satisfied decision. Simon (1997) characterized the computer as providing so much information that the time required to parse and understand all of the material replaced information as the scarce commodity for decision-making. The overabundance of information, the lack of time, and the propensity of the individual to be “subject to the influence of the organized group in which he participates” leads internet users to bounded rationality in decision-making (Simon 1997, 111).

An unfortunate reality for victims is the difficulty in intergovernmental administrative arrangements, where most of the public policy decisions are impacted by byzantine procedures that fail to connect public policies with a network of multiple organizations. Public administration has a responsibility to respond to the changes influenced by the social and technological environment, in as much as “the citizen blames the ‘bureaucrats’ and ‘politicians’ because the basic ecological causes have not been clarified for him. But he sometimes forgets the importance of the invention of social institutions or devices, and their continuing influences which coerce us” (Gaus 1947, 14). However, Gaus (1947, 16) contends that people are “originators of ideas and of social as well as physical invention,” which means cyber-enabled financial abuse, as a human artifact, can be fixed by humans. Like past inventions, cyber, as a recent technological development, will influence the role of the public administration (Haque 2015). After all,

for decades public administration has helped solve problems by giving political and economic voice to vulnerable citizens. The consequences of not addressing the citizenry's cybersecurity needs could be a citizen-collective financial catastrophe and a loss of confidence in the government (Frederickson 2008; Gaus 1947).

### **Statement of the Problem**

Older Americans are the fastest growing organic demographic of American society. Growing equally quickly is the internet use of older Americans, including use of social media applications, several of which are explicitly meant for older citizens' use (Perin 2015a; Cookson 2009; Greenwood, Perrin, and Duggan 2016). However, concurrent with the increased use of ICT is the growth of cyber-enabled crime, often specifically targeting older Americans (Goodman 2015; Iowa 2005; Interpol 2016; Duhigg 2007).

While some youth are vulnerable to cybercrime due to underdeveloped cognitive function and some seniors are at risk of declining cognitive function, most older victims of cybercrime are cognitively intact. As evidenced in the annual IC3 reports, all citizens are vulnerable to cyber-enabled financial abuse. The crux of the issue for victims over 60 years of age—who often are no longer participating in the workforce—is that they usually have neither the means nor the opportunity to repair their financial situation after victimization. According to Page Ulrey (2015), senior deputy prosecuting attorney for King County in Washington state, depending on the financial severity of the crime, an older victim may lose their entire financial savings and require public assistance. The type of public aid needed can range from emotional and psychological health support to basic subsistence: housing, clothing, and money. As the intensity and frequency of cyber-

enabled crime increases, research is necessary to understand the resources needed to address the needs of older Americans with respect to cybersecurity against financial abuse and the potential impact of that abuse on their quality of life. Examination of policies illuminates how existing and new US laws have adapted to the cybercrime problem and also reveals gaps in the laws, which affect older citizens' financial independence (Lukasik 2011; Wilshusen and Barkakati 2013).

### **Why Study Cyber-Enabled Abuse of Older Americans?**

As Americans live longer, senior citizens are becoming the fastest-growing segment of society (Kiel 2005). The oldest of the baby boomers, the “booming seniors” group born in and right after 1946, are already in their 70s. In a report to Congress, the federal government’s Administration on Aging (AoA) estimated there were 60 million resident adults aged 60 years and over in 2011. From 2000 to 2040, the number of US residents over the age of 60 years will more than double to almost 102 million, with 14 million of those citizens expected to be aged 85 years or older (AoA 2013). According to the National Center for State Courts (2019), the fastest-growing age group in this category are those aged 100 years and older. Life expectancy significantly increased from 1900 to 2010; based on the censuses in those years, in 1900 only 6.4% of the population was over the age of 60 years, compared to 18.4% in 2010 (AoA 2013).

Many factors have contributed to this increase in life expectancy, including advances in medical practice, greater safety standards, improved sanitation, increased financial security in old age, and a better food supply. This has led to what Olshansky et al. (2006) termed the *longevity dividend*, in which people have longer, more productive lives and are able to delay what many consider the adverse effects of aging. The

longevity dividend has many positive aspects, including the ability to work, which supports both the individual and society economically and often has social benefits (Olshansky et al. 2006). In many respects, this active, creative, and involved generation has worked hard and produced many social benefits, including the internet. Seniors use cyber-enabled means of communications to combat loneliness. The Senate Special Committee on Aging found that the mental and physical effects of social isolation have detrimental effects on older Americans' health comparable to those of smoking, obesity, and cancer.<sup>20</sup>

### **Finances in Retirement**

The terms *elderly*, *senior citizen*, and *older adult* are euphemisms to describe a stage of life that is not well defined. Like teenagers—who by rite of passage become eligible for driver's licenses, to buy cigarettes, and eventually to buy alcohol, rent cars, and sign legal documents—seniors are people who through rite of passage become eligible for pensions and medical benefits and become targets of marketing gimmicks, such as special meals at certain restaurants and “senior community living.” In some states, people qualify for senior services as early as 55 years of age. With retirement, many seniors simultaneously begin a new phase of their lives and a new level of vulnerability when making decisions about their pensions. Pensions have regulatory oversight, but often individual retirement accounts do not (Agarwal, Driscoll, Gabaix, and Laibson 2009). The change from pension plans to defined contributions has made individuals responsible for overseeing and managing their own retirement security. With an increasingly unpredictable economy, retired Americans face the intricate and complex

---

<sup>20</sup> Senate Special Comm. On Aging. Senate Aging Committee Examines the Mental and Physical Effects of Social Isolation and Loneliness (2017).

process of financial investment and savings. Success requires a thorough knowledge of financial basics, various financial tools, and investment choices (Banerjee 2011) such as savings accounts, equity investments, derivative and fixed-income instruments referred to as options, warrants, swaps, commodity-based futures and futures options, and auction rate securities (Analysis Group 2012). According to Banerjee (2011), participants usually choose lump sum payments over annuities with absolute control over how much money they will use each month (Hueler 2010). The National Committee for the Prevention of Elder Abuse (2017) website claims that 70% of US wealth is controlled by people over the age of 50 years; however, the majority of this wealth is invested in their homes and is not necessarily liquid. Their lump sum retirement accounts, however, are liquid and readily accessible.

In 2010, a MetLife study revealed reports of American senior citizens being defrauded of \$2.9 billion through a myriad of means, including online. While this seems like an astounding amount of money, experts believe the true value is much greater. The report is made more disconcerting by the National Incidence Study's revelation that 84% of all elder abuse cases are unreported (National Center on Elder Abuse 1998). Mason and Benson (1996) found victims tend to underreport their losses when they believe they were due to their own gullibility and are embarrassed by what they consider a self-made failure of decision-making. This all-too-often internalized embarrassment increases the probability of repeat victimization (Mason and Benson 1996; Herlery 2012). Like Willie Sutton,<sup>21</sup> who reportedly claimed he robbed banks because that was where the money

---

<sup>21</sup> Willie Sutton, June 1901–November 1980, was a well-known American bank robber who spent most of his adult life in prison (*Encyclopedia Britannica Online*, Academic ed., s.v. “Willie Sutton,” accessed December 3, 2012, <http://www.britannica.com/EBchecked/media/172200/Willie-Sutton>).

was, seniors are targeted because they possess an amount of readily accessible money worth going after and tend to be in a position to make unilateral financial decisions. This concept of the rich older Americans tends to be one of the reasons older Americans are targeted. Specific targeting, available assets, loneliness, and having more time available online are the primary reasons this group has greater financial losses.

### **Active Use of Technology by Older Americans**

The “younger set” (aged 60–84 years) of older citizens helped build the internet and adeptly use email accounts, download applications, and connect to communities of common interest through social networking. With its potential to extend social reach, social media has grown exponentially: the number of social media users increased 64% between 2005 and 2013 (Tsikerdeks and Zeadally 2014). Despite misperceptions of older Americans’ competencies with technology, these sage netizens<sup>22</sup> are online. A 2015 Pew Research Center report found that 58% of citizens aged 65 years and older use the internet, while a second report showed that 35% were using some form of social media (Perrin 2015a, 2015b). By 2017, the technology adoption rate for seniors was around 67%, with 42% using smartphones (Anderson and Perrin 2017). While the number of older Americans who routinely navigate the Web is increasing, the use is highly dependent on age, education, and household income. For example, 47% of seniors aged 65–69 years reported using social media compared to 41% of those aged 70–74 years, 24% of those aged 75–79 years, and 17% of those aged 80 years or older. Fifty-six percent of those with college education use social media compared to 39% of those with some college and 20% of those with a high school diploma or less (Anderson 2017).

---

<sup>22</sup> A netizen is “an active participant in the online community of the internet.” *Merriam-Webster.com*, (2019), s.v. “netizen (n.).”

Household income of seniors using social media ranged from less than \$30,000 per year (23%) to over \$75,000 per year (57%). Richer, better-educated, younger seniors are more likely to use social media, and their financial status make them an attractive and—too often—lucrative target for online fraudsters (Anderson and Perrin 2017).

The internet, including social media networks, is a valuable tool in the criminal's arsenal to defraud and rob unsuspecting and less-skeptical victims. The proliferation of technology has both improved and harmed individual users, nation-states, and businesses. There is an unrecognized but serious battle going on for the financial well-being<sup>23</sup> of the individual citizenry, including older Americans.

### **Background of Cyber-Enabled Financial Abuse**

In 2015, it was reported that over half of citizens aged 65 years or older use the internet; by 2017, the proportion climbed to two-thirds (Perrin 2015a; Anderson and Perrin 2017). Eighty-two percent of those aged 65–69 years, 65% of those aged 70–74 years, 60% of those aged 75–79 years, and only 44% of those aged 80 years or older use the internet (Anderson and Perrin 2017). Smartphone use across age categories has a similar pattern: 59% of those aged 65–69 years, 49% of those aged 70–74 years, 31% of those aged 75–79 years, and only 17% of those aged 84 years or older.

### **Unwitting Self-Victimization**

Many do not realize they unwittingly contribute to their own abuse and financial victimization using ICT. The IC3 reports between the years 2012 and 2016 show older Americans reporting a loss of over \$1 billion; in 2018, the IC3 reported over \$300 million

---

<sup>23</sup> “Consumers perceived financial well-being as a state of being wherein a person can fully meet current and ongoing financial obligations, can feel secure in their financial future, and is able to make choices that allow them to enjoy life” (Consumer Financial Protection Bureau 2015, 18).

was lost, and in 2019 over \$600 million was lost, which is staggering given that the Department of Justice (DOJ) believes this accounts for only 15% of victims (IC3 2013, 2014, 2015, 2016, 2017, 2018, 2019).

### **Public Service Delivery and Information Communication Technology**

The federal government, in its delivery of public services, proactively promotes older citizens' use of technologies like the internet to access and obtain benefits, such as those offered by the Social Security Administration (2016). For more than a decade, governments at all levels have shifted toward digital interface with the communities they serve; in 2002, the 107th Congress passed the E-Government Act in order to enhance citizens' access to the federal government's products, services, and information.<sup>24</sup> Martin (2003) found states were moving away from the costs associated with traditional notifications in newspapers toward online postings for public and legal notices, thereby saving taxpayers' money and driving the citizenry to use the internet for information and access to services. Now, financial institutions such as Citibank use web-portal biometric identity confirmation to send funds worldwide to retirees, even those living in remote areas (Friedman 2016).

The drive to online cyber-enabled service delivery requires the transmission of personally identifiable information along with personal log-on identification over ICT. As citizens age into the ranks of older Americans and bring with them familiarity with technology, the security of these systems is paramount. While thousands conduct hundreds of transactions online every day, the opportunity for error and the risk of data

---

<sup>24</sup> 44 U.S.C. § 101 as amended (2018).

exposure has significant implications for data that could be used against older Americans in scams.

### **Cyberattack-Gleaned Data**

Media outlets are replete with fact-laden stories of successful cyberattacks against banks, corporations, and the US government but not of the impact on the individual. Often the composition and impact of stolen data are not fully understood at the time of the theft. By the time the extent of the data stolen is discovered, weeks after the incident, the media has lost interest. Even when the type of data stolen is discovered, there is no method to determine the value of the sensitive personally identifiable information taken. The possession of the data by criminals may lead to secondary and tertiary impacts for the primary generators of the data (individuals), and since data are virtually unperishable, personal information may be available for use years later. Scott's (2017) research states that artificial intelligence and machine learning potentially enable criminals to use this information for decades to psychographically target vulnerable individuals.

### **Organizational Responses to Data Theft**

Data theft from just three US entities—Target in 2013, Home Depot in 2014, and the Office of Personnel Management in 2013–15—exposed personal data of practically one-third of the nation's residents. These data ranged from the seemingly benign, such as name, address, email address, and phone number, to the personal, such as age, gender, marital status, and race. More intrusive data harvested included social security numbers, education and employment history, data concerning health and life insurance, financial history, pension information, and information about family, friends, and acquaintances. Target, Home Depot, and the Office of Personnel Management, like other “hacked”

organizations, offered an apology accompanied by an offer of free limited-time credit monitoring to promote a sense of security among affected customers and clients. While the apology and free credit monitoring are considered positive, corrective steps and are required in some states, hacked data may be transferred around the cyber underground for years only to surface much later to the detriment of the individual who has been lulled into a false sense of complacency by one year of credit monitoring (GAO 2017). Credit card companies tend to be more proactive, primarily because there is a direct link to the card issuer and often larger sums of money are involved. To help potential victims, credit card companies monitor their cards for unusual activity. Naturally, this monitoring helps protect the companies' financial interests just as much as it protects individual customers. These small gestures for the protection of the consumer or client do not, however, stop criminals or data brokers<sup>25</sup> from collecting, correlating, and combining personal data for sale to retailers, businesses, or others who may then resell it on the worldwide underground market.

### **Privacy and Data Brokers**

A seemingly innocent visit to a website or an exchange with friends, acquaintances, or businesses is not menacing or alarming on the surface. In reality, however, data<sup>26</sup> contained in each email sent, website visited, and show watched on cable or smart<sup>27</sup> television may be collected by a data broker or aggregator. Every purchase

---

<sup>25</sup> A data broker collects activities of consumers while they watch TV, shop online, get married, “like” a Facebook page, do online searches, show interest in hobbies or books, and make offline purchases. Data brokers collect information such as phone numbers, email addresses, social security numbers, birthdates, leaked health records, income, number of children, and other facts that characterize an individual in order to perform analytics and sell the results (Matsakis 2019).

<sup>26</sup> Data are descriptions of a person’s or object’s attributes: what or who an entity is and where it is, including its temporal dimension. Information provides an explanation of data in a context.

<sup>27</sup> As of January 2019, the courts have decided to allow a class action lawsuit to move forward against Vizio for covertly tracking and then selling customers’ viewing information to data aggregators (Whittaker

made online generates a point of data that is collected and sent to a data bank. Data aggregators collect data from multiple sources under licensing agreements from various corporations and generally resell to other companies for legitimate purposes such as advertising. The original company that provided the data receives a share of the profits generated (Parker, Van Alstyne, and Choudary 2016). In addition, well-known “free” email services, such as Gmail, both collect metadata (to whom and from whom emails or text messages are sent and received, the length of each message, and the time of each message) and scan for key words to build a representative model of content, which is then scoured by algorithms for patterns. These data may be combined with data collected about offline behaviors, such as consumers’ vacation or travel preferences, buying habits, and use of loyalty discount cards, credit cards, GPS-enabled smartphone location tracking, and cable TV. Young’s (2013) research found users have been known to leave clues on their social media profiles. The study suggests that personal information such as religious or romantic interests made available online can be used to predict an individual’s motivations (Young, Dutta, and Dommety 2009). Data brokers combine this data, analyze it, divide it into distinct groups, and give it confidence levels of accuracy (Goodman 2015). This enables consumers to receive information about goods or services that are of potential interest. Algorithms, opinions in code, help scrutinize personal data for the benefit of the data consumer. The analytic capability of the algorithms assesses emotional, behavioral, and cognitive dimensions associated with the individual. Data aggregators bucket the information<sup>28</sup> into categories such as a “two-person household

---

2019). Related to this case, Vizio paid \$2.5 million in penalties to the government in 2017 for illegally tracking their customers (AP News 2017).

<sup>28</sup> Information provides an explanation of data in context.

with high income and expensive taste,” “sweepstakes enthusiasts,” “cash-hungry individuals,” “impulsive buyers . . . primarily mature,” “over the age of 40, with household income of approximately \$25,000,” or “compulsive online gamblers” (Iowa 2005; Drozdenko and Drake 2002). Some categories are aimed at older Americans, such as “Rural Everlasting”—men and women over 66 years in age with low educational attainment and low income—and “Thrifty Elders”—single men and women in their late 60s and early 70s who are in a lower-income bracket (Ramirez et al. 2014). This information is sold to interested merchants and other buyers who may use it for legitimate or dishonest purposes (Iowa 2005).

## **Big Data**

This collected, analyzed, information often is referred to as *big data*, which the National Science Foundation (2012, 3) defines as “large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future.” In May 2014, President Obama’s administration noted the risks and benefits from big data in a report (Podesta et al. 2014). The report pointed to the ethical concerns of big data ownership, inquiring whether data constitute a public resource or a private identity. The report questions who owns data, what principles guide how data are managed, and who has a right to data.

Degli-Esposti’s (2014) research describes how industries’ collection, analysis, and use of big data influences individuals’ behaviors for marketing purposes. It also provides insight into the potentially negative uses of big data. Roger Clarke (1988) used the term *dataveillance* to refer to the mediation or influence of people’s behavior using analyzed

collected data to monitor them (Degli-Esposti 2014). As a practice, dataveillance consists of recording observations (use of internet, cable TV, credit cards, cellphone, loyalty cards, viewing, types of purchases, and places visited), employing analytical applications (development of usable information from applying algorithms to raw data), and then using the resulting information to manipulate the behavior of the targeted individual, through advertisements or spam<sup>29</sup> emails, for example (Clarke 1988; Degli-Esposti 2014). Most citizens do not know that their ostensibly innocuous and seemingly irrelevant personal information is collected by undetectable devices and then used to target and manipulate them (Goodman 2015; Degli-Esposti 2014).

Data brokers and aggregators such as Equifax, Epsilon, Datalogix, Reed Elsevier, BlueKai, and Acxiom provide their clients with automated, real-time, tailored visibility of customers' and potential customers' predictable desires and behaviors (Goodman 2015; Talbot 2012). The price of these data is very low and is getting cheaper every day. For example, online data broker Docusearch sells personal information, including phone numbers, social security numbers, and bank account numbers for as little as one dollar (Angwin 2015). According to available information, Acxiom has an average of 1,500 data points on each of more than 200 million Americans, and Cambridge Analytica claims to have psychological profiles and 3,000–5,000 pieces of information for each of 230 million Americans (Boutin 2016; Funk 2016; Chessen 2017). “Those who collect and aggregate that data have an increased power to influence and even coerce our behavior—possibly through social shaming and financial incentives and penalties,” but

---

<sup>29</sup> Spam is unsolicited email with hidden or false information aimed at selling products, phishing, distributing spyware or malware, or attacking organizations. Personalized email advertisements are often phishing expeditions.

the “expansion of online networks that are connected to physical systems and that even control their operation, has dramatically expanded the ability of malign individuals to interfere with the physical world” (Chertoff 2018, 17). Well-armed with a deep understanding of their target’s likes and dislikes, predilections, vulnerabilities, and financial capabilities, criminals are in a superior position to persuade, manipulate, and defraud older Americans who, like everyone else, want to be able to make informed and reasonable decisions.

### **Data Brokers’ Use of Consumers’ Data**

A study of nine major data brokers showed that companies comply with the federal requirement to submit a privacy assessment of the data they collect, which is in line with the spirit of the Fourth Amendment of the US constitution and the UN General Assembly’s resolution on The Right to Privacy in the Digital Age (FTC 1996). Most companies follow their stated privacy practices because they collect personal data with the consent of the individual user. Social media companies such as Google and Facebook acquire consent by requiring the user to click to accept the terms of service before using their services. This legalese usually indicates some degree of privacy but often permits corporations and organizations to collect data about individuals. The terms of service usually comprise several dozen lines of small print describing the legal rights and protections of both the user and the corporation. According to Goodman (2015), Facebook’s privacy policy in 2005 was 1,004 words long; by 2014, it was 9,300 words long. The 2019 privacy policy admits that Facebook doesn’t charge users but adds that “businesses and organizations pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think will be relevant to

you and your interests. We use your personal data to help determine which ads to show you” (Facebook 2019, para 3). While this innocuous sounding agreement provides a user—who is about to consent to the collection of their personal information before using the “free” site—a sense of comfort from the legal rights and protections afforded them, in reality they have just given the company permission to use, reproduce, and monetize all of their information (Goodman 2015; Angwin 2015). What most consumers did not know about is the option to use Facebook Connect, where users can conveniently log onto other sites using their Facebook credentials, which also gives Facebook, and hence its advertisers, insight into the users’ internet use and websites visited. In addition, through mergers and acquisitions, Facebook has gained the ability to know everything about the user, including the facial recognition from uploaded videos, personal health through fitness trackers, emotional triggers, likely voting preferences, and buying habits (McNamee 2019).

Personal information is an important currency in the new millennium, and the consumer is really just a commodity (Schwartz 2005). Goodman (2015) found that Facebook’s service agreement allowed the company to change the terms and conditions of the agreement at any time without additional permission from, or notification of, users. For better or worse, Americans trust corporations.

As Angwin (2015) pointed out in *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, people want to be connected as well as to be able to judge companies’ and new online acquaintances’ trustworthiness, and they often make decisions regarding trust based on the number of acceptances or recommendations obtained from other online friends. In other words, for some online

users, someone who is trusted by others may be considered trustworthy. This confidence in others is a key component of social relationships, whether within or between groups, family, and friends. However, trust is foundational for more than social relationships: it is also crucial for business survival and conveys confidence in a corporation's integrity, capabilities, and intentions (Covey 2006). With over 200 data brokers collecting, analyzing, manipulating, storing, and selling personally identifiable information, Americans are placing a great deal of trust in institutions they most likely do not know exist. For example, Equifax, as a data aggregator, failed to protect consumer information. This negligence affected almost 44% of American citizens, who have no say as to whether their personal information is collected, stored, shared, sold, or—in this case—made public. In fact, “Equifax and third parties leveraged the aggregate data in complex psychographic and demographic big data algorithms to predict microscopic and macroscopic aspects of individual consumers and entire groups to assess the credit value of individual consumers and inform decisions about whether they were responsible enough to receive credit, borrow money, or take out mortgages” (Scott 2017, 6).

According to the Consumer Financial Protection Bureau website (2018), consumer reporting agencies such as Equifax have detailed information on individuals including, but not limited to name, nickname, social security number, telephone numbers, current and former addresses, all credit accounts (current and closed), account balances, payment history, creditors' names, civil suits, liens, date of birth, and place of birth. Following the Equifax breach, criminals may also have the ability to make decisions about how to use the personal and financial data of 143 million Americans. The Consumer Financial Protection Bureau, created in the Dodd-Frank Wall Street Reform and Consumer

Protection Act<sup>30</sup> stemming from the 2007–8 financial crisis, is charged with protecting consumers from credit card, investment, and other financial abuses. Both the Consumer Financial Protection Bureau and the Federal Trade Commission (FTC) have a mandate to protect American consumers and, as such, Equifax, the Consumer Financial Protection Bureau, the FTC, 50 states, and all US territories reached an agreement for a settlement plan (JND 2019). Equifax agreed to pay \$575–\$700 million to help compensate consumer losses (FTC 2019).

### **Legal Consequences**

Whenever it becomes known that a corporation was a negligent data broker, was unethical, or pursued illegal practices, the result can be tragic for the company and usually perturbs US financial markets. For example, on May 1, 2019, Robert A. Feuer filed a lawsuit in the State of Delaware against Mark Zuckerberg, Sheryl Sandberg, six other top Facebook executives, and Facebook, Inc. as a nominal defendant. This almost 200-page case filed in the Court of Chancery of the State of Delaware alleges a breach of fiduciary duty and insider trading in that the defendants caused “substantial, ongoing and escalating harm to Facebook” through “deceptively” downplaying the significance of the violation of trust by intentionally selling access to almost 90 million users’ private data, failing nominal security practices through the exposure of unencrypted users’ passwords, and the sale of stock prior to billions of dollars of market value losses (Leonard 2019, para 6; para 10).<sup>31</sup> The filing of this case occurred only one week after the FTC

---

<sup>30</sup> Pub. L. No. 111-203, 124 Stat. 1376 (2011).

<sup>31</sup> Feuer v. Zuckerberg, Docket 2019-0324-JRS (Del. Ch. 2019).

announced a fine of around \$5 billion for Facebook for violating a consent decree requiring better privacy safeguards (Leonard 2019).

The cases of companies such as Enron, Tyco International, Adelphia, and WorldCom, which were found to have committed fraud through corporate accounting practices, helped trigger congressional passage of the Sarbanes-Oxley Act<sup>32</sup> to quickly instill investor confidence in corporate accountability and responsibility. While the act helped to quell the public's concerns, it did not prevent Bernie Madoff from fleecing his fellow investors. The act is an example of what G. K. Chesterton (1905) referred to when he said, "When you break the big laws, you do not get freedom; you do not even get anarchy. You get the small laws." In other words, despite the hurt inflicted, the potential exists for future perpetrators to inflict harm because the legal measures to mitigate the crime do not adequately address the problem.

Thanks to confidence in corporations' and the government's capabilities, ignorance of security practices, and lack of concern with security, older Americans, like Americans generally, have adopted and continue to adopt many forms of technology. Yet few understand how the use of the technology may contribute to their own victimization. There are a wide range of cyber-enabled victim-complicit crimes, including investment fraud, confidence and romance scams<sup>33</sup>, business fraud, utility scams, state and federal government scams, charity scams, and product nondelivery. Among the types of crimes recounted in the IC3 annual reports are nonpayment for or nondelivery of a product, identification theft, romance cons, charity scams, lottery and advanced fee swindles,

---

<sup>32</sup> Pub. L. No. 107-204, 116 Stat. 745 (2002).

<sup>33</sup> A scam is a "fraudulent business scheme or a swindle." *American Heritage College Dictionary*, 4th ed. (2016) s.v. "scam."

Internal Revenue Service scams and other service scams, and fake investment schemes. These crimes are successfully committed because unwitting individuals made a decision that involved sharing an asset such as information or money.

### **Behavioral Economics**

The internet provides fertile ground for perpetrators who induce unwitting victims to give them money or important data such as passwords, bank account information, medical insurance numbers, or access to other personal information (Whitty 2013). Even worse, the gradual loss of cognitive capability, often unperceptively slow, may contribute in the victim's inability to detect lies, which conceivably makes individuals more disposed to gullibility and nefarious exploitation (Rankin et al. 2009; Nunes et al. 2010; Castle et al. 2010). However, wrong or bad information can mask any individual's ability to discern between what is real and what is not real and lead to a potentially bad decision (Seife 2015).

The ability to influence, even manipulate, the behavior of the targeted individual is recognized as an intentional desirable practice (Degli-Esposti 2014). Good marketing is based on knowing and meeting customer needs. The Stanford Persuasion Lab's "welcome to the lab" greeting posted on its website boasts that the purpose of the lab and its extended courses is to "create insight into how computing products—from websites to mobile phone software—can be designed to change what people believe and what they do" (Fogg n.d.). In Fogg's (1997, 6) dissertation, "Charismatic Computers," he proposes that people should "feel positive about themselves, positively about the interaction with the computer, and demonstrate behavior change in the direction advocated by the computer." B. J. Fogg understands the relationship between incentives and rewards and

how “computer applications could be methodically designed to exploit the rules of psychology in order to get people to do things they might otherwise not do” (Leslie 2016, para.9).

Criminals understand human desires, frailty, and fear of embarrassment as they tailor the scam to appeal to specific groups or individuals (Perri and Brody 2011). These criminals prey on emotions and ingratiate themselves knowing these older citizens are commonly alone, lonely, have free time, and have a retirement income (Long 2008; Mitnick and Simon 2002). Investing time to build trusting relationships with older citizens can reap great financial rewards. People tend to trust others whose ideologies or interests match their own, which the perpetrators of scams use by building trust relationships as they pretend to be members of the same identifiable racial, religious, professional, age cohort, or ethnic group as their victims or to have the same leisure interests as their victims. Unfortunately, there is no requirement for organizational affiliation or identification on social networks, and membership anonymity of online social groups creates conditions that are ripe for manipulation by criminals who may know everything about their target: marital status, financial ability, living conditions, religion and religiosity, interests, empathy toward or against a given issue, and consumer preferences. As an example, after the 2016 presidential election, the special counsel investigating Russian interference in the American electoral system, Robert Mueller III, charged 13 Russian nationals with trying to illegally influence the election. In addition, the indictment claimed that the defendants and others created hundreds of social media accounts to generate “political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social

movements.”<sup>34</sup> The indictment filed in the District of Columbia stated that the creation of “thematic group pages on social media platforms” addressing a “range of issues” had amassed “hundreds of thousands of online followers” (para. 34). The time required to establish the special kinship that exists normally within affinity groups is lessened when one party knows significantly more about the other (Perri and Body 2012).

Akerlof and Shiller (2015) discuss how fraudsters exploit individuals using both psychology and information in order to persuade the potential victims to do what they, the fraudsters, want. There are two types of psychology employed by criminals. The first type is emotional, in which emotions overpower common sense. The second type, cognitive bias, refers to unconscious inferences or distorted social reality that leads the victim to make irrational or illogical decisions (Akerlof et al 2015; Haselton, Nettle, and Andrews 2005). Information manipulation simply means information that is intentionally designed to mislead the victim, which can alter the perception of what is real (Akerlof et al 2015; Seife 2015). This sets the table for the criminal to defraud the unwitting yet complicit victim.

All Americans may be equally and innocently subject to manipulation and deception. For example, posing as Verizon employees, hackers who knew that John Brennan, director of the Central Intelligence Agency, used Verizon services tricked a real Verizon employee through social engineering into providing Brennan’s personal information in 2015. Having obtained enough of Brennan’s personal information, the hackers were then able to convince the AOL systems administrator that they were really Brennan, proceeding to reset the director’s personal password (Perez, Kopan, and

---

<sup>34</sup> United States v. Internet Research Agency, 18 USC. Supp.2371,1349,1028A;1:18-cr-0032-DLF (D.C. 2018).

Prokupecz 2015). Once the hackers had full access to the director's personal account, they were able to troll through the system stealing personally sensitive information (Zetter 2015). Naturally, the company, the administrator, and the victim were all concerned about how the crime was perpetrated, how to mitigate any fallout from the exposure of content, and how to prevent future occurrences. The strength of the hackers' professed authority and perceived honesty was sufficiently convincing to the system administrator to allow a cyber-enabled and politically embarrassing crime that spanned three days. The Federal Bureau of Investigation (FBI) receives hundreds of thousands of cybercrime complaints every year, but this high-profile hack received great interest and resulted in the arrests of a British teenager, Kane Gamble, and two Americans from North Carolina, Justin Gray Liverman and Andrew Otto Boggs of the Crackas With Attitude group (Turton 2016; Paganini 2017; Kumar 2018).

In addition to targeting Brennan and several other government officials, law enforcement agencies were targeted by the group, including James Clapper, then director of the Office of National Intelligence (Sterling 2018). According to the Eastern District of Virginia affidavit in support of a criminal complaint and arrest warrants, from October 2015 until the arrest of Gamble in February 2016, Crackas With Attitude successfully used anonymizing tools and social engineering techniques to gain access to and take over (jack) victims' online accounts, including Twitter, Facebook, email, and control their television channels. Members of the group asked about spouses and advised one victim that they (hackers) "will keep a close eye on your family, especially your son!" They followed this by posting a photo to the hijacked<sup>35</sup> system of the victim's son (Kumar

---

<sup>35</sup> To hijack is to seize control of something without permission or authorization and use it for one's own purposes. *The Free Dictionary*, s.v. "hijack," accessed March 18, 2018, <http://thefreedictionary.com>.

2018). Calls made to Director Clapper’s cell phone were diverted to the Free Palestine Movement (Sterling 2018). In 2015, WikiLeaks made the victim’s personal information available. Personal data like that belonging to Director Brennan are “golden nuggets” in the arsenals of criminals who use information and communication technologies to target, harass, and even threaten potential victims.

### **Reanonymizing Data**

Criminals’ research about their victims may be accelerated by illegally obtained data, data made accidentally publicly available from breaches, and purchases of legally aggregated data. Even data that have been anonymized, such as survey or aggregated data (e.g., internet service provider user preference or cable television viewing habits), can be added to other data and put individuals at risk of fraud. Under a grant from the US Census Bureau and the H. John Heinz III School of Public Policy and Management of Carnegie Mellon University, Latany Sweeney, and later Philippe Golle of Palo Alto Research Center, discovered it takes very little effort to identify an individual from anonymized data (Sweeney 2000; Golle 2006). A significant amount of research relies on anonymized data from organizations such as insurance companies, hospitals, and schools. These data, combined with seemingly innocent demographic data and other publicly available information—such as records of home sales (which include the prices of homes), home values, ethnicities, zip codes, voter registration and marriage records—significantly improve the ability to identify an individual. Ohm (2009) points out that data are either totally anonymized or are useful, but it is impossible for both to be true. The false assurance of anonymized data jeopardizes every American’s privacy and financial security.

## **Purpose of the Study**

This qualitative study of cyber-enabled financial abuse examines the social, economic, and policy attributes of the mechanisms whereby individuals fall prey to abuse. The goal is to highlight where intervention may help close the gaps in the complex cyber ICT policies and laws that place older American citizens at risk for financial insolvency, loss of independence, or degraded quality of life (Kaufman, Oakley-Brown, Watkins, and Leigh 2003).

## **Conceptual Framework of Cyber-Enabled Elder Financial Abuse Theory**

The conceptual framework (figure 1) is the logical structure of connected concepts that illuminates how ideas relate to one another within the theoretical framework and provides a general representation of the relationships involved in cyber-enabled elder financial abuse, including the relevant policies and laws. Many research theories have been applied to studies of financial abuse involving technology, influence, persuasion, social engineering, and crime. While the routine activities theory is not the center-post of the cyber-enabled financial abuse theory, it helps identify the three factors required for a crime to occur: motivation, opportunity, and absence of a capable guardian (Cohen and Felson 1979; Grabosky 2001). Cohen and Felson introduced the routine activity approach in 1979 as an approach for analyzing the cycles and trends of crime rates, and they argued that structural changes in activities could influence crime rates (Cohen and Felson 1979). The confluence of necessary activity elements—motivation, opportunity, and lack of capable guardianship—in time and space enables a criminal event and “the absence of capable guardians can lead to large increases in crime rates without any increase or change in the structural conditions that motivate individuals to

engage in crime" (Cohen and Felson 1979, 604). Routine activity theory refers to the customary work, family, and leisure activities in an ecosystem that exposes an individual to various situations advantageous to criminals. Hollis-Peel, Reynald, ban Bavel Elffers, and Welsh (2011), however, claim there exists a need for clarification of how guardianship is defined, what it involves, and how it transpires, as there is a lack of empirical research and evidence regarding the relationship between guardianship and lower crime levels. While not all characterizations of what may be considered capable guardianship are known, in this paper capable guardians are neighbors, social workers, law enforcement officers, and laws.

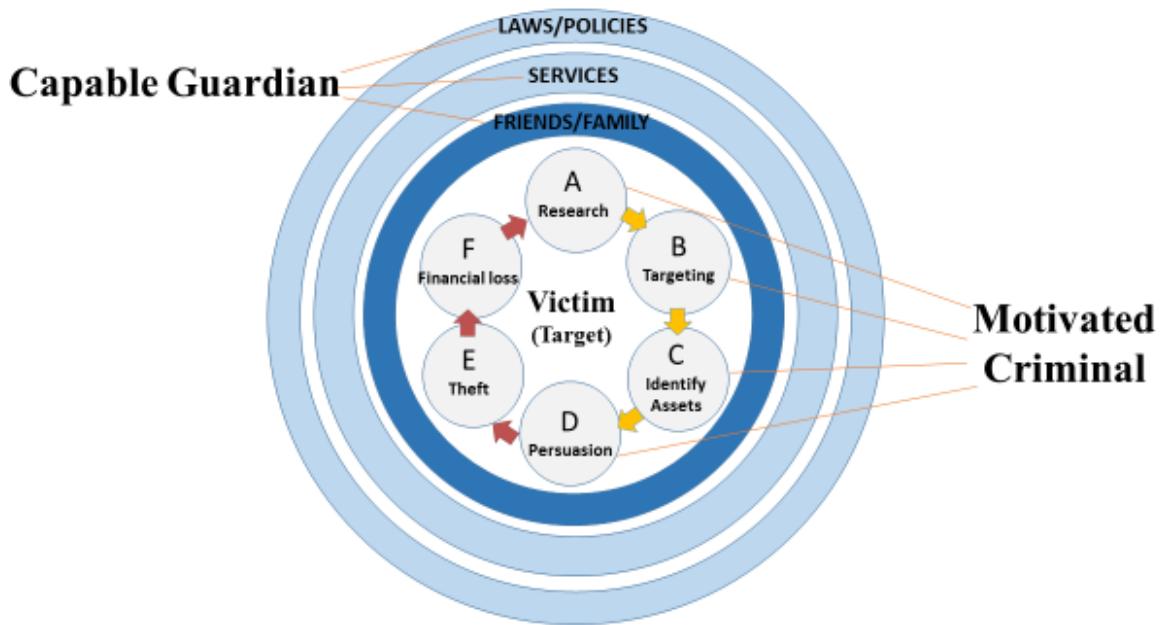


Figure 1. Conceptual framework

In the conceptual framework the motivated criminal conducts research and targeting of the potential victim to identify the potential victim's assets with the intent to persuade the victim to give away the assets; in this way the potential victim becomes the victim of theft. This theft, however, is due to the victim's own action, despite the victim being surrounded by people and services intended to act as capable guardians, including

laws and policies, adult protective services, financial and bank officials, and family and friends.

### **Theoretical Framework**

The theoretical framework outlined in figure 2 is the basis for analyzing and understanding the relationship among and between older Americans, cybercriminals, laws, policies, and senior services. A social structure of family, services, and policies and laws endeavors to protect older citizens against criminal behaviors that begin with criminal intent and proceed to financial abuse. Figure 2 depicts cyber-enabled financial elder abuse theory using the process-tracing theory-building methodology. This methodology has three stages. The first stage requires the explanation of key theoretical concepts, frequently employing deductive reasoning to derive new theory from existing literature. The theoretical concepts, represented by variables, indicate the possible underlying causal mechanisms among the variables. The second stage infers the existence of the underlying causal mechanism, which is often obtained from evidence that was not necessarily obvious. In the third stage, a link between the indicators and variables helps to build the theory, which in this case concerns cyber-enabled elder financial abuse.

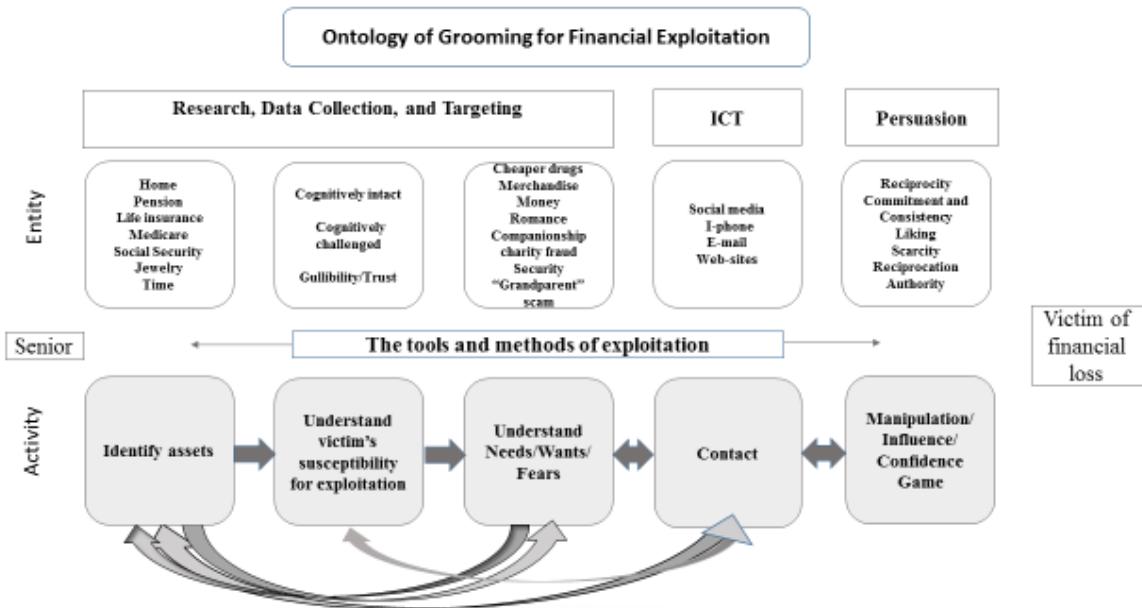


Figure 2. Theoretical framework

According to Beach and Pedersen (2013), process-tracing mechanisms are composed of entities (nouns, in this case ICT, needs/wants, cognitive function, assets, and manipulation/persuasion) that are used in activities (verbs, in this case researching, targeting, understanding, and manipulating) by an actor, which in this study is the criminal. These entities and activities comprise each part of the hypothesized causal mechanism of cyber-enabled elder financial abuse that turns a self-sufficient older citizen into a victim. More than variables, mechanisms are theories about how and why one event contributes to another event. Together these mechanisms represent the causal factors that lead to victimization. Every situation of exploitation is different; the path to victimhood is not necessarily direct, nor does any given variable have more weight than another. While the process may be generalizable, varying levels of intensity within and among the variables means each case is individual and does not allow for generalizing.

## **Grooming of the Victim**

While cyber-enabled financial abuse may have reduced physical dangers compared to other types of elder abuse, social media and the internet present risks for seniors not unlike the many well-known risks experienced by children and teenagers (Shulman 2007). The grooming techniques for financial fraud are similar to the cybergrooming used for the purposes of sexual exploitation of a child, in which perpetrators establish a trust-based relationship using computer-mediated communication. (Wachs, Wolf, and Pan 2012). Craven, Brown, and Gilchrist (2006) conducted a review of the theories and literature related to sexual grooming of children and found that theories of abuse often fail to consider the grooming process. In the case of this study, the abuse is financial. The range of means of abuse spans investments, product sales (e.g., drugs and beauty products), federal government scams, charity requests, and romance. The most relevant contribution to this study by Craven, Brown, and Gilchrist (2006) is their refined definition of the term *grooming* as it applies to a process. While their definition is specific to attributes of child sexual grooming, the applicability of the definition to the process of cyber-enabled financial abuse of older Americans—a process by which a perpetrator prepares a potential victim for abuse—is important. Specific goals include gaining access to the individual, gaining the individual's compliance, and maintaining the individual's trust to avoid disclosure. This process serves to strengthen the offender's abusive pattern and may be used as a means to continue the abuse and justify the offender's actions.

When an adult victim unwittingly contributes to their own victimization, it is difficult for the victim to fathom how they could “allow” themselves to be complicit. The

misplaced trust in an email from a charity, an online drug company, a tech help offer, an online dating service, or a supposed creditor who claims to be owed money can lead an older victim to unquestioningly provide credit card or banking data to a cybercriminal. However, the grooming process can be very complex. Theory building, a process-tracing methodology, helps to tie together the seemingly disparate factors and articulate the process of cyber-enabled elder financial abuse (Beach and Pedersen 2013).

Process tracing is a qualitative research methodology that provides the ability to identify interacting causal mechanisms as well as relations among these contributing mechanisms. To help orient the theoretical framework, the study borrows previous research conducted by Anna Burgard and Christopher Schlembach in which there are three phases (Burgard and Schlembach 2013). The three phases begin with the victim getting hooked on to the scam through an increase in interest and a decrease in any skepticism. Once hooked, the perpetrator develops the trust relationship, with the victim staying attuned even as they express concerns about the lack of product or the promised lottery winnings not being delivered. Zak (2017) provides possible insight into this desire to remain hooked or attuned via the body's release of natural oxytocin, a powerful hormone associated with positive social bonding, when a person feels trust. Following these phases of the victim's detachment from rationality, the victim tries to make sense of the ambiguity, fix the situation, and eventually must reengage with what the researchers referred to as *social reality*. This is the cooling out phase. During the cooling out phase (reality and return to normality) the body may release the hormone epinephrine, which is associated with stress and a racing heartbeat (Zak 2017). Victims often want to retain or regain the feelings associated with positive social bonding. Whitty's (2013) research

regarding criminals' ability to persuade victims in an online dating romance scam focused on criminals' ability to build trust in romance schemes. The study revealed the fraudsters' ability to keep individuals engaged, and sometimes reengaged, through several stages of victimization—all while the victim willingly sends money. To provide insight on scams, Whitty (2013) developed a model, the scammers' persuasive technique model (figure 3). In this study, Whitty (2013) examined various techniques criminals used in the online dating/romance scams. One important aspect of the model, the grooming process, is the focus of this study and the development of the ontology of financial abuse grooming, specifically the cyber-enabled grooming process to commit fraud against older Americans.

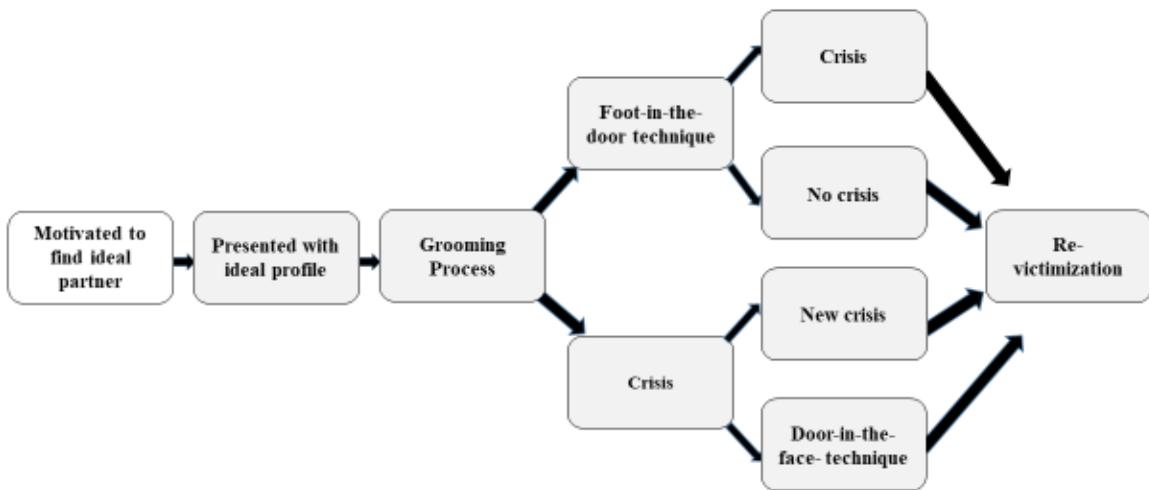


Figure 3. The scammers' persuasive technique model developed by Monica Whitty  
With consideration of the work by Burgard and Schlembach (2013) and Whitty (2013), the model depicted in figure 3 uses the process-tracing method to explore the relationship among a variety of factors that lead a senior to become a victim. This study explored aspects of the virtual or cyber environment that contribute to victimization and conducted a descriptive exposition of the associated fraud, elders, and technology laws and policies. Since cybercrime, cybersecurity, elder abuse, and financial exploitation

policies span multiple political, economic, international, legal, and moral or ethical dimensions, this study endeavored to focus only on the most salient policies.

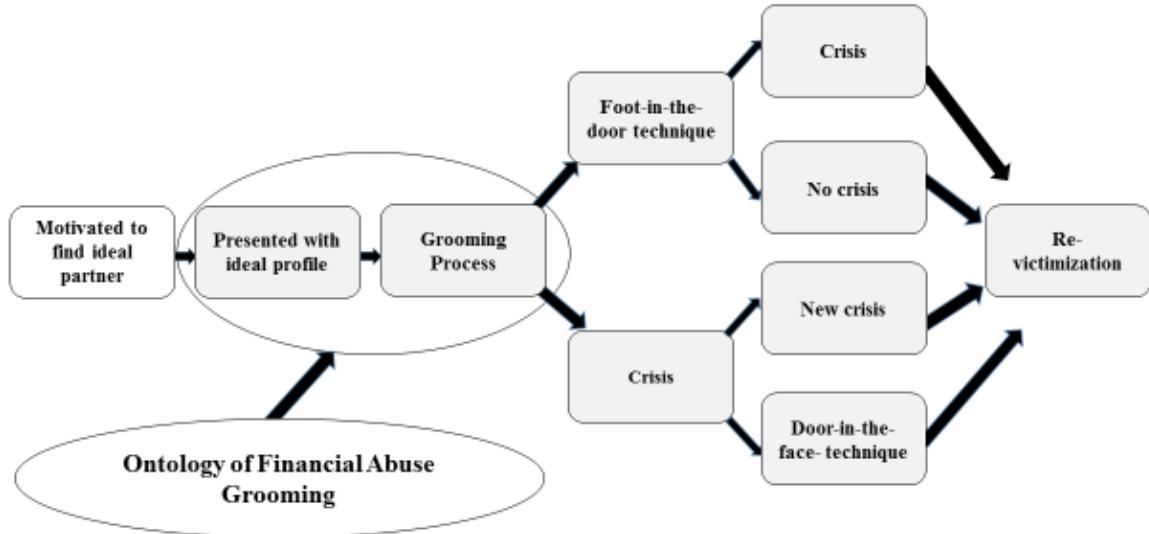


Figure 4. Integration of the ontology of financial abuse grooming into the scammers persuasive technique model

A brief overview of the ontology of financial abuse grooming follows in the literature review, along with an in-depth discussion of the roles of ICT, victims, perpetrators, and manipulation or persuasion. In the process of grooming the potential victim, the criminal collects information on the target using ICT to obtain data on the underground market, from data aggregators, by tricking the target to provide information, or a mixture of all three. Based on data, the criminal understands the needs and wants of the potential victim and the potential victim's propensity to fall for a scam. Knowledge regarding the value of personal assets of the target is readily available from various credit agencies and the underground market. The criminal uses ICT as a tool with which to manipulate the target into becoming a victim.

## **Review of the Literature**

The purpose of this chapter is to identify and analyze the literature relevant to the research question: How are cyber scammers so successful against older Americans? This requires an examination of information and communication technologies (ICT), cybercrime, and elder laws that either protect or mitigate the outcome of cyber-enabled financial crime. A review of the literature highlights the opportunity for a holistic approach aiming to understand the interconnectivity of the apparently disparate factors and to examine the lacunas in governance and policy that contribute to cyber-enabled elder financial abuse.

Socially constructed problems, which are inherently multidimensional, are often difficult to address. From a policy perspective, addressing cyber-enabled fraud is made more challenging by how quickly technology changes, precisely what occurs, the ephemeral nature of cyber, and society's use of technology. While governments encourage ICT use, governments also struggle with the effectiveness of the laws and policies governing use and security of these technologies. This study endeavors to avoid partisan or politically spawned policy debates, which are often caused by implementation differences rather than differences in ideology. However, the differences do form a basis for robust discussions that illustrate benefits sought, concerns over inequities, and complexities with both significant social and financial implications. While these debates slow the policy process, they also help to mitigate the enactment of poor policies caused

by a sense of urgency. However, the extended process often yields outdated and, therefore, seemingly feckless policies.

The current literature focuses predominately, at least quantitatively, on the financial impact of cybercrime on the general American population. Little qualitative research has sought to understand the process of convincing someone to actively participate in his or her own victimization or the laws that take a toll on older Americans. While there has been some scholarly investigation and research regarding the impact of financial abuse, there continues to be very little understanding of the scale of internet-enabled financial abuse perpetrated against older citizens. In this study, grey literature<sup>36</sup> is used to help develop the understanding of the effects of cybercrime on society and to complement peer-reviewed journal articles, public and private sector publications, and academic literature.

This literature review ties together several streams of work: (a) ICT and data aggregators, (b) the victim as a decision maker, (c) the perpetrator, and (d) governmental policy and law addressing cyber and older Americans.

### **Information and Communication Technologies**

The internet has evolved from homogenous hardwired systems to networks to wireless virtual connections on the world wide web supported by disparate security regimens. Internet 1.0 connected computers and supported data transactions via computers, credit card processors, and web-enabled services (Aston 2016). Internet 2.0 connects people for the purposes of data sharing via mediums such as smart phones and

---

<sup>36</sup>The Grey Literature website defines grey literature as literature produced “on all levels of government, academics, business and industry in print and electronic formats, but is not controlled by commercial publishers.”

social media, but Internet 3.0 will connect everything and will leverage the advantages gained from big data collection and analysis to provide autonomous data-driven decisions (Aston 2016). Connections small and large—from pacemakers and smart home appliances to power distribution centers—all have operational data that traverse the internet. Today there are billions of devices connected to the internet: 20 billion devices are expected to be connected by 2020, and 50 billion are expected by 2025 (Daniel 2017). However, this exponential growth in the dynamic power of technology over the last five decades has not been and is not matched by efforts to develop security (Williams 2015). In addition, the technology developments have outpaced the development of laws and other governance structures.

The lack of central internet control means that cybersecurity is often reliant on the decisions of users, whether those using the internet in their personal lives, businesses, or governments (Coyne 2004). While frequently conflated, the web and the internet are distinct entities. The internet is a complex, interwoven network of networks comprising billions of devices in communication with each other, and the web is a means of accessing information riding on the internet. These devices connect by means of internet service providers (ISPs) to network access points and then to the internet. While there is no overarching network for controlling the internet, network access points act as the highest level of the network on which applications ride.

The use of computers to communicate was a far-fetched idea described in the 1968 article “The Computer as a Communication Device,” yet the ability to instantaneously communicate, as well as collect, process, store, and transmit data, was thought to become a “boon to humankind . . . beyond measure” (Licklider and Taylor

1968, 40). Their groundbreaking work at the Advanced Research Projects Agency helped to connect computers in a way that spurred research in biotechnology, communications, transportation, and so on. Not unlike the Morse code scheme of dits and dahs (long and short), a computer's basic unit of data is a one or zero, and these bits (binary information digits) are grouped together and sent over the wire or ether in packets. The growth of ARPANET (the Advanced Research Projects Agency network) allowed researchers on subnetworks to connect one to one and one to many via email.

Tim Berners-Lee conceived the idea of the world wide web in March 1989 in an attempt to provide a way for researchers to share data at the European Organization for Nuclear Research, or CERN (Haque 2015). The intent was to retrieve information using a new technology, hypertext, via the internet. Berners-Lee's fundamental drivers were decentralization (no censorship or surveillance), nondiscrimination (net neutrality), and universality (computers speak the same language for maximum participation) using common standards. The web is the most popular network application for accessing and sharing information. A webbed together accumulation of files, text pages, and videos located on one computer or server is essentially a website.<sup>37</sup> A browser (e.g., Microsoft's Internet Explorer, Google's Chrome, Mozilla's Firefox, or Apple's Safari) is a software application that, while not technically required, helps in the access, retrieval, and viewing of information from websites. The user types in the actual address of the file or website and the browser delivers the document to the device's screen. Another means of information retrieval is a search engine, like Google, Bing, or DogPile. Though a search

---

<sup>37</sup>A website is a set of interconnected webpages, usually including a home page, generally located on the same server, and prepared and maintained as a collection of information by a person, group, or organization.

engine is not required to access data, a search engine makes finding information easy as it “crawls” through the web sorting and filtering millions of pages in order to retrieve relevant requested information to the user’s device’s screen. Each time this process occurs and the search engine retrieves information, it creates a copy of visited web pages and indexes them to expedite future searches. Several search engines not only collect and retain these data but also collect data on the person making the request. This user information is collated into user profile records.

Conceptually, the web has three levels, which may be described in nautical terms. The first is the surface web, where users connect to static or fixed pages (Iffat and Sami 2010). Google, Yahoo, Twitter, Amazon, and Wikipedia are examples of applications that enable users to surf pages on the web. Though search engines maintain indexes of the various files resident on servers connected to the internet, they catalog only a fraction of the information on the web. The surface web is both accessible and indexed.

The second level is the deep web, which, according to Goodman (2015, 254), is “500 times larger than the than the surface web,” with data quality about 2,000 times greater (Bergman 2001). On the deep web, dynamic pages and content reside in databases that are available by registration, paid subscription, or some type of recognized credential (Iffat 2010; Goodman 2015; DARKOWL 2016). The databases of the deep web contain government data, patient medical records, private network data, academic and specialized journals, corporations’ financial records, personal bank account data, customers’ private credit card information, and information from corporate intranets. The data stored here are accessible, usually with authorization, but are not indexed.

The third and lowest level of the web is the dark web, dark net, or the digital underground, which also rides on top of the internet (DARKOWL 2016). Access to the dark web requires special browser software and sometimes other specialized tools like Tor (The Onion Router). The intention of Tor, which the US Navy developed, was to protect intelligence communications (Goodman 2015). The navy gave Tor location concealing and anonymity capabilities to help international dissidents and encourage free speech. The intent was and is to protect users' personal information, privacy, and ability to communicate from the threat of surveillance. However, dark web activity is heavily focused on maintaining anonymity for illegal purposes such as anticensorship, political activism, hacking tool exchange, illicit drug sales, money laundering, and sales of personal information. Tor encrypts traffic and passes it through a series of Tor nodes to mask the source's internet protocol (IP) address. The software enables privacy and security on the internet via a virtual private network. Other software has similar abilities to enable anonymity by concealing users' locations and communications, but Tor is the most widely used anonymity tool with a dark web connection.

Even elementary school students hide their locations or real IP addresses by using proxies. A proxy server is a tool to transnavigate a firewall in order to directly access a forbidden website. The request for access to a website is sent to the proxy server, which in turn contacts the desired website and retrieves the requested material. The reason proxy servers are used is because the IP address identifies where the computer user is located. If the computer is located in a public library, a foreign country, or a business, the user may be blocked from accessing certain content. A proxy server allows online activity under a different IP address without switching ISP. The request travels from the

user to their ISP to the proxy server and then to the final destination. The proxy uses the IP address set up via one of several websites that provide free proxies. There are benefits as well as dangers to using proxy servers. For example, a transparent proxy will still provide the user's IP address; a distorting proxy identifies itself as a proxy yet sends an incorrect user's IP address; an anonymity proxy identifies itself as a proxy, but does not identify the user's IP address; and a high-anonymity proxy does not identify itself or the user's IP address. Anonymity tools provide a variety of services, such as chat and web access. Companies often use proxies for security reasons; however, criminals often use malicious proxy servers. Unfortunately, anonymity and location concealment also helps cybercriminals hide. In the underground, data are an important currency.

The years 2006 to 2008 were witness to what amounted to the beginning of a technological revolution. Social networks such as Facebook and Twitter became mainstream during this timeframe. Steve Jobs's smartphone, the Apple iPhone, combined the ability to make a telephone call, view videos, listen to music, and have on-demand access to the internet anywhere (Friedman 2016). AT&T has been continuously working toward a more software-centric network using the cloud as both storage and transport, which supports the greater demand created by the smartphone revolution. VMware enabled multiple operating systems to run on one computer, while Hadoop made big data available for everyone (Friedman 2016). During this timeframe, the e-reader Kindle, the electronic cash system Bitcoin, and IBM's Watson were launched (Friedman 2016). These technologies combined, with a myriad of others, enabled users to consume information, create content, and socialize; it also allowed users to inject into these

activities persuasive false data in order to influence the decision-making of others (Chessen 2017).

Data make up a new and important asset. Data are so important that data sets are now considered philanthropic donations. As an example, the United Nations (UN) uses its Global Pulse initiative to gain insight into the conditions that affect human lives. Started by the secretary general in 2009, the initiative's collected and analyzed data enable the UN and its global partners to tackle hard problems and implement innovative solutions (Kirkpatrick 2013). This UN initiative seeks to engender a socially responsible partnership between the public and private sectors to exploit the full potential of big data for the benefit of all societies (Kirkpatrick 2013). In other words, data philanthropy helps transform big data in to a public good (Kirkpatrick 2013). In industry, data are transformed into information as they are processed from collection to analysis to distribution. Kirkpatrick (2013) understands that to gain the cooperation of data holders, the initiative will need to maintain both competitive equities among stakeholders and privacy. Alan Westin (1976) claims that this is where the importance of understanding privacy versus confidentiality is imperative. According to Westin (1976), privacy is the balance between the legitimacy of requiring personal information and the individual's need to control disclosure of that information, whereas confidentiality concerns the law of privileged communications or how data are collected, stored, and used by an organization.

The lack of privacy afforded to the normal internet user is an important contributor to the financial system that flourishes underground. Information is collected, bought, sold, traded, and gathered via numerous means. There is a delicate and intricate

relationship among the entities that have a level of connection to the settings of cyber-enabled fraud: the technology industry, social media and data companies, the US government, and US citizens. Kirsten Martin's (2016) research makes a strong argument for the web content owners, data aggregators, and supply-chain managers to responsibly collect, store, and share information. Users falsely place trust in the terms of service proffered by the ISPs, online stores, or other customer-facing entities (Martin 2016). Terms of service and terms of use agreements underpin the legal relationship between the service provider and the individual. While terms of service provide a user about to consent to the collection of their personal information before using a "free" site a sense of comfort from the legal rights and protections afforded them, in reality they are about to give the company permission to use, reproduce, and monetize all of their personal information (Goodman 2015; Angwin 2015). Meanwhile, the user is encouraged to add personal information in the form of preferences, social connections, and private thoughts in order to be fully part of the social network (Buchanan 2011). Goodman (2015) found that Facebook's service agreement allowed the company to change the terms and conditions of the agreement at any time without notification of, or additional permission from, by the user. The result, according to Silverman (2017), is that the private lives of citizens have become more transparent while corporations and their surveillance activities have simultaneously become opaque. This became evident when it was revealed that Facebook allowed Cambridge Analytica and Aleksandr Kogan access to individuals' posted data and privately sent messages in order to target them with personalized advertising (Gonzalez 2017; Hern and Cadwalladr 2018).

Additionally, research demonstrates that personal data may be leaked during transmission, usage, or storage (Spiekermann, Acquisti, Bohme, and Hui 2015). Martin (2016) categorized entities in the information chain into four types of actors based on breadth of information and type of relationship. Entities with strong customer interfaces are online stores and web portals. Hidden from the user are the behind-the-scenes information processors, like data aggregators—who have broad abilities to collect, track, store, and sell consumer information—and advertising networks, which have limited but specific information (Martin 2016). The difficulty for the consumer is the inability to know what information is collected, how it is stored, to whom it is sold, and with what other offline data it is combined. Martin (2016) refers to this ability as being akin to surveillance of the individual.

Network typology studies expose a hydra-headed system of criminals who rarely, if ever, meet in person and are usually only known by one of their aliases (Secretary of State for the Home Department 2010). Cyber criminals meet in internet relay chat<sup>38</sup> rooms, on web forums, or in other internet-supported social media locations (Secretary of State for the Home Department 2010). These technologically savvy criminals conduct their trade over ICT and, whether called computer-related crime, cybercrime, digital crime, or internet crime, it is a growing global phenomenon (Sela-Shayovitz 2012).

The social media phenomenon's reach has transformed the way that society interacts and the speed of that interaction. Social media is a web-based technology application that enables users to connect, collaborate, and socialize online; it is a place

---

<sup>38</sup> Internet relay chat is a method of broadcasting and receiving live, synchronous messages. There are hundreds of separate networks globally, hosted on servers, where people with the same interests communicate. Internet relay chat is similar to text messaging but enables large groups of users to communicate (George Mason University Website 2019).

where users are able to create public profiles, display their social connections, and search for other connections within the confines of a given environment such as Facebook (Boyd and Ellison 2007; Fuchs 2017). The user's created profile is a web page consisting of personal information and photographs about hobbies, family, and other interests. The profile enables the user to link to other users' profiles, thereby facilitating a virtual meeting. The social structure created via these affinity groups produces a social network site, and while communication helps shape human behavior, social media is shaping the way humans communicate.

Joseph Walther termed the category of communication that supports interaction among people over digital technology *computer-mediated communication* (Griffin and Ledbetter 2012). Computer-mediated communication is facilitated by the internet, the underlying technologies of which support a variety of social media such as social networks, blogs, podcasts, instant messaging, and other forums that connect users globally (Kaplan 2009). Walther's original research reflected the traditional communication model of sender-receiver-channel-feedback, which he extended to include the dynamics of computer-mediated communication. Computer-mediated communication may occur between physically proximate locations; however, most of these conversations occur without any face-to-face meeting and lack the intrinsic understanding afforded by nonverbal cues and body language (Griffin and Ledbetter 2012).

Walther's other theory, social information processing, underpins the understanding how of people engage and develop affinity with one another in a computer-mediated conversation as users' communication behavior adapts to technology

(Griffin and Ledbetter 2012). A study conducted by Dai et al. (2016, 365) found that computer-mediated communication is as effective as face-to-face communications as the communicator's self-disclosure enriches the intimacy of the relationship; in fact, "what enhances online relationships and psychological well-being could be a cathartic result of self-disclosing, regardless of how one's online partner responds." The relationship continues to be further enhanced when the communicators endorse each other's messages and connect with a perceived depth, making nonverbal communication irrelevant (West and Turner 2018). When one of the communicators "reveals" personal information, that "revealing [of] personal information is a gesture of trust" (Dai et al. 2016, 397).

While the telephone, Skype, and Facetime are forms of real-time communication; voice mail, texting, Facebook, and email are asynchronous, affording senders the opportunity to carefully curate the quality of messages. This enables senders (possibly criminals) to present themselves in positive ways that serve as the basis for relationships. A receiver processes and evaluates a message's content by relying on minimal cues and risks idealizing the sender by overestimating the similarities between sender and receiver (Griffin and Ledbetter 2012). "The relatedness of the content" in the communication creates a "perception of a bond between the participants" and "people who compliment others can be perceived as more attractive because the recipient of the compliment feels obligated to like the complementor" (Dai et al. 2016, 398). Walther refers to this as channel management: the receiver relies on perceived information in the channel. When the receiver reciprocates with a reinforcing confirmation message, the sender's expectation of the receiver's acceptance is sustained.

## **The Perpetrator**

Gary Becker, sociologist and winner of the Nobel Prize for Economics, researched and wrote extensively on the theory of crime, rational actors, and punishment. Becker (1993) pointed out that criminals are rational actors who respond to incentives and weigh the benefit of committing a crime against the risk of being caught and, if caught, the severity of the punishment. More specifically, Becker (1993) stated that the economic and social environment created by public policy, including expenditures on police and potential punishments for crimes, help criminals determine the value of committing their crimes. The anonymity online and the ephemeral nature of online data contribute to the attractiveness of crime committed in cyberspace.

The internet's sanctuary of obscurity and facelessness allows global, well-organized, underground economies to flourish, often with elaborate trade relationships (Franklin and Paxson 2007; Aransiola and Asindemade 2011). In addition, this underground has benefitted from trusted digital currencies, like Bitcoin. Even when an entity's activity is disrupted, it often reappears in another manner to revictimize a person or defraud more victims. These underground businesses have very favorable returns on investment with little chance of punishment, making fraudsters rational, albeit sinister, actors.

## **Classifications of Cybercrime and Cybercriminals**

Cybercriminals fall into various groups that are associated with a type of crime, the target victim, and the professional or technical prowess of the perpetrator. Jonathan Lusthaus (2013) claims cybercriminals may be organized but asserts that there are significant problems in labeling cybercriminal actions as organized crime in the

traditional sense. From Lusthaus's perspective, the overarching organized crime characteristic is governance, and he offers three high-level components of this governance in which sources of power and resources highlight the differences.

First, traditional organized crime uses violence to control and regulate members, and research indicates that cybercriminals appear to lack similar tools other than denial of service or virtually taking over an ICT asset<sup>39</sup> (Lusthaus 2013; Chickowski 2014). The second crucial organized crime trait is control over territory (Lusthaus 2013). While Lusthaus's research does not find evidence of cybercriminals maintaining control over a territory, Brian Krebs (2014) provides several examples of cybercrime turf wars. One of those chronicled by Krebs (2014) was the partnership "gone bad" between two Russian spammers, Igor Gusev and Pavel Vrublevsky. After years of running a very successful online illicit pharmacy business that spammed email inboxes and lured unsuspecting clients into buying ineffective or sometimes lethal drugs, the two parted ways and became competitors. Eventually, the competition turned ugly, with each applying a new twist to what traditional organized crime elements did to ruin the competition. They used the media and law enforcement to try to incarcerate one another and, in effect, stop the one other's businesses. Vrublevsky spent some time in prison, while Gusev and his family quickly moved from Russia to an undisclosed location (Krebs 2014).

The third challenge regards the resiliency of the group's alliance. In this regard, researchers have had difficulty finding verifiable data to help determine whether cybercriminals' activities are compatible with the historical categorization of organized crime (Lusthaus 2012; Holt et al. 2012; Decary-Hetu, Morselli, and Leman-Langlois

---

<sup>39</sup> Ransomware is one form of service denial by which a computer, server, or collection of data is hijacked until a fee is paid or a debt is settled.

2011). Alternatively, there is evidence that when an organization of cybercriminals falters, the lucrativeness of hacking and spamming results in the cybercriminals eventually reconnecting with others and reconstituting their business endeavors, indicating a level of resiliency (Krebs 2014). In addition, Lu et al. (2010) studied the social networks of cybercriminals and found that there were cybercriminal networks that showed cohesion and resiliency.

The nature of organized crime and the disparate international approach to organized crime offers an additional challenge to defining organized crime and distinguishing among types of cybercrimes and criminals. Jay Albanese's (2012) research contributes to the understanding by delving into the similarities and differences between organized crime and transnational crime. From his assessment, perpetrators of organized crime and transnational crime exhibit the same behaviors (Albanese 2012). Thus, cybercrime is a domestic problem as well as an international concern.

There are two major types of borderless organized crime: international crime and transnational crime (Albanese 2012). International crimes are large-scale acts committed against civilian populations, including murder, genocide, enslavement, war crimes, and acts causing great suffering (often referred to as *inhumane acts*) that may or may not have a financial component and include persecutions based on political, ethnic, cultural, racial, or religious grounds. International organized crime tends to be ideologically driven, may involve more than one country, and may or may not have a financial component (Albanese 2012). Nation-states' cyberattacks against other nations to steal defense secrets, steal employee data, steal industry secrets, steal money, or inflict harm to

computer systems to interrupt the functions of government are usually considered international crimes (Martinez 2013).

According to Matiasek (2012), there is not a universally accepted definition of transnational crime; however, this study uses the definition from the National Security Council's website (2014, para 1) definition:

Transnational organized crime refers to those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures.

Cybercrime is normally for financial gain, and transnational crime always involves at least two countries (Albanese 2012). According to Clough (2014), even when the perpetrator and the victim are in the same country, the cyberevidence of the crime will often travel through other countries. A UN study showed over 80% of cybercrime is committed by organized criminals, and more than half of those responding to the study reported between 50% and 100% of cybercrimes were transnational (United Nations Office on Drugs and Crime 2013).

Albanese (2012) groups transnational crimes as depicted in table 1.

Table 1. Classification of transnational crimes

Class	Examples
Provision of illicit goods	Drug trafficking Stolen property Counterfeiting
Provision of illicit services	Human trafficking Cybercrime and fraud Commercial vices (e.g., sex, gambling)
Infiltration of business/government	Extortion and racketeering Money laundering Corruption

*Note:* Developed by Jay S. Albanese (2012).

If the perpetrator, the victim, or the computer systems involved are located in at least two countries, the crime is transnational. According to Albanese (2012), cybercrime and fraud are classified as provision of illicit services.

Joel Best and David Luckenbill's typology for identifying the social organization of deviant<sup>40</sup> associations facilitates understanding of the organization of cybercriminals and is shown in table 2. Best and Luckenbill list five categories of deviant organization characterized by four variables of social organization: association, participation, division of labor, and extended organization. The categories of deviant organization are loners, colleagues, peers, mobs, and formal organizations. Loners do not participate with or associate with other deviants. Colleagues have a social relationship with each other and perform the same activities, but act alone. Peers participate in the same kind of work and associate with one another. Mobs, or groups, share in the work with an intricate division of labor. Aransiola and Asindemade (2011) found that Nigerian scammers, also known as

<sup>40</sup> Best and Luckenbill define deviance as “any behavior that is likely to be defined as an unacceptable violation of a major social norm and elicit strong negative reaction by social control agents.”

*Yahoo boys*, helped one another when working with difficult “clients” and worked with the local banks in order to cash Western Union checks that exceeded the normal number an individual would normally receive in the course of a month (Aransiola and Asindemade 2011). Formal organizations are the most complex as they have the ability to extend outward over time (Best and Luckenbill 1982). However, the financial underground is supported worldwide, with communities of cybercriminals manipulating millions of dollars garnered from victims in the well-organized underground marketplace where high-functioning business is conducted through an interconnected financial web supported by credit cards, bank wire transfers, digital currency, and electronic money transfers (Franklin 2007; Hutchings 2009). According to Best and Luckenbill (1982), the more sophisticated the division of labor among an organization’s members, the greater the structure of the organization and the probability that the deviant behavior will be systematic.

**Table 2. Best and Luckenbill’s (1982) characteristics of social organization of deviants**

Organization	Mutual association	Mutual participation	Division of labor	Extended organization
Loner	No	No	No	No
Colleague	Yes	No	No	No
Peers	Yes	Yes	No	No
Mob (group <sup>a</sup> )	Yes	Yes	Yes	No
Formal organization	Yes	Yes	Yes	Yes

<sup>a</sup>Group is not original to Best and Luckenbill’s classifications.

The original hackers were often considered computer “nerds,” evoking a vision of an introverted, socially incompetent loner without a social life. However, cybercriminals often share information and data freely and form partnerships with mutual association (Meyer 1989). Cybercriminals associate with one another, but usually perpetrate alone

(Broachurst 2014). A key component of Best and Luckenbill's (1982) characteristics of relationships among colleagues is the ability to perform alone. For Best and Luckenbill (1982), mutual participation requires the perpetrators to concurrently offend in the physical presence of one another. However, in cyberspace virtual presence has physical connotations.

Alkaabi, Driscoll, Gabaix, and Laibson (2011) provide greater granularity to help security professionals, policy makers, and law enforcement accurately identify and report cybercrime by introducing a cybercrime typology. Classifying all crime committed using a computer as cybercrime is a disservice to those trying to understand the severity, frequency, or impact of a particular crime, as not all cybercrimes are equal. The tragic online bullying of a child who eventually commits suicide is very different from an I LOVEYOU virus, which in turn is very different from the exploitation and unauthorized use of someone's personal data. The typology shown in table 3 classifies cybercrime into two types of crime, each with subclasses, and allows for organization, some clarity regarding units of analysis, trend analysis, and potentially advancing means of countering crimes (Holt 2013).

**Table 3. Cybercrime typology of Holt (2013)**

Type	Role of computer/network	Subclasses
I	Target	Unauthorized access (hacking) Malicious code (worms, viruses, denial of service, botnets)
II	Tool used to commit crime	Content (child pornography, intellectual property theft) Unauthorized alteration of data or software for personal gain (online fraud) Improper use of telecommunications (cyber bullying, stalking, spamming)

Gordon Meyer (1989) examined the social organization of the computer hackers' underground. His graduate thesis showed that hackers during the 1980s were colleagues who shared information in a loose socially networked organization, even when the means of obtaining that information were illegal or ethically questionable (Thomas 2005). The hackers displayed organizational characteristics found in other groups that transformed to become criminal in nature (Meyer 1989). One of those characteristics is the use of pseudonyms or "handles" as identities in the underground as one means of preventing discovery by law enforcement. Law enforcement, policy makers, and ethical hackers were struggling with this new mode of crime in an attempt to define and distinguish between activities that were unintentionally malevolent and those that were intentional, malicious, criminal behavior.

The hacker ethos and culture began to change in the late 1980s. The major reasons for this transformation had to do with the increase in computer security, a change in society's tolerance for hacking behaviors, and the arrest of more well-known and nefarious hackers. By the 1990s, criminal behavior started to cause significant damage. In 1994, Russian hacker Vladimir Levin transferred approximately \$10 million by fooling or co-opting Citibank's computers. He gained access by stealing passwords from Citibank customers when they used their personal identification numbers (Public Broadcasting System 2001). This particular theft involved both telecommunications and the internet, but eventually these two communication paths converged when telecommunication companies merged these separate yet interrelated media technologies into one digital operating platform. This convergence of communications complicated law enforcement's capabilities, since previously internet activity was accomplished over a

telecommunications-enabled modem and could be traced back to a telephone's physical location. In 1996, Timothy Lloyd, a dismissed system administrator, left a "bomb" that sabotaged his former company's system and cost the company nearly \$10 million (PBS 2001). Kevin Mitnick, now an author and cybersecurity consultant, was rearrested in 1999 for gaining access to a computer across state lines when he stole computer files from Sun Microsystems and Motorola (Mitnick and Simon 2002). In 1999, David Smith unleashed the virus he named Melissa, which spread widely and caused over \$80 million in damages at more than 300 companies (Haury 2012). In August 2000, 15-year-old Canadian Michael Calce launched a denial-of-service attack that brought down the websites of CNN, Amazon, Yahoo, eBay, Dell, and E\*Trade at a cost of \$1.2 billion (Gross 2011). Bragging on an internet relay chat room led to Calce's discovery. There is not one kind of cybercrime or cybercriminal, and some of the noted actions of early hackers give the false impression that the computer underground community is full of antisocial loners (Broadhurst 2014). By the early 2000s, these criminals were replaced by a financially-driven criminal hacking culture (Broadhurst 2014; Gross 2011). That does not mean finances are the only drivers. There are hackers who look for a challenge, want political gain or increased hacker reputation, have a bent toward destruction, or simply hack for the fun of it (Raymond 2000; Howard 1997). For transnational organized crime, however, the unifying goal is profit.

While the European Cybercrime Center's (2018) *Internet Organised Crime Threat Assessment* refers to members of organized crime not as gang members but as members of organized crime groups, Spamhaus (2018), an organization committed to eradicating spam, claims there are approximately 100 persistent, organized spam gangs.

Research does indicate that the internet underground consists of individuals who reside within a loosely connected macrocriminal network who help each other to improve capabilities and raise productivity (Broadhurst 2014). Strong hierarchical structures of traditional gangs are supplanted by a federation of knowledgeable and technically skilled members who come together for a one-time or many-time exploit (Smith 2015).

Cybercriminals are stakeholders in the underground community and derive benefits from the relationships they build with one another. In these cyberorganizations the pseudohierarchical leadership role is based on how technically skilled and connected to others in a network an individual is. Those who are highly skilled play a central role in the network. Tightly connected players have an important responsibility in the network, a phenomenon also suggested by other studies of criminal social network analysis (Easton and Karaivanov 2009; Schwartz and Rouselle 2009; Lu et al. 2010). According to Smith (2015, 104), while there is no persistent gang membership, there is “a complex management and organizational structure” for very seasoned and highly technical exploits. The more sophisticated organizations will have high levels of complexity in the division of labor, coordination among roles, and tenacity in pursuit of goals (Best and Luckenbill 1982). Smith (2015) notes the skills needed by cybergangs are more technical than those needed in traditional crime organizations and usually don’t require face-to-face confrontation. Membership in cybergangs, however, can be as ephemeral as the data that passes over the internet, with little loyalty between members (Smith 2015).

The cybercriminal organization is similar to other business ventures, with segmentation of processes and functions along business lines. Lusthaus’s (2013) research shows cybercriminals use forums or underground marketplaces to buy and sell illicit

goods and services. Criminals often advertise and trade products such as stolen credit card data, stolen identifying personal information, or malware (see note 13 on p. 7). These forums have a division of labor, with specific roles that specify who has administrative charge of the website, who enforces rules, and so on. (Lusthaus 2012). Cybergang members are recruited for their expertise and exploits (Brenner 2002). While there are numerous names and roles for both general and specific functions, Shadowcrew provides an illustrative example. Shadowcrew was a global, complex, highly structured, yet decentralized organization that was involved in—among other things—illicit credit card sales and identification theft (Lu et al. 2010). The US District of Massachusetts's sentencing memorandum noted a well-orchestrated operation that spanned two continents with individuals in the United States, Ukraine, and Estonia. The list of retail victims was extensive and included NASDAQ, Dow Jones, TJX, BJ's Wholesale Club, Barnes and Noble, Forever 21, JCPenney, 7-Eleven, Boston Market, and the payment processing company Heartland. Each member of the organization played a defined role: Christopher Scott breached the wireless access points of retailers to obtain card data, Humza Zaman laundered \$400,000–\$600,000 of profits, Stephen Watt coded the key computer hacking program (a packet sniffer), Jeremy Jethro wrote the zero-day exploit to gain access to and redirect computers, Patrick Toey breached networks and sold card data, Ukrainian Maksym Yastremskiy was a card hacker who stole over 40 million card numbers, and Estonian Aleksandr Suvorov sold the stolen credit cards.

For most underground markets, a potential cybercriminal marketer must offer evidence of a skill level, show trustworthiness, and be vetted by another member in order to enter even on a trial basis (Davis 2014; Lusthaus 2013). The administrator or

moderator decides who may be part of the forum. Cybercriminals advertise professional services and offer various products. Cybercriminals even provide consulting services for the products they sell (Smith 2015). These black-market sites provide private environments for cybercriminals to communicate with other cybercriminals. Conversations may occur in covert internet relay chat rooms or in “darknet” private networks where trust is realized by the stability of the relationship between the two parties. The relationship starts out with total anonymity, and the cybercriminal builds an online identity to attract partners and clients.

Decary-Hetu and Dupont (2012) studied hackers’ social networks and found a paucity of real technical skills for many of the members of the hacker community. Specifically, there are few hackers with the necessary skills to create tools, techniques, and software that is complex enough to conduct systematized attacks against a diverse set of systems (Holt 2012). Unlike the earlier years of hacking, today’s hacker community relies on the ability to buy a “desktop” tool online, while some look for the opportunity to learn from the more skilled hackers through educational forums (Gross 2011).

Cybercriminals help colleagues advance their skills and provide advice and guidance to neophytes (Holt 2012). As the unskilled gain talent, they are able to expand their proficiency at skills necessary to engage in attacks and earn respect for their skill, even when the exploit requires only basic computer skills (as in the Equifax breach<sup>41</sup>). The hacker’s reputation is important, as a good reputation is critical for a malware writer to sell his or her wares and make a profit (Holt 2013).

---

<sup>41</sup> Senate Comm. on Homeland Security and Governmental Affairs, Permanent Subcomm. on Investigations, *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach*, S. Rep. Hearings Cong. 115<sup>th</sup> (March 6, 2019).

Products are offered by those who are technically savvy enough to write software, often referred to as coders, writers, or hackers, to produce Trojans, viruses, worms, phishing<sup>42</sup> tools or customized bot<sup>43</sup> services (Lovett 2007). While it is a secretive community driven by the necessity to reduce detection by law enforcement, success brings status and profit. Therefore, criminals exercise a carefully orchestrated balance between advertising to a wide audience and maintaining privacy. Hackers' reputations are associated with their pseudonyms or handles, which are how they identify themselves online and advertise their malware on the online black market. As Holt et al. (2012) pointed out in their study of the hackers' and writers' social networks, this is a meritocracy-based community where skill and ability are respected. DarkMarket, an underground market for items like stolen credit cards, had over 2,000 members who knew each other only online when the organization was shut down in 2008, yet each "knew" the others by reputation (Davis 2014). Reputation, as in all businesses, is key for future business.

As on eBay, sellers are rated for the quality of the product and their trustworthiness. Unlike on eBay, sellers are also rated for their technical prowess. The moderator arbitrates members' ratings and statuses. The administrators and moderators

---

<sup>42</sup> Phishing is a method of committing credit card fraud, identity theft, or generic theft. Phishing attacks use "spoofed" emails and fraudulent websites designed to deceive the recipients into divulging personal information such as credit card numbers, account usernames and passwords, social security numbers, and so on. Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials by deceptive means. Technical subterfuge schemes plant crimeware onto personal computers to steal credentials directly, often using systems to intercept consumers' online account user names and passwords and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes) (Anti-Phishing Working Group 2012).

<sup>43</sup> A bot, or web robot, is a software application that runs automated tasks over the internet. A malicious use is the takeover of one or several computers for coordinated and automated attacks on other networked computers. A spambot is a bot that spams large amounts of content onto the internet, mostly in the form of advertisement links.

mediate disagreements among members and are often paid a percentage of the profits from sales (Lusthaus 2013). To help to sustain the forum's viability and increase market share, administrators and moderators mimic legitimate escrow companies and provide third-party enforcement for online transactions (Davies 2014). For the more sophisticated organizations, the cyber underground market offers other services, such as means for exchanging e-money into real money or bulletproof connections to the internet (Krebs 2014).<sup>44</sup>

According to Trend Micro (2014), cybercriminals have increased the use of social engineering and phishing attacks, and today these cybercriminals are organized to conduct their work on a global scale without consideration of nationality or borders. As noted by Lu et al. (2010) in their research on criminal hacker social network analysis, defense in the cyber environment is behavioral, not technical, in nature. Technically savvy and intelligent, these cunning criminals are unscrupulous risk takers without concern for the victim or the law. There are several methods of snaring victims. One is buying lists of potential victims who are most likely to be vulnerable to scamming. The other is using botnets<sup>45</sup> and other technologies to spam emails out in a wide net to see who responds. Once someone expresses an interest in a business deal, charity, or romance, the criminal is able to study their target by culling through the potential victim's biographical data—easily purchased on the underground market or hacked from unsecured computers and servers. Criminals then process the profits from the sales through banks worldwide (Kramer 2013). Denial of service, sale of fake antivirus

---

<sup>44</sup> Bulletproofing is a service provided by an ISP that has obtained some level of political or legal protection and ensures the internet connection will not be terminated (Krebs 2014).

<sup>45</sup> A botnet is a network of bots, which are software applications that run automated tasks.

software, ransomed computer access, threats of revealing embarrassing harvested information, and even threats of violence against family members are some of the tactics that are becoming commonplace. As of February 9, 2018, Spamhaus claims the top ten world's worst spam-enabling countries are the United States, China, Russia, Ukraine, Japan, Hong Kong, the United Kingdom, India, Turkey, and Brazil. Spam has enriched Russian criminal gangs by as much as \$60 million a year (Kramer 2013).

Cormac Herley (2012) authored a compelling argument regarding how the internet fraudster maximizes profit while maintaining low expenses. While seemingly obvious, the Nigerian email offering immense returns for a small investment is a scam that successfully draws in the naive. A 2010 Symantec study showed that 89% of the internet email volume is Spam (Symantec 2012). This cheap broadcast method snares the unsuspecting or gullible to respond to the email offer with initial requests for trivial sums of money. For the con artist, requests for small amounts of money help avoid a bank or other financial institution triggering a Bank Secrecy Act report.<sup>46</sup> As Western Union discovered in 2017, failure to have an effective anti-money-laundering program is a very expensive (\$586 million) lesson (Hudak 2017). The continuous need for revenue requires the fraudster to develop personal relationships with victims as well as a steady stream of new, profitable victims; therefore, staying under the radar is key for maintaining a steady flow of money. Cybercriminals are sophisticated enough to obtain millions of dollars from victims each year in an elaborate, well-organized marketplace with refined trade relationships (Franklin 2007). To do this, fraudsters seek and sell private information in

---

<sup>46</sup> A monetary instrument log is created when an individual purchases a negotiable instrument such as a money order, cashier's check, or traveler's check with a value between \$3,000 and \$10,000. An international transportation of currency or monetary instruments report is generated when more than \$10,000 is transferred out of the country.

the underground economy (Hutchings 2009). This business model is part of the underground market and requires relatively small amounts of the cybercriminal's personal time until the prey sends money (Herley 2012). While there is a cost to the criminal for doing business, false positives are reduced by conducting behavioral analysis of potential victims. Since each scam requires time and targeting has a cost, it is important for the criminal to ascertain who is not put off by the lack of poor communication skills or the ridiculousness of the email's content to which only the most likely target will respond or self-identify (Herley 2012).

Matsakis (2019) compares the value of seemingly innocuous personal data to the hundreds of organizations that collect and sell such data to that of oil. Consumers most likely do not know up front that that the DNA-testing results of the saliva provided to 23andMe may be sold to pharmaceutical firms or that the record of the minute pause made while looking at a product online will be sold to a retail store as a potential indicator of customer interest (Matsakis 2019). Smartphones collect and transmit data as customers stop in various stores or linger at particular displays, which retailers collect in store. According to Yael Grauer (2018), data brokers collect information from courts, motor vehicle agencies, credit card companies, social media sites such as Facebook, the census, state licensing agencies (e.g., marriage, professional, etc.), and voter registration. Data miners make sense of data by organizing and reformatting the analyzed information for resale (Hannigan 2017). While the Fair Credit Reporting Act places restrictions on data brokers, for the most part they remain unregulated (Matsakis 2019). Wolfie Christl (2017) found that companies influence consumers using their personal data by monitoring behavior and guiding them toward desired behaviors through subtle

psychological cues. Several of the data aggregator companies claim to deliver highly targeted messages that drive economically beneficial behavior; Borgesius and Poort (2017) claim that this allows for online price discrimination. These companies have “access to personal information . . . to ‘accurately’ discriminate between people in order to take advantage of them” (Christl 2017, 42). This personalized automated targeting is derived from the individual’s characteristics and behaviors and “may affect people’s choices and life-chances, and, on a fundamental level, their general autonomy and human dignity” (Christl 2017, 17). While Christl (2017, 42) acknowledges that there is no known company that takes advantage of consumer vulnerabilities, he claims that “data-driven decisions are discriminatory in the sense they use personal information and data mining methods in order to distinguish between people of certain groups.” Tristan Harris (2016), Google’s former human persuasion design ethicist and Center for Humane Technologies cofounder, writes in his online series of blog essays about how technology hijacks a person’s psychological vulnerabilities by controlling the availability of predetermined choices, providing a supply of instantaneous notifications (an interrupted person pays attention), encouraging users to give mutual social approval, and enticing users to spend significant amounts of their time clicking or scrolling on enticing visual images. Criminals are in this business too.

To maintain a stream of profitable victims, criminals sell victims’ information to each other, whether these data are obtained through personal contact with victims, heists similar to those perpetrated against Target, Home Depot, and the Office of Personnel Management, or by purchases from data aggregators in the well-organized underground marketplace (Franklin and Paxson 2007; Hutchings and Hayes 2009). Possession of a

victim's private information and anonymity on the internet embolden criminals to conduct high-functioning businesses through an interconnected financial web on the dark net supported by credit cards, bank wire transfers, digital currency, and electronic money transfers (e.g., Western Union). Until the Federal Bureau of Investigation (FBI) dismantled the DarkMarket, this particular transnational criminal organization had over 2,500 members across the globe who bought and sold financial data (Chabinsky 2009).

With a rich biographical understanding of the victim garnered through identity theft, purchase, or eliciting information directly from the victim, the fraudster uses his knowledge and the opportunity to manipulate the victim (Burgard and Schlembach 2013). Cybercriminals are emboldened by knowledge of the victim's private information and operate with absolute anonymity while maintaining an elevated level of functionality. Perpetrators exhibit several behaviors in the course of committing a cybercrime. One is to mine information on a potentially lucrative target to exploit him or her. When an individual uses a computer connected to the internet, a certain amount of information is left behind, often referred to as a digital footprint. Blogs and social web sites, such as Facebook, contain cookies and beacons<sup>47</sup> that can record information regarding users' viewing habits and interests. Search engines retain search terms, patterns of searches, page requests, and so on and leave a permanent record of where the user has been. Hackers have broken into numerous companies and sold stolen data, such as the account numbers of Target's customers, personal information from the Office of Personnel Management, or financial vulnerability from the Equifax. In addition, data aggregators sell personal data to other businesses. Once the aggregator sells the information, that

---

<sup>47</sup> A cookie is data sent between a website and a user's web browser regarding previous activity on the site. A beacon is used by a third party to monitor the activity of a site.

information is the property of the buyer, who can sell it again. All this is conducted without the knowledge of the person the information is about.

The various means of contacting unsuspecting prey include users opening one of the millions of daily botnet-issued spam emails coursing across the internet advertising medical products for male enhancement, necessary prescriptions, or weight reduction. These spam pharmacies frequently claim to be Canadian companies, but most likely are based in Eastern Europe, luring Americans who are looking for a means to save money. The products these pharmacies sell are often counterfeit or less than optimal, and these criminals simultaneously cheat patent-owning American companies out of millions of research-invested dollars (Kramer 2013). In fact, Lovett and Mackey (2013) found the online medical marketplace to be a prime area for what they termed *eElder abuse*. The combination of rising health costs and the ubiquity of the internet placed seniors at significant risk for counterfeit drugs as well as unverified medical procedures and testing (Lovett 2013). Cyveillance answered a 2010 National Institute of Standards and Technology query about cybersecurity challenges and the internet economy by warning of the lethal aspects of illegal online pharmacies. In their response, Cyveillance (2010) listed three overarching issues with online pharmacies: the high risk of harm or death due to the lack of appropriate medical oversight in the issuance of prescription drugs, the risk of unregulated drug production overseas or in facilities not approved by the US Food and Drug Administration, and the potential for counterfeit drugs that may contain harmful chemicals.

While there are dozens of crime types, the types of scam where the victim unwittingly complies with his or her own victimization include confidence fraud,

romance fraud, investment fraud (gold, diamond, or treasure), inheritance fraud, advanced fee scams, .419, lottery or sweepstakes scams, health-care scams, and government impersonation. Once an email recipient responds regarding a business deal or romance scam, the criminals combine their intuitive understanding of what drives people to respond with the victim's personal data to identify vulnerable pressure points for exploitation. This business model requires relatively small amounts of a cybercriminal's personal time until the prey sends money (Herlery 2012). For example, the Nigerian fraudsters, called *Yahoo boys*, often assist one another, especially with difficult victims (Aransiola and Asindemade 2011). Cybercriminals often befriend someone online and use them as unwitting money mules in the various countries to help collect and move money, thereby victimizing their "friends" if police become involved. While some victims fall prey due to a form of greed, many are manipulated through deception (Smith 2015).

The perpetrator lures the victim into wanting or needing a particular good or service, helping another in need, or avoiding something bad: in essence, they separate the victim from reality and transform the victim's sense of normalcy (Burgard and Schlembach 2013). As a result of their exploration of victimization processes, Burgard and Schlemach (2013) refer to the stages of the victimization as *getting hooked* and *staying attuned*, which are followed by a *cooling out* phase, or the return to some sense of normality for the victim. While the financial cost of victimization is high, the loss of a friend or romantic interest can be just as devastating or even more devastating. The sense of loss and the potential release of the body's epinephrine hormone often drive victims to

try to regain the special relationship, even when they know they were scammed (Whitty 2013; Zak 2017).

The investment scam may start with the offender sending an obvious, seemingly ridiculous request, such as that of a financial advisor looking for an investor, which allows the fraudster to segregate possible victims from nonvictims. Email addresses have been traded and sold since the 1990s, and the potential victim's interest may already be algorithm analyzed; therefore, when a large number of emails are sent, the target field is reduced to the possible addressable market and further refined by whoever responds to the email (Seife 2014; Herley 2012). For a potential "investor," the question may surround the fidelity of the advice. The information shapes the victim's thought process and decisions (Seife 2014). An investment email sent to 100,000 inboxes may yield 1,000 respondents; the financial advisor may give advice to 500 of the respondents that a specific stock will go up and to the other 500 respondents that the stock will go down. The 500 whose stock advice was correct may require more proof, and so 250 receive advice that a particular stock will go up, and the other 250 receive the opposite advice. The fraudster has reduced the addressable market to 250 potential "clients" to defraud. Only individuals who are interested respond to the spam email and, most likely, the email address was sold to the criminal as belonging to an individual who either is interested in or may be manipulated into being interested in an investment, charity, romance, or product (such as cheap, but necessary, prescription drugs).

Popular offers of assistance with computer technology to hapless users who stumble upon an email with a computer virus pop-up have garnered tens of thousands of dollars from the victims. Cybercriminals send emails that, once opened, alert the potential

victim to call immediately to take care of a serious computer problem. Once the user dials the given number, the criminal instructs the victim to type in a code that will clear the problem. The “problem” goes away, but the newly installed spyware stays. The victim unwittingly gave the scammer full access their computer. This begins a cycle of computer “freezes” and technical problems for which the cybercriminal demands payment.

### **Limitations of Law Enforcement**

Robert Hanser’s (2011) research demonstrates the federal- and state-level constraining parameters for law enforcement in searching for and obtaining forensic evidence. The more sophisticated the gang, the less likely law enforcement will be successful. This makes overseas gangs even less likely to be caught, because cybercrime’s “illegality is defined by the governmental jurisdiction in which the crime is conducted, not from where the attack was launched” (Smith 2015, 105). Aransiola and Asindemade (2011) conducted a study of the Nigerian cybercriminals who have formed one of the most successful cultures of financial fraud. Their investigation included 40 young undergraduate men between the ages of 22 and 29 years. The study chronicled the perpetrators’ business activities, which included cooperation of local security and bank officials and collaborating partners on all but one continent. These technically savvy entrepreneurial criminals send spam emails with offers of merchandise, romance, investments, advance fees, or lottery winnings (Aransiola and Asindemade 2011). The classic Nigerian email offers immense returns for a small investment, which often successfully draws in the unsuspecting. In Nigeria, most of the online transactions surround romance and the sale of fake merchandise. Asserting product expertise and a sense of product scarcity and urgency, criminals persuade victims into advancing

payment or fees for products that will never arrive (Chang 2008). While Ekman (1985) claims lying is a central characteristic of life, many people feel remorse, uneasiness, guilt, or even fear about lying or deceiving others (Ekman and Frank 1993). For most, the root of fear associated with lying is in being discovered (Ekman and Frank 1993; Vrij, Granhag, and Mann 2010). Bok (1999), however, found people who lie tend to have a self-benevolent interpretation of their actions or a self-identified moral reason for lying. They may even believe the lie as an acceptably valid story (Vrij, Granhag, and Mann 2010). However, fraudsters are information manipulators who rarely feel guilty about lying, and Aransiola and Asindemade's (2011) study revealed that Nigerian cybercriminals lack empathy for their victims (Vrij, Granhag, and Mann 2010). Guilt is akin to shame, and scammers or manipulators do not necessarily feel any shame in their actions (Bok 1999). According to Glenny's (2009) research, many Africans lay the blame for their corruption on Western culture, for a multitude of reasons ranging from invention of the computer to colonization. Some view their lying, deception, and scamming as means of redressing the decades of Westerners' exploitation of Africa (Glenny 2009). From the Nigerians' perspective, scamming is a way of equalizing past transgressions (Glenny 2009). In fact, Ekman and Frank (1993) claim that there is less shame or guilt for the criminal when the perpetrator and the victim do not share the same cultural or social values. In several African countries, including Nigeria, corruption is so vast and the citizenry so ambivalent that prosecution is fundamentally impossible (Oke 2014). While Nigeria is not the only country with online perpetrators, Nigeria does account for over 30% of dating fraud (Edwards et al. 2018). Nigeria, Ghana, Malaysia, South Africa, the

United States, Jamaica, Canada, Costa Rica, Israel, Romania, and Russia are among the biggest known perpetrators of online fraud (Stanger 2015; Edwards et al. 2018).

Since 2000, the Internet Crime Complaint Center (IC3), cosponsored by the FBI and the National White Collar Crime Center, has maintained a database of complaints to assist federal, state, and local law enforcement. In 2010, the IC3 managed over 25,000 complaints per month, referring many to law enforcement for additional investigation and prosecution. Pattern analysis of these seemingly disparate incidents provides investigators insight into the economic threat posed by high-tech cybercriminals who are emboldened by the anonymity of the internet. Acts of computer intrusion, denial of service attacks, and viruses and worms are acts of internet crime or cybercrime. Cybercrime includes the theft of another's resources through credit card theft, bank account theft, identity theft, intellectual property theft, extortion, money laundering, and technical subterfuge and social engineering (Anti-Phishing Working Group 2012). Only drug trafficking tops cybercrime as the fastest-growing illegal activity (Glenny 2009). Cybercrime, unlike other types of crime, occurs in virtual environments, spreads at astounding speed, and results in low prosecution rates owing to the ephemerality of digital fingerprints (Maurushat 2010). A substantial number of internet users believe that the government or their ISP provides internet security. Case law, however, does not hold ISPs or websites accountable for misdeeds of users, even though their proprietors may be best situated to regulate the actions of their users (Parker, Van Alstyne, and Choudary 2016). Internet users often unknowingly assume the risk, at least as far as US laws are concerned.

## The Victim

*The Wealth of Nations*, an early study of the nature of economics written by Adam Smith (1991), focused on human idiosyncrasies and social dynamics. Smith (1991) believed that as each person pursued his own interest he intentionally or unintentionally promoted the general good of society. An economic equilibrium occurs when an individual makes a decision that maximizes his or her own self-interest, such as a farmer deciding to grow wheat while others benefit from the resultant crops in the marketplace. Adam Smith's (1991) faith in his fellow humans' ability to make self-benefiting decisions assumes that everyone's decisions are rational, which is the foundation for classic economic theory (Ariely 2009). This assumes that the rational decision maker is imbued with consistent and logical means of determining the best possible action, including relevant and factual information.

Several Nobel prize recipients have contributed to the understanding of the specific effects of cognitive, emotional, psychological, social, and cultural factors on human judgment in financial decision-making, including Gary Becker, Herbert Simon, Daniel Kahneman, and Richard Thaler. Their contributions are often referred to as behavioral economics and are concerned with three overarching themes: heuristics, framing, and rational versus nonrational decision-making (Kahneman 2011; Simon 1997).

Kahneman's research into uncertainty showed a cognitive reason underpinning human decision-making errors due to bias and heuristics (Kahneman 2011). Heuristics are an individual's mental shortcuts based on memory or known references for reducing seemingly risky decisions. According to Tversky and Kahneman (1974), these include

representativeness (probability of occurrence), availability (bias due to imagining or remembering an occurrence), and adjustment and anchoring (a reference point).

Framing refers to how facts are presented so as to elicit a specific response. Kahneman and Tversky's (1979) prospect theory suggests that people display a risk preference contingent on how the opportunity is framed in terms of loss or gain; the individual's satisfaction changes as the size of the loss or gain changes. Individuals tend to exhibit an aversion to loss and thus are inclined to be more disposed to risk (Kahneman and Tversky 1979). Gains or losses are tied to the reference point: losses are below the expected reference point or level and gains are above the point or subjective expected utility (the decision weights). Utility derived from gains is often diminished when compared to the fear of loss, which is why individuals frequently engage in risky behavior to avoid further losses. Mishra and Fiddick's (2011) research found that individuals in negatively framed situations perceive themselves to be in high-need circumstances. In these high-need cases, people tend to set minimal thresholds for risky choices (Mishra and Fiddick 2012; Mishra, Gregson, and Lalumiere 2012).

While individuals may be best to decide for themselves, there are limits. Rational choice theory is based on the precept that the individual will make a rational utility-maximizing decision (Simon 1997). Herbert Simon (1997), a Nobel economist, applied his studies of human behavioral and cognitive processes specifically to human decision-making. He combined studies of economics and psychology to argue for the inability of humans to know all details, all alternatives, all possible consequences, and then compare and contrast the alternatives and consequences to arrive at a perfect decision. The boundaries of human capacity led Simon (1997) to proffer his theory of bounded

rationality, a theory rooted in the understanding of humans' cognitive limitations with respect to assimilating and analyzing data sufficiently. Simon's (1956) research into decision-making indicated that people often satisfice,<sup>48</sup> or make a satisfactory decision in a specific environment using known facts and cognitive capabilities. Satisficing embraces the notion that a decision is the best one given the context and the available information. Behavioral economics provides insight into decision-making, rationality, and the interplay of psychology and economics.

While people may make self-interested decisions to maximize their own welfare, Akerlof and Shiller (2015) argue that what people want and what people decide may be two different things. For example, some may want to have a financial nest egg in the bank yet give it away to charity as a sort of social exchange. The desire to be wanted and needed negatively affects decision-making when selflessness creates a situation of self-neglect, a form of elder abuse. This is true when a victim feels a true relationship exists and has a desire for the relationship (Cross 2019). This desire helps criminals convince people to give them money and possessions. Social exchanges include gift giving, romance, charity, and friendship, whereas market exchanges have a decidedly financial cost. According to Airely (2009), social exchanges are not only cheaper and more effective than market exchanges, they also motivate people and provide a sense of self-definition and self-worth. Airely (2009) found that market exchange—which is about money, products, and services—and social exchange have different norms, and people respond differently to these exchanges.

---

<sup>48</sup> *Satisficing* is a combination of two words, *suffice* and *satisfying*, and recognizes the model of rational choice that accounts for human behavioral characteristics in the economic model (Simon 1997).

Dan Ariely (2009) claims that humans are far from perfect decision makers and usually focus on the comparative benefit of one option over another. Retrospectively, a poor decision may easily be viewed as a poor decision; it is, however, often difficult to foretell that a particular evolving event may lead to a poor decision. Decision-making may be complicated by the context, the amount of data available, and potential outcomes, and it is made infinitely more difficult by questionable or unreliable information. Time spent online often helps combat loneliness, yet social media also has the potential to lead individuals to isolation in affinity groups and to what Angwin (2015) calls *false intimacy* in an environment with predatory actors.

Marketers, as well as fraudsters, look for ways to help decision makers depart from rationality, and studies in behavioral economics acknowledge the unconscious formation of decisions (Brooks 2011). Legitimate and spurious marketers use heuristic methods to attain their goals. One technique is priming, which is simply embedding an idea that unconsciously drives a person to a particular decision. Priming may spur a memory associated with a particular response; for example, the sound of running water may unconsciously make a person need to use the restroom. Anchoring is another tool based on the assumption that the amount of money a product “should” cost derives from previous exposure to the cost of that product. Decision makers compare products against the cost to find the “best value.” Shoppers often find it challenging to calculate the worth of various options, so most people take the middle option (Ariely 2009). Sellers know these mental comparisons are difficult, which is why stores carry very expensive, high-end products or very cheap, low-end products that don’t sell. According to Ariely (2009) the reason stores do this is to provide a point of comparison to make the product that the

store wants to sell seem reasonable and, therefore, desirable. Both legitimate and fake sales are often successful because the sale price is favorable compared to the original price. The preference of a decision maker may be influenced by how the product or opportunity is framed, which is a significant element in many studies associated with the theory of rational choice (Tversky 1986). For example, a product that has a failure rate of 15% is more appealing when it is advertised as having a success rate of 85% (Brooks 2011). However, Kahneman and Tversky (1982) found that people willingly made risky decisions when the perceived compensation was high enough. Research demonstrates there is little regret if a less-than-optimal decision is made under pressure or during a stressful time (Kahneman and Tversky 1982). Lea, Fischer, and Evans (2009) found criminals often use vividly emotional triggers to appeal to the victim. Unfortunately, an imbalance of economic equilibrium occurs when one person is made better at the expense of another, yet fraudsters are successful in their dedication to a customer making a decision that benefits the criminal. Thaler and Sunstein's (2008, 6) nudge theory highlights the role of behavioral economics in decision-making when nudging an individual alters their behavior in a "predictable way without forbidding any options or significantly changing their economic incentives." The thrust of nudging an individual is to influence their decision; however, it can also be a means of authoritarian manipulation or a route to compliance (Michalek, Meran, Schwarze, and Yildiz 2016).

### **Persuasion and Trustworthiness**

As social animals, humans establish, develop, and maintain relationships; this also underpins the nature of marketing relationships (Purkey and Novak 2015; Morgan and Hunt 1994). All relationships are built on trust, and relationship trust is a crucial

component for society's existence (Morgan and Hunt 1994; Covey 2006). According to Cross (2005), trust is not a binary decision, where an individual is either all trusting or all distrusting; it is a continuum developed through social relationships. General membership in an affinity group may short-circuit the perceived need for a prolonged process to establish a relationship. Commonly, relationships use accepted social norms for interaction with rules of acceptable and unacceptable behavior such as clothing versus nudity, speech versus hate language, and personal contact versus uninvited touching. Sometimes these rules in society are codified as manners, which, Margaret Mead (1975) remarked, are ways for people to tolerate one another. Unfortunately, scammers or fraudsters are also marketers who understand the relationship between the potential victim and themselves as well as the victim and the victim's customs. Neuroscientists Stephen Macknik and Susana Martinez-Conde (2011) researched the relationship of cognitive neuroscience and magic. Magicians, not unlike fraudsters, distract the victim so that the person cannot fully deliberate on a given issue (Macknik and Martinez-Conde 2011). They also use humor and empathy to disarm a target (Macknik and Martinez-Conde 2011). Fraudsters and magicians understand how the passage of time can make recalling facts accurately difficult, especially if the recipient heard what they wanted to hear and had no reason to object at the start of the discussion (Macknik and Martinez-Conde 2011). Lying is part of the magic show and life in general. In fact, "lying is such as central characteristic of life that better understanding of it is relevant to almost all human affairs" (Ekman 1991, 23). People tell the truth, conceal or withhold information, and lie; it is all part of the normal social fabric (Ekman 1985).

To trust is a decision an individual makes through conscious intellectual reasoning and analysis of the opportunity, risk, and credibility or competence of those involved (Covey 2006). Gullibility occurs when a person devotes little effort to analysis and is highly inclined to trust, but people who do not trust anyone have little social interaction (Covey 2006). Truth rests at one end of the scale, and lying, cheating, and deceiving are at the other end. While there are subtle differences in the definitions of lying, cheating, and deceiving, for the purposes of this research each receives the same treatment in meaning. A perpetrator lies, cheats, and deceives in order to commit a sham<sup>49</sup> or scam on a victim who has been convinced to trust the perpetrator. For centuries, the marketplace has been a place for social activity. It is the means by which goods are bought, sold, and traded and is a place where social interaction occurs. In recent decades, as the marketplace has moved into the virtual world, so has social interaction. Biases are inherent in the decision-making processes regarding the perception of trustworthiness. There is a tendency in our society to trust professionals such as doctors and distrust people outside of one's own known group or who are associated with a perceived risk (Hill and O'Hara 2006). The problem is being able to accurately process the level of risk in context. Laws provide safety nets—licensing of doctors, Food and Drug Administration drug approvals, and corporate accountability—but the government cannot replace a citizen's ability to process relevant information in the decision-making process to determine trustworthiness (Hill 2006).

Scammers understand the market as well as the need for social interaction. Whether offering a product, requesting a donation for a charity, or proffering a romantic

---

<sup>49</sup> A sham is “a trick or fraud. An imitation that is meant to deceive; counterfeit; deception; fake.” *Webster’s New World Dictionary*, 5th ed. (1967), s.v. “sham—(n).”

liaison, scammers are building relationships. According to Purkey and Siegel (2003), these relationships are developed and maintained by four foundational principles: intentionality, respect, trust, and optimism. Intentionality implies the individual acts with a purpose, which gives meaning to what is experienced in the relationship (Purkey and Siegel 2003). In the world of criminal deception, the criminal actor creates an illusion in which the victim is intentionally made to feel respected and optimistic. The criminal and victim develop a trusting relationship.

The victim experiences respect when they perceive they are valued and appreciated in a caring manner. Optimism focuses on the future and is based on two perceived probabilities: the probability of actually being able to achieve a goal or outcome and the probability of belonging to a group where meeting this goal is likely (MacInnis and Chun 2007; Roth and Hammelstein 2007). The victim is encouraged to join the effort to help achieve the outcome or goal. The euphoria generated by this optimism improves the sense of overall well-being and is key to a greater feeling of happiness (Rasmussen, Scheier, and Greenhouse 2009; Youssef-Morgan and Luthans 2015). A vital ingredient of a scam is for the victim to have a sense of hope. This positive emotion is comforting and may make the victim not only susceptible to deception by the scammer, but to self-deception by processing information in a biased manner because of the yearning for a specific outcome (MacInnis and Chun 2007). The more a victim desires an outcome, the greater the potential for information to be processed cognitively to support a strongly held or desired belief (MacInnis and Chun 2007). As though blind to the truth, the victim ignores information that does not comport to the desired outcome by self-deception, satisficing, or unconscious decision-making.

Communication in online communities is no different from the in-person communication that has existed since the dawn of humanity. Aristotle classified three types of influence or persuasion: deliberative, often used by politicians in campaign speeches; forensic, frequently used by lawyers to convince juries of the guilt or innocence of an individual; and epideictic, used either to publicly praise or condemn another person (Borchers 2013). According to Borchers (2013), the validity of the speaker rests on ethos (credibility), pathos (emotional appeal), or logos (logical soundness). In many ways, the purpose of persuasion is to help another individual overcome cognitive dissonance<sup>50</sup> and to trust the persuader. Persuaders know individuals use mental shortcuts, or cognitive heuristics, when making decisions (Shadel and Pak 2007). The criminal counts on the victim using mental shortcuts to make a decision rather than a comprehensive analysis of the situation, whether due to limited time or emotional appeal.

Emotionally appealing stories often evoke empathy in the target. Dennis Krebs (1975) found that people identify with, and feel more empathy for, those who are reportedly similar to themselves. There is evidence that empathy for another is so strong a motivator that people willingly place others' needs above their own (Batson et al. 1981; Krebs 1975). Whether the empathy and desire to help is altruistic or to lessen their own distress, guilt, or shame from knowing another is suffering, scammers understand that ultimately the victim will see this as a form of self-benefit (Krebs 1975). In order to cooperate with commission of the crime, the victim must take some action and oblige the request. The victim is persuaded under false pretenses.

---

<sup>50</sup> Cognitive dissonance involves conflicting thoughts, attitudes, or beliefs leading a person to change in order to relieve the associated discomfort.

Persuasion is “human communication that is designed to influence others by modifying their beliefs, values or attitudes” (Simons 1976). David Modic and Stephen Lea’s (2013) research in the psychology of persuasion showed that susceptibility to scam compliance is a function of authority, social influence, and the need for consistency and self-control. Modic and Lea (2013) claimed that the three stages of persuasion compliance are plausibility (does it make sense), response (action), and loss (victimization). Social psychologist Robert Cialdini (2001) has researched and written specifically on the art and science of influence and persuasion, describing what he considers are the six universal principles of influence.

Authority is the first universal principle of influence. Humans respect others in positions of authority and often seek out leaders who are experts. The symbols associated with authority, such as impressive position titles, add to an individual’s credibility . Compliance to authority is influenced by society’s standards of behavior. Stanley Milgram, a Yale social psychologist, conducted a study to understand the likelihood that ordinary individuals would obey an authority’s orders despite the risk of killing another person. His research showed compliance as long as the individual perceives the person giving the order as having legally based authority (Milgram 1963).

Liking is the second universal principle of influence. People like to do business with people they like and continue to make contact with such people with increasing familiarity. This is particularly true if the person makes a favorable impression and has similar interests, background, religion, or political leanings. Brown, Asher, and Cialdini (2005) found a positive relationship between influence and the desire for decision makers

to do business with people they knew and trusted. In romantic relationships, physical attraction is a strong source of persuasion.

Social proof is the third universal principle of influence. Social proof is a concept that is seen in individuals from an early age, when the best friend or neighbor gets a toy or new go-fast sneakers. People are guided by peers or others they admire, which is why famous models are paid high salaries for wearing specific fashion designer clothing. Consumers are influenced by those around them and endorsements from satisfied customers, particularly peers, where others who are like them have purchased the same service or product or given to the same charity. When in an ambiguous situation, observing the decisions or actions of others may entice the decision maker to accept the observed individual's lead. A form of normative social conformation is to be liked or accepted, even if one does not believe in what is said or done (Asch 1956). Solomon Asch, a university professor and social scientist, conducted conformity experiments and found that the degree of conformity was a function of a person's cognizance of persuasion, the degree to which the person believes in what is said or done, and the depth of desire to be accepted by another person (Asch 1956; Mallinson and Hatemi 2018).

Scarcity is the fourth universal principle of influence. When a product is rare or difficult to find, it may give the impression that it is of greater quality or—in the case of water during hurricanes, for example—it may be a necessary item that achieves a heightened, life-saving value. Often the item is attractive because others find it attractive.

Reciprocity is the fifth universal principle of influence. People feel indebted to someone who has given them a gift or done something for them. Cialdini (2001) found that the gift or act does not need to be big or expensive: even information is effective in

getting the customer to agree to a sale. The underlying emotion of indebtedness may entice an imbalanced repayment, even if the obligation was uninvited. Beiers, Pandelaere, and Warlop (2007) found higher compliance rates for charity donations, even when near-worthless gifts were given. Reciprocity can be a strongly felt obligation: as Cialdini (1993) noted, in 1985 Ethiopia sent a reciprocity gift of \$5,000 to Mexico to help victims of that year's earthquakes in Mexico City. The money was sent despite Ethiopia's economic collapse due to years of internal war, drought, and thousands of its residents dying of starvation and disease. The funds were sent because Mexico was the only member of the League of Nations that sent aid to Ethiopia when it was invaded by Italy in 1935.

Commitment and consistency make up the sixth universal principle of influence. The primary driver in consistency alignment enables the decision maker to rely on previous decisions and reduces the need to revisit long-established beliefs and attitudes. Brown, Asher, and Cialdini (2005) discovered that older individuals who found themselves in a situation that demonstrated inconsistency experienced emotional upset and they were specifically driven to consistency in their activities, cognition, and interactions with other people. As Arsonson (1995) and Pak and Shadel (2007) write, commitment and consistency refer to an individual's large commitment followed by a seemingly small commitment, and being consistent is a heuristic that helps deflect cognitive dissonance.

The research of Eric Knowles and Jay Linn illustrates how persuasion fits into one of two categories: increasing the desire for something or decreasing the resistance to something (Konnikova 2016). This underpins how social media companies build habit-

forming apps by making it easier to buy online, upload and send pictures, or check to see if grandchildren responded to your text. The more an emotional trigger like loneliness or boredom is soothed by an association with an email, a like on Facebook, or some other life-affirming response, the greater the chance of becoming addicted to the persuasion tactics prevalent on the internet (Schull 2012; Greewald 2014). Embedding a product need with a customer reinforces the customer's desire to acquire that product; people tend to overlook the part that trickery and deception may play in their decision-making (Akerlof et al 2015). For example, R. J. Reynolds Tobacco Company used Joe Camel television commercials in the 1980s to increase the sales of cigarettes. The cigarette sale campaigns were very successful, but the impact to society's overall health was inverse to the campaign's success (Levy et al. 2001; Friend and Levy 2001), which is why C. Everett Koop lobbied for a smoke-free society by the year 2000 (Koop 1985). Along with encouraging Congress to pass legislation for cigarette labeling, strong, negative, and often graphic media interventions helped decrease the resistance to the ban on smoking in public buildings (Ito et al. 1998; Koop 1989).

Much of the marketing industry is based on the science of influence; its methods are designed to impede deliberate critical thinking and trigger a heuristic decision in an automatic, predictable, and fixed pattern that influences the individual's behavior. While Cialdini argues for the ethical use of influence in business, he recognizes that there are those who manipulate or unethically use influence and persuasion to achieve their own desired outcomes (Cialdini 2001, 2016). It is not only psychology that is employed in helping an individual make decisions; there has been a significant investment in recent decades to boost the ability of technology to assist in decision-making. While there is a

long history of decision support systems that alleviate some burdens in the decision-making process, it is persuasive technology systems—“computerized software or information systems designed to reinforce, change or shape attitudes or behaviors or both without using coercion or deception”—that are of interest (Oinas-Kukkonen and Hajumaa 2008, 202). B. J. Fogg (2003, 1998) classifies persuasive technologies by their function as tools, media, social actors, or some combination of these. Tools help with task completion that increases capabilities, media are interactive technologies that support experiences (such as games), and social actors create relationships by adopting animated personas like Siri or Alexa. Oinas-Kukkonen and Harjumaa (2009, 487–88) give seven postulates that strengthen persuasive systems:

- Information technology is never neutral and in some manner is “always influencing attitudes and behavior.”
- People like their views about the world to be organized and consistent, which is compatible with Cialdini’s principle of commitment and consistency.
- Direct and indirect routes are key persuasion strategies reflecting the multitude of persistent technologies used to influence individuals—from texts, emails, and television commercials to telephone calls—with the intent to trigger a heuristic-based decision.
- Persuasion is often incremental, starting with small requests and building to larger targeted behavior.
- Persuasion through persuasive systems should always be open in order to maintain an unbiased means of helping users change attitudes and behaviors.

- Persuasive systems should aim at unobtrusiveness to avoid ill-timed prompting of the user.
- Persuasive systems should aim at being both useful and easy to use, thereby driving the user to engage with the technology more often.

B. J. Fogg's dissertation and work as the founder of Stanford's Persuasive Technology Lab is committed to helping entrepreneurial web developers research and design technologies to change users' attitudes and behaviors and help keep them engaged with the technology (Fogg 1997, 2003). Newspapers, radio, and television are time tested and well understood mediums that deliver persuasive messages through hard-hitting news interviews, "reports from the front," investigations, and everyday advertising. The new persuasive technology falls under categories like on-demand video streaming, internet games such as Words with Friends, online chat sites like Facebook, online news and advertising, and computers with social companions such as Siri and Alexa. These interactive technologies are delivered through hyperlinked content, audio and video, graphics, animation, and simulation. Oinas-Kukkonen and Hajumaa (2008, 201) concede "serious consideration is needed to determine who is the persuader [, as] computers do not have intentions of their own." Fogg (1998) contends there are ethical concerns that manifest themselves in terms of financial, trust, privacy, and time losses, which require social action and advocacy.

Peter W. Singer and Emerson T. Brooking (2018, 3) wrote that social media engineers "design their platforms to be addictive" to ensure a constant source of followers. Adam Alter's (2017, 8–9) research shows "tech[nological] developments do promote addiction" and "activate the same brain regions" as other addictions as they fuel

“some of the basic human needs: social engagement and social support, mental stimulation, and a sense of effectiveness.” He asserts that research reveals as many as 46% of US citizens are hooked on their smartphones, with as many as 40% possessing a level of internet-based addiction. The application of social rules makes interactive technologies more likeable to the user; therefore, these technologies have greater persuasive capabilities. Boredom encourages individuals to spend time online, often behaving in ways that they would not behave offline, such as giving away personal information, undertaking romantic endeavors, or gambling (Ng and Wiemer-Hastings 2005). A study in 2007 of college-educated middle-aged Caucasian males who were addicted to the internet indicated that they suffered from maladies such as internet gaming, internet pornography, and social isolation (Young 2007). There is debate regarding the diagnosis of internet-based addiction, as the internet may be the place where the addiction occurs rather than the object of the addiction; however, internet-based addiction is best explained as compulsive internet use with negative outcomes (Ryan, Reece, Chester, Xenos 2016). Humans are social animals and need affirmation that their life is important and has meaning. Likes on Facebook and email responses are some types of social affirmation (Alter 2017). Responses or feedback on social media help fulfill the need for social affirmation as well as provide the opportunity for social comparison of where one fits in the social structure (Alter 2017). The phenomenon of social acceptance and need is often fulfilled online when the user experiences pleasure so that the brain releases dopamine (Alter 2017). At the neurological level, dopamine is released when a user posts messages and receives responses, oxytocin is emitted when a person perceives trust, and the stress hormone epinephrine inhibits the release of oxytocin during times of

stress or distrust (Zak 2017; Singer and Brooking 2018). Unfortunately, tolerance to dopamine release increases over time, which requires the user to increase their online behavior to reach the previously attained dopamine level. It is about the experience: even when the user knows that the experience may cause a stressful situation, have a negative outcome, or result in unhappiness or even pain (Alter 2017).

Each decision or experience becomes part of the brain's memory bank and influences the next decision. Elizabeth Loftus explored memory fidelity and found not only that recall was inaccurate but also that memory was susceptible to manipulation (Eagleman 2015). How we recall information is influenced by a myriad of factors including present state of mind, the current environment, and the expectations of others (Hallinan 2009). The con artist may frame the expectations to include the thought processes of others in the form of flattery and common interests or trigger an emotion of perceived expertise that provides credibility (Lea, Fischer, and Evans 2009). Manipulated memory stored in the memory bank also influences later decisions. Manipulated memory is a form of social engineering. Christopher Hadnagy (2010, 181) defines influence as "the process of getting someone else to want to do, react, think, or believe in the way you want them to."

The degree of trustworthiness and the balance of trust between the perpetrator and the victim is directly related to the victim's trust in the perceived honesty and reputation of the perpetrator. Often these qualities are combined to make an individual's—in this case, a criminal's—reputation. Reputation is built online through the number of likes on Facebook or by testimony from others, both real and fake. Reputation ascribes the idea of behavior and idealism if perceived behavior aligns with the potential victim's goals or

desires. Philippe Jehiel and David Ettinger (2005) contend that victims may be susceptible to deception due to insufficiently perceiving fine cues, or what Akerlof and Shiller (2015) call cognitive bias. The potential victim underestimates the importance of cues in the particular circumstances involved, resulting in a fundamental attribution error (Jehiel and Ettinger 2005). Cognitive bias, also seen in magic and confidence games, consists of unconscious inferences or a distorted social reality, which may lead the victim to make irrational or illogical decisions (Akerlof et al 2015; Haselton, Nettle, and Andrews 2005). Heuristics, intuitive judgments that home in on one aspect of a complex problem when little information is available, may lead to cognitive bias.

While there is no single definition of trust there are sources of trust, which are the perceived qualities that engender trust: dependability, authenticity, honesty, intent, and expert knowledge (Hill and O’Hara 2006; Purkey and Siegel 2003). Hill and O’Hara (2006) argue that trust and mistrust can coexist, and individuals may be trusted in one context but not in another. An example is an employee who is trusted to make an important presentation but not trusted to manage the business’s finances. The context is beneficial to understanding the conscious and subconscious cognitive processes that provide the ability for an individual to assess another’s trustworthiness, whether deception is involved or not.

Deception is the “process by which actions are chosen to induce erroneous inferences so as to take advantage of them” (Jehiel and Ettinger 2005). Deception is psychological cheating or what Bell and Whaley (1991, 47) call the “advantageous distortion of perceived reality.” Bell and Whaley (1991) claim there are two categories of deceit—hiding what is real and showing what is false—each of which has three variants.

These variants are examples of information that is intentionally designed to mislead the victim, which can alter the perception of what is real (Akerlof et al 2015; Seife 2015). This deceit sets the stage for the criminal to defraud the unwitting yet complicit victim. While all deception involves hiding what is real, showing what is false never involves hiding.

Hiding, like that written about in spy novels, ranges from the ingenuous to the convoluted, and the three variants are: masking, repackaging, and dazzling (Bell and Whaley 1991).

*Masking* is the ability to hide in plain sight like the 2002 District of Columbia sniper or Sherlock Holmes in *A Game of Shadows* (Downey 2011).

*Repackaging* has been done for decades. Retailers have repackaged products for decades; some are immaterial or harmless, such as Procter and Gamble's Top Job, a green-colored liquid with ammonia, and Mr. Clean, a blue-colored liquid with ammonia. Essentially the same product, this advertising repackaging strategy met the needs of consumers who found it unsettling to use a floor cleaner on their counters and other areas that might contact food. Drug companies or pharmacists often execute a different kind of repackaging. This happens when a drug is sent to the pharmacy in a quantity greater than prescribed by a patient's doctor, and, therefore, the drug is repackaged for the patient's use (U.S. DHHS 2017). However, drug repackaging activities can be dangerous when a package that appears to contain the real item actually contains a counterfeit version (Sklamberg 2014).

*Dazzling* is the third type of hiding deceit. Shakespeare (1596) warned in *The Merchant of Venice* that “all that glitters is not gold” (act 2, scene 7). The victim is

dazzled by an assertion of facts that draws their attention away from true nature of the guise.

Showing what is false also has three variants, which are mimicking, inventing, and decoying (Bell and Whaley 1991).

People use *mimicking* in order to offensively produce a beneficial outcome (Bell and Whaley 1991). As an example, during the First Gulf War (August 2, 1990–February 28, 1991), Iraqis faked a surrender to US Marines, who then were fired upon as they attempted to receive the surrender.

*Inventing* refers to the ability to look like something one is not. An example is the common use of fake snow in movies, like the foamite, sugar, and water mixture used in *It's a Wonderful Life* (Silverman 2019). Humans also invent themselves into what they are not—such as a knowledgeable investment broker or an interested and worthy mate.

*Decoys* are prey that entice others through deceptive means. While General Eisenhower decided General Patton was not the right general to lead the Allied invasion of Normandy, the Nazi hierarchy disagreed, and Eisenhower knew that. Eisenhower understood that Patton was the right decoy for the fake 1944 invasion of France at Pas de Calais, allowing for the successful invasion of France at Normandy.

The strength of an undetected deception, deceit, lie, or instance of coercive persuasion is critical successfully convincing the potential victim to participate unwittingly in his or her own victimization. Con men and women have a long and lucrative history of exploiting and defrauding members of society. Books, plays, and movies are replete with warnings and famous examples of chicanery, such as the feats of Amy Archer Gilligan, which were ironically made into the comedy play *Arsenic and Old*

*Lace* by Joseph Kesselring. Her victims resided in the convalescent home she ran in the early 1900s, where at least 20 people, including both of her husbands, died of “old age,” ostensibly helped by the addition of arsenic to their daily nourishment. The modern-day Amy does not necessarily need to resort to murder to gain access to her victim’s finances; they just need to convince their target to provide access to their savings over an ICT medium (Holt 2003). Whitty’s (2013) research showed that the foot-in-the-door technique is commonly used in romance scams. According to Freedman and Fraser (1966), a small request is followed by another that is larger. In other words, if the victim has complied with the original request and the new request is consistent with the original request, using this technique will garner compliance with the new request.

Schein, Schneier, and Barker (1961) first noted that social, physical, and psychological factors contribute to a person’s inability to leave a situation. Research demonstrates that the social process of coercive persuasion involves a complex series of events in which the brain is constantly making both conscious and unconscious decisions, taking in hundreds of pieces of data, and culling options to make an optimal or suboptimal decision (Schein, Schneier, and Barker 1961; Eagleman 2015; Fogg 2003).

The perpetrator does not necessarily steal anything; the victim willingly surrenders assets such as money, trust, or emotional support (Konnikova 2016). Because it is seemingly easy to recognize the eventual outcome of fraud, friends, family, and social workers often question why the victim did not understand they were being scammed or defrauded and walk away to begin with. Lea, Fischer, and Evans (2009, 121) found that the victimization was a result of decision errors: “there was no evidence that any of the decision error propensities distinguished victims . . . from non-victims more

effectively than others.” However, persuasion is a form of social power in which social identification is a dominant force for maintaining cohesive affinity groups.

Frequently, embarrassment of their role in their self-victimization prevents many people from reporting the crime. The idea of being identified as gullible and not capable of self-management prevents many more from reporting their victimization. People who were victims of security failure and hacker activity tend to report the occurrence of fraudulent activity; however, Mason and Benson (1996) found that victims often underreport crime when they perceive their situation may be due to their own gullibility. Often the embarrassment is internalized, and the individual becomes more likely to become a victim again (Mason and Benson 1996; Herlery 2012).

### **Older Americans as a Cohort**

As Americans live longer, senior citizens have become the fastest growing segment of society (Kiel 2005). The oldest of this “booming seniors” group, born between 1946 and 1964, are now in their 70s. The Administration on Aging (AoA 2013) estimated there were 60 million resident adults aged 60 years and older in 2011. From 2000 to 2040, the number of residents over the age of 60 years will more than double to almost 102 million, with 14 million of those citizens aged 85 years or older (AoA 2013). Life expectancy significantly increased from 1900 to 2010, and this phenomenon is reflected in the censuses from those years: in 1900 only 6.4% of the population was over 60 years of age, compared to 18.4% in 2010 (AoA 2013). A myriad of factors have contributed to this increase in life expectancy, including advances in US medical practice, greater safety standards, improved sanitation, increased old age financial security, and better food supply. This has resulted in what Olshansky (2006) and colleagues refer to as

the *longevity dividend*: people have longer and more productive lives and are able to delay what many consider to be the adverse effects of aging. As Welsh poet Dylan Thomas (1953, 239) advised, today's seniors "do not go gentle into that good night," as they have chosen to remain active and industrious members of society and the workforce. There are many positives to the longevity dividend, including the ability to work, as working supports both the individual and society economically and often socially (Olshansky 2006).

Aging is an inevitable part of life and is more than a mental and physical permutation; it is a rite of passage. This rite of passage is different from the cohort type of transition experienced following college graduation and has less social support than individual milestone events like reaching adulthood. This liminality event, however, is similar to most life transitions, when the familiar gradually gives way to a new identity, community, or lifestyle (Gennep 1960). Aging is also a social process, a process that is repetitively redefining how an individual fits into the American societal fabric.

There is a downside to portraying the aging process as a dreaded aspect of life or a curable disease. Anxiety tied to the disconcerting consequences of aging has spawned a multi-million-dollar industry willing to cash in on maxim that 'looking young, being active is happiness.' However, the ability to adapt continuously to changes allows an individual to have a sense of well-being (Stuart-Hamilton 2006). Acceptance within the fabric of society requires communication and interaction with others (Cavan 1962). Yet studies indicate that society aligns expectations by classifying age-related social categories based on an individual's chronological age (Divita 2012). This becomes evident when a senior retires and their new lifestyle changes the nature of their

interaction. Retirement is usually associated with a pensionable age and a self-determined level of financial security. Nevertheless, economic or social value may be regarded differently upon retirement. Social value is an evanescent distinction fixated on some inexpressible societal contribution, and retirees are occasionally viewed as financially reliant or even a burden on society's stalwart contributors (Payne 2012). The perception of seniors as social burdens, financial liabilities, or having the purse of Fortunatus sometimes leads to abuse.

Gaus (1947) characterized American society's place for older Americans after the shift from farm life, where older Americans had meaningful work to accomplish and a relationship with younger generations, to pensioners disconnected from business. When an individual stops contributing to the growth of society, society becomes less efficient and the individual is perceived to be, or perceives themselves to be, a burden. A sense of purpose and social interaction along with diet and physical activity keep the brain active and cognitive decline at bay (Eagleman 2015).

### **Financial Exploitation**

Financial exploitation threatens lifestyle- and life-preserving assets and potentially undermines the prevalent concept of the "golden years." Elder abuse, including financial fraud and exploitation, is a pervasive and often underreported crime against the nation's senior population. Among the six types of elder abuse, financial exploitation is the most prevalent—representing one-third of reported elder abuse cases (Teaster, Dugar, Oto, Mediondo, Abner, and Cecil 2006; Choi 2009; National Center for Victims of Crime, n.d.). Research exploring cyber-enabled or internet crimes and the victims' vulnerability to these crimes often cites lack of education, gullibility, declining

cognitive capability, lack of financial acuity, and lack of communal life as contributing to the victimization—in essence, blaming the victim for the crime (Applewhite 2016). The problem is compounded because older citizens, as a cohort, have a relatively high level of unemployment, with over half of those actively seeking employment failing to obtain work even after two years (Li 2010). While the longevity dividend may enable individuals to work, the opportunity to find work does not necessarily exist. A financial scam that could deplete an entire lifetime of savings with little recourse may lead a senior to seek public assistance, which then impacts all citizens by increasing the fiscal burden within and beyond the social security system.

All sectors of society are susceptible to scams. It is not unusual for well-educated individuals to fall prey to the most unscrupulous perpetrators' romance scams, "you've already won" rackets, hoaxes, and other confidence games. However, studies show the onset of cognitive impairment significantly increases the potential for bad financial incidents, and the victims who suffer financial theft are four times more likely to resort to public assistance or support (Lachs, Williams, O'Brien, Pillemer, and Charlson 1998). The Department of Justice (DOJ) acknowledges the millions of US residents who are victims of fraud each year suffer a significant emotional impact due to that fraud. Frequently, there is a sense of guilt or shame for "falling" for the scam, with the additional potential of financial ruin and loss of independence, particularly for older citizens (DOJ 2016). Despite the large reported financial losses, only 15% of fraud victims report the crime (DOJ 2016). Embarrassed or afraid of what will happen once family or friends discover how they were "foolishly" defrauded, victims often suffer increased emotional and medical problems (DOJ 2016). Pratkanis and Shadel (2005) found that older fraud

victims suffer severe negative effects: the often-repeated victimization and loss of life savings results in lowered life expectancy. The financial costs of emotional and medical support compound the expenses from the loss of independence, and the required financial assistance places a burden on friends, family members, and society. In 2015, the IC3 reported 288,012 complaints, with 236,137 (82%) of the reports generated from victims under 60 years of age. Yet the senior victims are often depicted as individuals who have cognitive failures or issues as a major contributing factor, which affects their perceived ability to live independently or make life-affirming decisions (Emile et al. 2015).

Studies over the last few decades indicate a serious and growing problem with elder abuse. As an example, the National Institute of Justice 2010 survey of older citizens revealed 1.6% experienced physical abuse, 0.6% were victims of sexual abuse, 5.2% had been financially exploited, 5.1% had been potentially neglected (including self-neglect), and 5.1% had suffered emotional maltreatment. Some of the victims endured multiple types of abuse. The 1998 National Elder Abuse Incidence Study report estimates five unreported cases of abuse for every substantiated report of abuse or neglect of an older person to law enforcement. The report describes the lack of reporting as the tip of the iceberg as a way of indicating the potential magnitude of the problem hidden deep from public view. According to Page Ulrey (2015) of the King County Prosecutor's Office in Seattle, Washington, there are very logical reasons why elder abuse is so underreported. Eliciting accurate, timely information from victims is often problematic due to gradation in cognitive ability, isolation, health issues, and physical problems complicated by the influence of guardians, family, and care givers. Ulrey (2012) addressed the difficulty for the criminal justice system in proving cases of elder abuse in a 2010 white paper

submitted to the first Elder Justice Coordinating Council. Ulrey (2012) apprised the council of how gaining insight into abuse requires understanding the individual victim's situation holistically, including the social fabric. Often the abuse is inflicted by someone with whom the victim has a close emotional relationship, which may prevent the victim from seeking help—either due to the victim's feelings for the abuser or fear of the abuser (World Health Organization 2011). Victims of this “national disgrace” often suffer anxiety and depression, are unable to convey the level or type of abuse, and may also lack knowledge of where to go for help.<sup>51</sup> There is a lack of expertise in understanding the indicators of elder abuse among law enforcement officers, social workers, lawyers, and medical personnel, especially the formidable indicators of financial exploitation (Ulrey 2012). While all ages have been victims of financial crimes, seniors—unlike their younger counterparts—have fewer options for remedying a bad financial decision.

### **Cognitive Function and Grooming**

The adage that age is a state of mind may well be prophetic, in that age often contributes to the state of an individual’s cognitive processes. It is impaired cognitive processes, such as the descent into dementia, that may present financial perils. In a 2014 study on susceptibility to scams in older adults without dementia, the researchers found seniors with “lower levels of cognitive function, lower psychological well-being, and poorer health and financial literacy appeared to be the most susceptible to scams, independent of level of education or income” (James, Boyle, and Bennett 2014, 7). The study showed that a confident, optimistic attitude contributes to sense of well-being, but financial knowledge and high cognitive function are determinants of susceptibility. It is

---

<sup>51</sup> House Select Comm. on Aging, Subcomm. on Health and Long-Term Care, *Elder Abuse: A National Disgrace*, H. Rep. No. 99-502 (1985).

not unheard of for previously savvy individuals to become prey to the most unscrupulous of fraudsters. In this regard, there are some core misunderstandings about the process of grooming the victim. Scholarly research conducted on seniors' cognitive abilities and the effects of aging on those abilities provide very few fruitful articles that chronicle the change to the self-determined quality of life of senior citizens who have suffered cyber-enabled financial abuse. A few studies flag the need to understand the relationship between age and cognition (Peters 2006). The University of California conducted a behavioral study using a neuroimaging methodology (magnetic resonance imaging), which revealed a difference in the ability of older adults (aged 55–84 years) to discern trustworthiness when compared to participants aged 20–42 years (Castle et al. 2012). During the data collection, the younger adults' anterior insula cortex (AIC) indicated negative reaction to photos of untrustworthy individuals, whereas the response from older adults indicated trustworthiness and approachability. The AIC is believed to be vital for human self-awareness and the social cognition commonly referred to as the gut reaction to ideas and feelings. While this study was based on visual cues, it is a significant supplement to the University of Iowa's study of the ventromedial prefrontal cortex (vmPFC). The researchers in this study used misleading advertisements to compare individuals with either injured or aged vmPFC against individuals who were considered to have overall healthy brains (Asp et al. 2012). Those considered cognitively healthy were able to discern potentially fraudulent ads twice as often as the other participants in the study. The vmPFC, which controls emotions such as doubt as well as planning and decision-making, provides another potential clue to the underlying reason why some older adults may be predisposed to make suboptimal financial decisions. Annamaria

Lusardi (2012) claims older Americans have a widespread lack of financial literacy, particularly older women. The United States overall scores C– on financial knowledge, according to a report authored by John Pelletier (2016), the director of the Center for Financial Literacy at Champlain College, meaning older Americans are not alone in their lack of financial knowledge and expertise. Yet there is an inclination to conflate and exaggerate the strength of the link between victimization and the victim's cognitive abilities (Applewhite 2016). Li et al. (2015) report older citizens with age-related cognitive decline continue to make sound financial decisions when they have a level of financial knowledge and expertise. In fact, DeLiema et al. (2018) and Carlson (2006) suggest seniors may benefit from financial education and enhanced professional financial assistance to reduce exploitation. While several studies indicate older citizens are more likely to be victimized, other studies claim they are less likely to be victimized (AARP 1996, 1999, 2003; Shadel and Pak 2017; Kerley and Heith 2002; Anderson 2013). A Florida statewide survey of 922 adults conducted by Pratt, Holtfreter, and Reisig (2010) dispels the long-standing use of demographics such as sex, size, and age as indicators of risk for victimization. Ageism, however, is a threat.

Ageism, the dismissal of a person as a second-class citizen due to advanced age, is a social construct within which potential inequality and oppression can exist (Applewhite 2016; Nelson 2005). In the United States, older Americans are often marginalized, stripped of authority and responsibility, and thereby denied dignity (Nelson 2002, 2005). Pulitzer-winning author Robert Butler (1975, 48) claims that “ageism allows the younger generations to see older people different than themselves; thus, they subtly cease to identify with their elders as human beings.” Older Americans often fall victim to

what is referred to as the *stereotype threat*, the threat of conforming to an affinity group's expected behavior, performance, or desires. This leads elders to question their own abilities based on by others' expectations—a kind of learned helplessness (Applewhite 2016). In 2003, the National Academies Press found a dearth of investigation and support regarding the phenomenology, extent, etiology, and consequences of elder mistreatment (Bonnie and Wallace 2003). Condescending communication, infantilization, and stripping a person of their decision-making ability are ageist, insulting, and show a level of expected dependency that has negative effects on older citizens' self-worth and independence (Nelson 2005). Fear of losing independence and fear of living out life warehoused in a facility are real fears for many older Americans, but these are sanctioned institutional and social practice (Nelson 2005). Only 4% of Americans over the age of 65 years, and 10% over the age of 85 years, live in nursing homes, yet anxiety associated with this perception has deleterious effects (Applewhite 2016; Nelson 2005). Social prejudice research shows older citizens enjoy better mental health than other age groups (Cartensen 2009). The phenomenon of memory inaccuracy affects all ages, yet socially approved ageism prejudicially associates this phenomenon with older citizens (Applewhite 2016; Eagleman 2015). The driving factors for cognitive decline are social and psychological dynamics such as loneliness, anxiety, and depression. Several studies show loneliness, living alone, and little social interaction or connectedness as indicators of isolation that pose health risks (House 2001; Uchino, Cacioppo, and Kiecolt-Glaser 1996; Barnes, Mendes de Leon, Bienias, and Evans 2004).

Older citizens online often use technology to provide social connectedness as a proxy for limited and possibly decreased real-life social interaction, yet the rate of

technological change presents another challenge. A former Microsoft strategy chief and supercomputer designer referred to the technological isolation phenomena as *dislocation*, which happens “when the rate of change eventually exceeds the ability to adapt . . . when the whole environment is being altered so quickly that everyone starts to feel they can’t keep up” (Friedman 2016, 29). Early adopters usually find the rapidity of change exhilarating, yet others may suffer from a feeling of disconnectedness and social isolation due to their inability to adopt and adapt to evolving technological advances. However, context plays a large role in how the victim perceives the situation.

As individuals age and retire, separation from their well-known work or social infrastructure, fading awareness of mechanisms to cope in new social structures, and (all too often) broken interpersonal reliance on trust mean seniors often require additional protections. Like the young, older citizens are looking for group acceptance or for justification of an attitude or experience, such as an admiration for a certain music group or admittance to a social club. Older victims also often look to reconnect with someone of past value, like an old army “buddy” or a fraternity brother or sorority sister from college. The political challenge for placing focus on elder abuse is the underlying fact that many seniors do not want to acknowledge their vulnerability by being segregated into a group requiring special consideration. Older citizens often perceive or interpret their separation from the mainstream of society as a signal that they are less useful to that society, and a new policy could possibly lead to encroachment on their personal freedom. Their fear is that the policy emphasis might perpetuate perceptions of dependence and encumbrance rather than the joyful, natural aging process all citizens hope to live long enough to experience (Applewhite 2016).

The multitude of state and federal regulations form a confusing labyrinth for a victim to navigate in order to solicit aid. Older adults suffering from abuse, like any victimized group, lack the political capital and legislative influence (i.e., lobbying) needed to achieve social justice. Elder justice advocates are de facto active participants in the legislative process, which is in stark contrast to the victims, who are not active in the process (Dempsey 2008). Social justice comes with social policy changes, and the changes happen when seasoned advocates help drive the political process toward equality and fairness (Dempsey 2008). Without assistance from well-informed advocates, seniors are vulnerable to abuse with few means of recourse. For decades, it has been the states' adult protective services (APS) that have been on the frontlines of combating elder abuse in the United States (National Adult Protective Services Association 2014).

Unfortunately, the training has been insufficient, and rules of engagement to combat cyber-enabled financial abuse are not clearly defined. States' approaches to protecting elders differ widely, according to APS statutes depicted on the American Bar Association (Stiegel 2007). For example, 48 states have physical abuse as a stand-alone category; one state has it included in another category within an APS statute, and South Dakota has no separate APS statutes. All APS in South Dakota are incorporated and authorized in other state laws. In 2014, only 43 states had a stand-alone statute for financial exploitation. Emotional abuse legislation, including psychological, mental, or verbal maltreatment, is a stand-alone statute in only seven states, and is integrated under other categories in the APS statutes of 39 states. Laws concerning elder abuse differ substantially from state to state with regard to the types and levels of prohibited behavior and reporting requirements (GAO 1991). For example, in 2019 Arizona became the 24th state to adopt

report and hold laws for financial institutions to help prevent financial exploitation of older and vulnerable adults, while Florida (with the highest proportion of senior citizens) failed to do the same (Bressler, Amery & Ross 2019). Another difference between states is the qualifying age. In Maryland the qualifying age for additional protection is 55 years, and in California it is 65 years, yet in 1987 Congress used 60 years as the age at which an individual could be considered a victim of elder abuse (GAO 2011; Teaster, Dugar, Oto, Mediondo, Abner, and Cecil 2006). The differences between various states' policies may be magnified when older citizens retire and either move or are moved to a different state where the rules and means for accessing assistance are different.

## **Victim Services**

Three intertwining government ecosystems service victims of elder abuse (GAO 2013). The first, social services, is led by the secretary of health and human services and comprises organizations such as APS, state aging agencies, area agencies on aging, and local assistance organizations. The second ecosystem is the criminal justice system, led by the DOJ, law-enforcement agencies, states' attorneys general, state courts, local law enforcement agencies, district attorneys, and county or local courts. The last ecosystem, consumer protection, is led by several agencies, including the Consumer Financial Protection Bureau, the Department of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission. At the state level, this ecosystem includes state insurance, banking, and securities regulators. At the local level it includes workers at bank branches and post offices. One Government Accountability Office (GAO 2013) report found little overlap or duplication of services among these agencies servicing elderly victims of abuse; however, the lack of coordination among federal

agencies in addressing elder abuse creates inefficiency and reduces effectiveness when a problem straddles more than one agency. A 2019 GAO report to Congress on elder justice indicates that while the DOJ has “established several efforts to address elder abuse,” it has not developed or documented goals, nor does it have a means to measure success (Goodwin and Grover 2019, 1).

Financial exploitation of the elderly constitutes nearly one-third of all reported cases of elder abuse; however, only one in 44 cases of financial exploitation is reported (Lachs and Berman 2011). Policy and financial advisor Leonora Miles (2008, 28) referred to the financial exploitation of seniors as “economic violence.” Victims of financial exploitation and fraud often fall to a lower quality of life, with the devastating loss of lifelong hard-earned assets leading them to require some level of public assistance (Deem 2000; Teaster et al. 2006). In written testimony to the Senate Special Committee on Aging, Ulrey (2015) stated that the damage caused by financial exploitation often results in the premature death of the victim and can potentially affect a family for generations.<sup>52</sup> Ulrey added that the costs of Medicare, Medicaid, and other social services, such as housing, are also increased due to the loss of financial assets.

The Elder Justice Act, enacted as part of the Patient Protection and Affordable Care Act of 2010, established the Justice Coordinating Council within the Office of the Secretary of the Department of Health and Human Services (DHHS). This council is charged with reporting its accomplishments and activities to Congress every two years (DHHS 2014). The secretary convened the first Elder Justice Coordination Council meeting on October 11, 2012, a year and a half after the passing of the Elder Justice Act;

---

<sup>52</sup> “*Broken Trust: Combating Financial Exploitation Targeting Vulnerable Seniors*”, before the Senate Special Comm. on Aging, 114th Cong. 13 (2015) (written testimony of Page Ulrey).

the second meeting was held in May 2013. The council comprises 12 federal agencies from the DHHS, the DOJ, the Social Security Administration, the Department of the Treasury, the Department of Veterans Affairs, the Consumer Financial Protection Bureau, the Federal Trade Commission, the Department of Housing and Urban Development, the Securities and Exchange Commission, the Corporation for National and Community Service, the Department of Labor, and the US Postal Inspection Service. The council made eight recommendations to help stem elder abuse, neglect, and exploitation, aiming to improve awareness as well as prevent, and improve response to, elder abuse, neglect, and exploitation. The biannual report discussed the issue of cyber-enabled threats to seniors but fell short of explaining how the council will address this issue.

There is the additional advocacy problem. Age is the sole criteria for protection under these acts, which may provide insight into why legislators play a part in the slow policy process. Sam Johnson, born in 1930, was sworn in for his 14th and final term as a Republican congressman from Texas in 2018, and California Democratic Senator Dianne Feinstein, born in 1933, won another six-year term in 2018. Of the federal legislators elected in 2016, 254 were eligible for special protection and assistance under the Elder Justice Act. The 115th Congress was the oldest in US history (King 2017). This represents a potential paradox for legislators who are called on to endorse an act for special protection of senior citizens and simultaneously, as senior citizens, pursue reelection as the most capable among the population to represent the citizenry. The fact is, not all people age equally.

Society has yet to recognize when and what type of intervention is necessary, as people's capabilities age unequally. Galvanizing support for elder care requires understanding the extent and effect of elder abuse. The paucity of elder abuse and neglect information and understanding has prevented effective policy development for decades (DHHS 1992). A National Research Council report indicated that the council could not even articulate a research plan because of issues such as varying categorizations of abuse, insufficient evidence in evaluations of abuse that had been conducted, lack of demographic data, and ambiguous biographical reports. Supporters of elder justice claim that one in 10 adults over the age of 60 years—as many as 5 million people—are victims every year, that 50% of seniors with dementia living with family are abused, and that seniors who were abused have a 300% higher risk of death than others; however, the actual numbers are not known. (NCOA 2014; NAPSA 2014; Ulrey 2012; NCEA 1998).

According to the National Center on Elder Abuse, an astonishing 84% of abuse incidents may be unreported. The Elder Justice Act requires the DHHS to establish a data and information collection capability. Funding is critical to collect data in order to establish the scale of the problem and its effects on society, but acquiring financing is a challenge.

There are numerous laws protecting citizens that should apply to seniors by virtue of their citizenship. However, as individuals age and retire, separation from the well-known work and social infrastructure, fading awareness of mechanisms to cope in new social structures, and (all too often) broken interpersonal relationship trust contribute to seniors requiring additional protection. The problem for gaining focus for elder abuse justice is the underlying fact that many seniors do not want to acknowledge their

vulnerability by being segregated as a group requiring special consideration, because the emphasis might be on perceptions of dependence and burden rather than on the joy of the natural aging process that all hope to live long enough to experience.

Bill Bytheway (1995) wrote about cultural attractiveness of power and money and the perceptions that people are worthwhile if they are esteemed and are valuable economically. Payne (2012) further rationalizes this in his book, discussing how citizens spend their lives contributing to society and helping it to grow economically; when an individual stops helping society grow, society is less efficient and the individual is perceived as, or perceives themselves as, a burden. Seniors may not want a specific segregated policy, as it has the potential to codify that conception.

The small investment in resources for protecting senior citizens and providing restitution to victims negates the value of older Americans if one believes the government has some level of responsibility to safeguard all citizens' rights to justice, fair treatment, and their standard of living (Payne 2012). Making any serious means of intervention, protection, deterrence, and restitution for abuse more challenging are inconsistent and conflicting laws, intergovernmental complexities, and fiscal constraints. While the blame ultimately lies with the criminal, policy makers have failed by applying existing policies to the policy problem or, as Bytheway (1995) noted how easily society lets down those who helped them.

The umbrella term *cyber law* encompasses legal and regulatory properties of the internet, including the world wide web. US and international policy makers and legal experts continue to inadequately apply existing policies and laws to the emerging technology-enabled crimes committed in a borderless arena (Gillen 2012). The

complexities of combating cybercrime are exacerbated by a maze of governance structures across not only federal interagency and state jurisdictional boundaries, but also international borders (Bertoni 2009; Goggin et al. 1990; Brown 2012). This nascent amalgamation of civil and criminal law concerns a broad range of law, including intellectual property, first amendment rights, fraud, and stalking (Hollis 2011).

*Cybercrime* is a term for prohibited activity perpetrated using digital technologies that includes fraud, theft, feigned romance, stalking, traditional white-collar crimes, privacy violations, illegal drug transactions, or any other offense that occur in an electronic environment for the purpose of economic gain or with the intent to destroy or otherwise inflict harm on another person or persons.

The spread of crime through the disparate and autonomous states, the aggressive and motivated behavior of cybercriminals, and the naïveté of the typical internet user create a confluence of circumstances that make exploitation almost inevitable. Bank robbery is an illegal activity, yet capturing perpetrators has historically proven difficult; and the anonymity of the internet exponentially increases the problem of solving crime committed there. Stephen Lukasik (2011) dismisses the hypothesis that cybercrime is a technology issue requiring a technological remedy as woefully underestimating the nature and complexity of the worldwide network. The laws governing the internet are a web themselves, in part because cybercrime often crosses several federal agencies' jurisdictions and interconnects with other heinous crimes such as identity theft, credit card theft, romance scams, and mortgage scams (Bertoni 2009).

The US government's adaptation of existing laws to the cyber problem has proven appallingly inadequate for many individual internet users, leaving a vulnerable public to

attempt to defend themselves (Lukasik 2011). For example, the Identity Theft and Assumption Deterrence Act of 1998 criminalizes the possession or use of another person's means of identification (e.g., social security number) with the intent to commit unlawful activity that constitutes a felony under state or local law, but it is difficult to pursue, and the Federal Trade Commission receives 15,000–20,000 inquiries a week from victims and concerned consumers. Charged with reducing identity theft, the commission collects and maintains a database for law enforcement, but the number of inquiries is an indication of the growing magnitude of the problem (Bertoni 2009).

### **The Historical Framework**

The value of the American legal system is based on the premise that laws help maintain order and law enforcement and have the ability to react, which increases the citizenry's rational trust of each other (Brenner 2013). The American system of laws, created under the framework of the Constitution, has enabled the country to meet the needs of its citizenry structurally, economically, and politically. The rule of law supports society's ability to work, produce and sell goods and services, and trade reliably and securely. As a nation-state, America emerged and flourishes because of trust. The antecedents of trust of the US legal system arguably come from the political contributions of Thomas Hobbes, Niccolo Machiavelli, John Locke, Jean-Jacques Rousseau, and Jean Bodin (Martin 2011; Phipott 2016; Weinert 2007). The troubles of their day led them to believe that a sovereign with power over a defined territory and domestic affairs, without the intrusion of external powers, was necessary for survival of the nation and the benefit of its citizens. These political reflections underpinned the development of a system of sovereign states reflected in the Treaty of Westphalia.

After signing the Treaty of Westphalia in 1648, nation-states implemented controls that permitted sovereign nations to limit the import and export of goods along with immigration and emigration across national boundaries (Goodman 2016). This Westphalian system of sovereign nation-states has prevailed for centuries and is maintained through a system of recognized borders, defense forces, sentries, manned accesses, and armaments (Goodman 2015). In this system, the nation-state embodies the framework of justice, with full responsibility for internal state business as well as providing for civil order, security, and safety. The sovereignty of nation-states is recognized and provided for in the 1945 Charter of the United Nations. The sovereignty exercised by legitimate governments exists in a complicated balance of acceptance internally (by citizens) and externally (by other nation-states). Over time, many sovereign nation-states have committed to nonbinding UN declarations, such as the 1948 Universal Declaration of Human Rights, pledging to respect over 30 separate rights for individuals, as well as subsequent human rights covenants, the Covenant on Civil and Political Rights and the Covenant on Economic, Social and Cultural Rights (Philpott 2016). Since the UN is not a sovereign nation-state but exists to reinforce sovereigns and is a champion of human rights, it is often challenged to intervene in sovereign nation-states to end human atrocities. In 2005, member states at the high-level UN World Summit meeting committed to the principles laid out in the report, *The Responsibility to Protect*, first sponsored in 2001 by the UN and the International Commission on Intervention and State Sovereignty. This commitment further defined the recognized role of sovereignty in that “sovereign states have a responsibility to protect their own citizens from avoidable catastrophe—from genocide, war crimes, ethnic cleansing, and crimes against

humanity—but that when they are unwilling or unable to do so, that responsibility must be borne by the broader community of states” (UN 2017). While this commitment is a political obligation of states, the commitment also helps fortify the role of international courts and tribunals.

Globalization has made the role of nation-states more important to their citizens in for national economic and political stability. Today’s cybercriminals are organized to conduct their work on a global scale without consideration of nationality or borders, which directly affects a state’s ability to respond to its citizenry’s cybercrime concerns (Goodman 2015). Many countries have internal laws and policies addressing crime committed through ICT, but Crisan (2010) claims that since international laws often do not contain defined penalties, there is a need for the international community to undertake action in order to ensure justice. Currently, the recognized organization that authoritatively addresses cybercrime committed across the boundary-free internet is the Council of Europe’s Convention on Cybercrime, the first international treaty to attempt to harmonize nation-state laws and increase international cooperation in this area.<sup>53</sup> The convention, also referred to as the Budapest Convention, fosters international cooperation among nation-states who are parties to the treaty (Seger 2016). The convention aims to provide common standards for the criminalization of cyberattacks, offer principles for procedural law for the investigation of cybercrime and the preservation of electronic evidence, and foster international police and judicial cooperation on cybercrime and electronic evidence. As of August 2017, the Council of Europe website shows that 55

---

<sup>53</sup> Convention on Cybercrime, Nov. 2001, E.T.S. No. 185.

nation-states have ratified the convention; four more have signed but not ratified the convention. The United States ratified the convention on January 1, 2007.

For a variety of reasons, several countries refuse to become signatories to the convention. Some countries do not have the necessary legal standards in their domestic laws to be able to sign, and others refuse to sign on principle (Broadhurst and Chang 2012). In 2012, China, India, and South Korea proposed a new global cybercrime treaty to the UN, but the UN turned down the request even though some argued it would be perceived as more inclusive. In a Congressional Research Service report, Kirstin Archick (2006) claims the convention lacks real effectiveness, as less than half of all internet users' countries are signatories. This is due, in part, to some countries viewing the convention's tenets as an infringement of sovereignty.

The UN General Assembly in May of 2011 declared, "Ensuring universal access to the Internet should be a priority for all States" (UN 2011, 4). The special rapporteur<sup>54</sup> recommended the promotion of the right to freedom of expression, including the right to "seek, receive, and impart information" (UN 2011, 4). In May 2018, the European Union's General Data Protection Regulation went into effect. This regulation requires businesses to protect the privacy and personal data of residents of the European Union. It is yet to be determined how effective this law will be in either helping regulate corporate data collection or deterring criminal behavior.

Arno Lodder (2013) argues that central to internet law are fundamental human rights of privacy, freedom of speech, and copyright. However, too many legal scholars and lawyers lack sufficient internet understanding to either adequately apply existing

---

<sup>54</sup> A special rapporteur is an independent expert who works on behalf of the UN.

laws or generate evidence for better legislation (Lodder 2013). Gillen (2012) claims it is the lack of appropriate cyberspace perception that results in woefully inadequate legal theory and practice. Max Weber's bureaucratic model of organization fits well in the physical world, but assumes a hierarchically ordered concentrated sovereign authority with control mechanisms (Brenner 2013). Geography, a nation-state control mechanism, is irrelevant for cyber and cybercrime, which creates a conflict for law enforcement regarding who is responsible and who has the lead for investigating a crime (Brenner 2013). US laws generally allocate responsibility for internal crime to law enforcement and external threats to the Department of Defense, which causes operational conflicts in the virtual world where it is difficult to differentiate what is criminal in nature and what is war. The wide range of cyber threats—cyberbullying, cyberstalking, cybercrime, cyberespionage, cyberterror, and cyberwarfare—blurs the lines between the military and law enforcement. Police and other law enforcement officers are tied to a geographical area, where they look for evidence at the location of a crime (Brenner 2013). However, cybercrime evidence is scattered in cyberspace. Applying physical-world laws to cybercrime requires determining who is responsible and who should bear the blame, which is neither intuitive nor straightforward. It is quite possible for the victim, the perpetrator, and the servers that store the evidence to be in many different countries, where access to the necessary information would require assistance from government and civilian entities in the various jurisdictions (Brenner 2013; Hakmeh 2017). The complexities of the internet compound the challenge of addressing cyber-related crime, as it crosses not only federal agencies and state jurisdiction, but also international boundaries (Brown 2012).

When the state is unable to adequately solve challenges or perform critical functions through laws, nonstate entities—from corporations to terrorist groups—conduct business in the resulting legal void. The lack of ubiquitously accepted or established international internet and cyber laws often puts multinational corporations in the position of regulators (Parker, Van Alstyne, and Choudary 2016). This puts corporations like Facebook, Amazon, or Twitter, whose user populations and financial resources rival those of many nation-states, in the position of acting in the role of a nation-state without the international recognition or legitimacy of a sovereign nation-state. Individual corporate policies exercised in various countries indicate a corporation’s approach in those countries to issues such as human rights, censorship, and privacy. Individuals have little recourse for restitution from harm with nonstate entities, as these entities work across borders. In fact, several of these corporations collect, aggregate, manipulate, and sell individuals’ personal data with impunity, with the exception of data belonging to residents of the European Union.

Cybercriminals are technically savvy and adeptly thwart the traditional methods of those charged with fighting organized crime. The criminals understand the lackluster international legal capacity to intervene, and they circumvent arcane or impotent laws to successfully gain significant return on investment with little chance of being caught or punished (Brenner 2002). The preponderance of the government’s focus is on protection of national security systems, such as critical infrastructure. This effort seemingly overwhelms the resources that otherwise would work to protect the ordinary citizen. The theft of \$5,000 (usually a felony, depending on state laws) normally results in a law enforcement response and, if the formal investigation is successful, prosecution.

However, online crimes involving significantly higher figures are habitually not investigated because law enforcement lacks the capability or ability to gather necessary evidence (Barrett, Steingruebl, and Smith 2011). It is the uninhibited growth of crime committed over the internet that regularly renders its victims helpless. In most cases, law enforcement bureaucracies are organized according to Weber's principles, which results in a complex, segmented, but overlapping and, at times, conflicting series of law enforcement bureaucracies.

Criminologists categorize cyber offences by the broad target of the crime: government, business, or individual. Crimes against the government include cyberterrorism, cyberwarfare, and attacks against infrastructure, such as the Office of Personnel Management hack announced in June 2015. Greg Wilshusen and Barkakati's (2013) GAO report to Congress revealed that data were not adequately protected at 18 of 24 federal agencies. Some of these agencies have been given greater responsibility in the last few years to deliver services to citizens, including the DHHS, the Veterans Administration, and the Social Security Administration. The failure to meet the statutory and regulatory requirements of the Privacy Act of 1974 and Health Insurance Portability and Accountability Act of 1996 potentially exposes the federal government to complaints and loss of respect of its citizenry. The Office of the Assistant Secretary for Planning and Evaluation's website for the DHHS in May 1997 referred to privacy as "a deeply felt but elusive concept" (para. 1). All federal government agencies are required to keep safe all data relating to US persons; criminals, however, have no such restriction.

## **Statement of the Research Problem and Significance of the Research**

Older Americans are increasingly at risk of financial insolvency and degraded quality of life due to cyber-enabled financial abuse. Despite governmental efforts, defrauded individuals lack the ability to obtain restitution. Governments acknowledge there exists a gap in ICT user knowledge and a gap in the ability to prosecute cybercriminals (Brenner 2013). While national and international efforts have tried to address cybercrime, there is a significant gap in knowledge concerning victims of cyber-enabled financial abuse. Should these gaps persist, the goal of financially secure retirement may be at risk for many older Americans.

Cyber-enabled elder financial abuse is an emerging public policy problem, affecting all levels of bureaucracy: municipal, county, state, federal, and even global. This study addresses two challenging public policy areas of cybercrime and elder abuse to improve understanding of the mechanisms of exploitation and provide an assessment of the extent to which regulatory policies either mitigate, or unintentionally contribute to, the financial abuse of older citizens.

## **Methodology**

The phenomenon of cyber-enabled financial abuse of the elderly and its implications for public policy is a vast yet underresearched subject. This mixed-methods dissertation (defined by Creswell 2009 as a methodology where the investigator collects, analyses, and integrates or triangulates quantitative and qualitative data into a single study) applies process tracing and case studies as the research strategy.

Triangulation is a strategy to ensure internal validity so as “to minimize the degree of specificity of dependence on particular methods that might limit the validity of scope of the findings, a researcher can use two or more methods of data collection to test hypotheses and measure variables” (Frankfort-Nachmias and Nachmias 2000, 189; Creswell 2009). The amount of supporting data collected from more than one source was used to ensure internal validity by analyzing interview data as collected from the researcher’s notes as well as participants’ reviews. The participants’ reviews also helped to identify and control for any researcher bias. External reviewers of the study results and process provide, according to Creswell (2009), external validity.

The data comes from three places. Data from the Internet Crime Complaint Center (IC3) answers the question, What is the status of cyber-enabled financial abuse of older Americans? Data from surveys provides insight into perceptions of older Americans’ vulnerability to cyberfraud and financial ruin. Data from interviews and case studies gathers the “insider’s perspective [from] the meanings . . . others attach to

situations, settings . . . to understand their interpretations of those situations” (Luton 2010, 25). The third source of data is a document review of existing laws and recent criminal cases. The first part of the inquiry used quantitative collection of secondary cybercrime reporting data from the IC3 website to determine the year-on-year trend in cybercrime complaints of financial exploitation to demonstrate the magnitude of the problem. While the secondary quantitative data gleaned over 10 years from the IC3 demonstrates the growth of criminals’ financial success against older Americans, the survey serves to provide insight into beliefs or opinions regarding older Americans as potential or actual victims. A random sampling or statistical subset of the population in which all Florida, Maryland, and Virginia residents had equal probability of being selected for the survey was not feasible from either a time or access perspective. Therefore, a nonprobability convenience survey sample was used (Frankfort-Nachmias and Nachmias 2010). An attempt to find people who were willing and possessed a basic subject understanding was an intentional choice for a purposive sample in an “attempt to select sampling units that appear to be representative of the population” (Frankfort-Nachmias and Nachmias 2010, 168).

### **The Survey: Justification for Narratives and Case Studies**

The second part of the research is focused on individuals who were willing to share their experiences in a protected setting that also respected their confidentiality. Participants were able to review the descriptions of their interviews to improve reliability and to help identify and control researcher bias. Use of police and adult protective services case reports as well as external review of the process and the study results helped achieve external validity. Creswell (2009) explained that peer review provides external

validity by allowing external reviewers to examine both the process and the written conclusions of the study. The inductive, qualitative methods of observation and interviews used in this study emphasize the importance of personal knowledge, seeking to understand individuals' decisions through the lenses of those who made them and those who experienced them secondhand (e.g., family members and service providers). That experience helped to confirm or disconfirm the theory of cyber-enabled financial abuse of the elderly.

Contextualizing the phenomena or describing the victim's own account of cyber-enabled financial abuse, where the victim is connected to the phenomena, focuses on the interpretation and understanding from the perspective of the victim. The purpose was to gain insight from the experiences of the victims and their families as these narrative case studies were analyzed to understand how cyberscammers were so successful against older Americans and examine the following key question: What are individual's perspectives of victimization?

"Qualitative case studies are better suited for exploring poorly understood topics and understanding complex relationships" (Luton 2010, 129). Qualitative research techniques are less structured than quantitative methods, and the exploration is from the participant's perspective (Riccucci 2010). Through narrative inquiry, information is gathered from stories about participants' lives, including their "feelings, hopes, [and] desires" (Clandinin and Huber 2010, 4). "In narrative inquiry, the researcher deliberately constructs interviews to obtain narratives or stories because of the special way that stories have of displaying the meanings of actions and events" (Luton 2010, 54). The inquiry "use[s] stories to interpret meaning, focus[s] on lived experience, honor[s] the meaning

[victims] give to their experiences, provide[s] windows into different points of view, assist[s] in giving voice to marginalized persons . . . recognize[s] human agency—choices, motivations” (Luton 2010, 63). “People shape their daily lives by stories of who they and others are and as they interpret their past in terms of these stories . . . a portal through which their experience of the world is interpreted and made personally meaningful” (Clandinin and Huber 2010, 3). The aim of collecting data about the case studies was to analyze these experiences gathered from narrative stories in thematic categories. “Thematic analysis categorizes the content of the stories based on themes” of interest, which in this case is cyber-enabled financial abuse (Clandinin and Huber 2010, 4). The themes garnered in interviews allow for understanding of participant perceptions. Evidence from these conversations provides insight and a level of confidence that discrete parts of the proposed causal mechanism exist or do not exist. Each interview allowed inferences to inform the level of confidence. The causal mechanisms are “a complex system, which produces an outcome by the interaction of a number of parts” to help identify the theories relevant to the problem in order to explain the outcome, in this case financial abuse through fraud (Glennan 1996). These inductive, qualitative methods of observation and interviews emphasized the importance of personal knowledge and helped to understand individuals’ active decisions from those who lived them, those who experienced them secondhand (e.g., family members), and those who assist older victims.

“Yin (2014) says that exploratory ‘what’ questions can be addressed using a wide variety of research approaches, including case studies” (Luton 2010, 130). What marks case study research distinct from experimental studies is that a case study is explored in context, examined in its real-world setting, and is a motive for using a qualitative case

study approach (Yin 2014, 16). Other motives include the “focus on the special characteristics” and “to assist in theory development” (Luton 2010, 129). Yin (2014, 16) defines a “case study as a form of empirical inquiry” and “notes there are several different purposes that these types of case study might pursue: exploration, description, and explanation.”

### **Law and Document Analysis**

The document analysis helps answer the question: What policies, laws, or other mechanisms are needed to help protect against the grooming process that results in victimization? This data collection supplements the other data to provide context to the environment in which abuse occurs. According to Luton (2010, 143), it is important to understand the original purpose of each document and its impact on the cases studied.

### **Process Tracing**

Process tracing is a method for studying cyber-enabled financial abuse based on individual cases for a sufficient explanation using nonsystematic or case-specific mechanisms. It helps answer the question: What are the grooming mechanisms leading to victimization?

This holistic exploration of the mechanisms of victimization is to build a sufficient explanation of the outcome for a specific case of financial abuse. The intended outcome of process tracing is not to test theories but to provide a minimally sufficient explanation, from a historical perspective, of a particular case by operationalizing the process-tracing theory-building causal mechanisms with observable manifestations (Sil and Katzenstein 2010). Sil and Katzenstein’s (2010) research supports the use of various theoretical constructs in scholarly endeavors and recognizes three common eclecticism

attributes: pragmatic engagement, including the “spirit of fallibilism”; “messy” real-world problems not necessarily narrowly defined in scope; and the interaction of “complex causal stories” without the limitation of traditional analytic isolation (Sil and Katzenstein 2010, 412). The case-specific aspect of explaining process tracing means the explanation is not generalizable. However, analytical eclecticism frames various modes of inquiry to help highlight the implications for policy and the opportunities for change.

Process tracing enabled an understanding of the process of how Americans are scammed, and descriptive case studies are the “systematic inquiry into an event or set of related events which aims to describe and explain the phenomenon of interest” (Bromley 1990). Robert Yin’s (2014) work on case study research helps explain the applicability of the study of human experiences as a methodology to public administration research questions and provides guidance on the process and challenges associated with case studies.

Prior to employing the case study methodology, it was important to assess the research question’s suitability for case study. Yin (2014) writes that a case study is an in-depth investigation of a phenomenon where the research addresses a descriptive (how) or an explanatory (why) question (Yin 2014). Next, the research must ensure the research question is appropriate to capitalize on the strengths of a case study. Accordingly, Yin claims that case studies are beneficial when research examines events that concerns “a contemporary set of events over which the researcher has little or no control” (Yin 2003, 1). The researcher associated with this paper has no control over the process or the ability to conduct experiments in the collection of information. Interviews and collection of relevant policy data and secondary data are the fundamental sources of information.

Yin's case study research design provides a rigorous methodology for clear identification of research needs and data collection requirements. This dissertation examined the scamming process through the various victims and meets Yin's underlying definition for research that may benefit from case study analysis. Yin asserts an adequate case study design has five components: the question, the question's proposition, the unit of analysis, a determination of how the data are linked to the proposition, and the criteria for findings interpretation, which are discussed below (Yin 2003).

The first component is to identify the research question to be examined, which is, How are cyber scammers so successful against older Americans? This question addresses the requirement for examination of the current volume of scams, the laws addressing the scams, the process of grooming, and the experiences of the individuals affected by the scams. The research question underpins the direction of the study as well as Yin's remaining components of research design.

The second component is the development of the study proposition, or the scheme that shapes the study (Yin 2014). The case study method allows direct data collection to understand the first-hand experiences of affected individuals as well as policy and law documents and secondary data. The research question, method, and literature are tied to the conceptual and theoretical framework. The significance of cyber-enabled financial abuse to the affected individuals is central to the study and, therefore, the rationale for this design is to help identify the individual experiences. These rich accountings help the researcher gain a comprehensive understanding of the cyber-enabled financial fraud committed against older Americans.

The purpose of Yin's (2003) third case study research component is to identify and bound the units of analysis. In this study, the cases are bounded by age (60 years or older) and the requirement to have experienced online fraud or attempted online fraud, salient policies and laws, and specific cybercrime data available from the IC3 for 2008 to 2017.

Yin's (2003) fourth component logically links case study data to the study proposition or scheme. Application of this method to the direct collection of affected individuals' experiences identified in Yin's second component is tested by the evidence collected during the research phase. Based on the data identified, the proposition was to be confirmed or denied by the weight of the evidence available. For this study, the cyber-enabled financial fraud of older Americans is confirmed if evidence shows that the grooming processes are successful, but current policies and laws are insufficient or ineffective.

The fifth research component is the formation of criteria for interpreting the study's findings. According to Yin (2003), this step may rely on addressing rival explanations for the study's findings. The major rival theory related to the cyber-enabled financial fraud was the intentionality of self-victimization or lack of sufficient evidence of a grooming process. Data were purposely pursued during the data collection phase, with the theory addressed in the next chapter's findings.

The subject area and specific research question studied fit Yin's definition of appropriateness for examination through case study methodology, and his five research components make up the foundation of the development of a broad approach to data collection and analysis. For the purpose of developing a hypothesis and analysis of

evidence of the causal mechanisms that may explain the cyber-enabled grooming process, the tracing methodology is used. According to Bennett and Checkel (2012), the use of evidence from cases to make inferences for causal explanations has historical roots back to the early Greeks. More recently, cognitive psychology used process tracing starting in the late 1960s as a way to study the grooming process to influence an individual's decision-making. As a political science and public administration research tool today, process tracing uses evidence from a specific case to make inferences about the causal explanations of that specific case (Bennett and Checkel 2012). The method enables the study of divergent inputs that enable a scam to progress from one point to another and attempts to identify the decision-making influences. Outcome-explaining process tracing focuses on the outcome when the mechanisms are critical to understanding the specific outcome. This required describing nonsystematic, case-specific parts that are significant to that particular case (Beach and Pedersen 2013). Process tracing is the appropriate methodology to examine the cyber-enabled grooming process because of the small case sample size and the study's objective of identifying where it may be possible to influence policy and the decision-making process.

A significant advantage of process tracing was the ability to obtain valuable information from small samples. According to Vennenson and Wiesner (2014), when there is a lack of a substantial statistical sample, experiments are neither ethical nor practical, and if the subject under study is of a unique nature then process tracing may be the best method to use. Neither experiments nor statistical analysis of large data sets are possible for this study, therefore, process tracing is the best method to use because it allows conclusions to be obtained from limited data sets. This holistic exploration of the

mechanisms of victimization was to build a sufficient explanation of the outcome for the specific cases of financial abuse. The aim was to operationalize the theory's causal mechanism with observable manifestations. The causal mechanisms were either present or not, and the confidence gained with each case allowed for inferences regarding the sufficiency of the outcome explanation.

Most significant to this study was the potential to identify paths and influences on decision-making. Process tracing examines the interactions between independent variables, actions taken, and the dependent variable (Beach and Pedersen 2013). Bennett and Checkel (2012) claim that a study must meet a three-part standard for good application of process tracing. First, the method is “grounded in a philosophical base that is ontologically consistent with mechanism-based understandings of social reality” (Bennett and Checkel 2012, 25). The study will acknowledge the requirement for these systems and still address the potentially diffuse environment. The third Bennett and Checkel (2012) standard is the serious consideration of alternative pathways through which the outcome could occur (equifinality), which is a principle stating that in open systems an outcome may be achieved via several paths or means. Figure 3 provides insight into the causal mechanisms used by the criminal. This figure indicates paths of activity perpetrated by the criminal. There is no order to the variables, but all must exist. No one variable is sufficient to explain the outcome of cyber-enabled financial abuse of older Americans, but each of the variables is necessary.

### **Conceptual Framework**

Figure 2 illustrates the theoretical framework. Bennett and Checkel (2012) summarize process tracing by describing the method's place in academic use as well as

providing guidance on implementing the method. The authors claim 10 best practices allow for a “systematic, operational, and transparent application of process tracing” (Bennett and Checkel 2012, 21). This study endeavors to apply each of the 10 best practices when exploring the grooming processes:

1. Cast the net widely for alternative explanations.
2. Be equally tough on the alternative explanations.
3. Consider the potential biases of evidentiary sources.
4. Take into account whether the case is most or least likely for alternative explanations.
5. Make a justifiable decision on when to start.
6. Be relentless in gathering diverse and relevant evidence, but make a justifiable decision about when to stop.
7. Combine process tracing with case comparisons when useful for the research goal and feasible.
8. Be open to inductive insights.
9. Use deduction to ask, “If my explanation is true, what will be the specific process leading to the outcome?”
10. Remember that conclusive process tracing is good, but not all good process tracing is conclusive.

Once data were collected, case analysis helped to develop an understanding of the processes, heuristics, and critical elements behind human decision-making through process tracing (Bennett and Checkel 2012). In addition, documented legal proceedings were reviewed and interpreted to give meaning while acknowledging inherent challenges.

To obtain volunteers for this study, the researcher solicited the support of Montgomery County, Maryland, Adult Protective Services (APS), Montgomery County, Maryland, police fraud department, and other personnel. These public servants interact with older Americans and selected participants, which enabled sufficient data to confidently obtain insight into senior citizens' experiences. Interested potential participants were provided with a letter requesting their participation that described the particulars of the study, such as the overall process, the interview process, confidentiality, and identity protection.

Interviews were conducted in a private, quiet setting to reduce interruptions and distractions. Each interviewee was informed of the study's purpose, the researcher's obligation to protect their identity, their right to not answer specific questions, and their right to end the interview at any time. In addition, the participants were provided with an informed consent form to sign and were encouraged to ask questions regarding the study.

### **Types of Data**

The phenomenon of cyber-enabled financial abuse of older Americans is best understood from a myriad of data sources, which when combined provide insight and information.

The first area of consideration was the volume of secondary data from the IC3. This longitudinal data shows the growth of the problem in terms of the number of complaints and financial loss. While not every year is represented, due to variation in reporting mechanisms, from a purely contextual perspective, the data from the IC3 provides tremendous volumetric insight to the problem. The second area of research was the qualitative and quantitative data collected from a survey of a convenience sample of

168 residents of Florida, Maryland, and Virginia. The third area was the interviews with members of a convenience sample of victims and victim advocates that included social workers, law enforcement, friends, and family members. The next set of data came from the criminal actors highlighted in eight cases of cyber-enabled financial abuse of older Americans committed by 26 individuals. These cases were reported as part of the Department of Justice's (DOJ 2018, para 1) public announcement regarding "the largest coordinated sweep of elder fraud cases in history," in which 250 defendants received criminal charges. The selected example cases met the criteria of cyber-enabled financial abuse and were adjudicated by December 2018. The last collected data is a document analysis of the myriad of laws surrounding information and communication technologies (ICT) and cybercrime. When discussing ICT law, there are three overarching categories: computer law, which includes all those laws related to the computer itself; information technology law, which concerns how information is collected, transmitted, and stored; and cyber law or internet law, which governs the use of the internet. Then there are three categories of cybercrime associated with ICT: crimes against property, such as hacking, intellectual property theft, and vandalism; crimes against the government, such as accessing government systems, cyberterrorism, and cyberwarfare; and crimes against individuals, which includes stalking, bullying or harassment, credit card fraud, bank fraud, slander, and manipulation.

### **Data Collection**

The a three-phase data collection process employed quantitative data collection and analysis followed by qualitative data collection and analysis. Quantitative results come from the results derived from the secondary data obtained through the IC3. The

qualitative data collection includes participant-provided cyber-enabled financial abuse narratives, a general survey of individuals of all ages over 18, and a comparative analysis of the most salient overarching laws and policies that shape the cybercrime environment.

## **Data Sources**

Sources of data include law and policy documents as well as published material, such as academic journals, relating to cyber-enabled financial abuse. The literature review is the foundation on which the interview material is built.

Data regarding cybercrime reporting were obtained from the IC3 website for 2008–11 (with the exception of those years for which IC3 data are not adequate for the study). A survey of residents of Florida, Maryland, and Virginia was conducted. Victim advocates, victims, and family members of cyber-enabled crime were interviewed. References for laws and policies come from the European Union, United States, and the Budapest Convention. Case and docket data of adjudicated court cases of perpetrators of cyber-enabled crimes were obtained from the website for Public Access to Electronic Court Records.

## **Data Collection Methods**

Secondary data collected include age and financial loss categories from the IC3. The results of the survey help to identify the scope of the problem and the means by which older Americans became victims. Qualitative inquiry was composed of open-ended questions to help gain insight into the effect internet elder financial exploitation and abuse has on senior citizens. Central to the inquiry were questions such as What led to the abuse? What was the interaction between the perpetrator and the victim? What is

the senior's social infrastructure? What is the interviewee's perception of the financial abuse and how it happened?

### **Data Analysis**

Meaningful statements were extracted from the interview notes. These statements were then organized into categories. The categories are thematic in nature and provide a rich context for the experiences. The three stages of the process-tracing theory-building methodology require the explanation of key theoretical concepts derived from existing literature to discern variables, which indicate possible underlying causal mechanisms among the variables (Beach and Pedersen 2013). The second stage infers the existence of the underlying causal mechanism, and the third stage, a link between the indicators and variables, helps to build the theory, which in this case concerns cyber-enabled elder financial abuse.

Process-tracing theory-building allows for the application of other theories, such as routine activity theory. In routine activity theory, three criteria must exist simultaneously for a crime to be committed: a suitable target, no capable guardian (e.g., police or security), and a motivated offender (Cohen and Felson 1979). Bossler and Holt (2009) established that routine activity theory is applicable to cybercrime.

### **Assumptions and Strengths and Limitations of the Study**

#### **Assumptions**

A significant challenge for this research was collecting data from perpetrators, which was difficult, expensive, and possibly dangerous. The researcher assumed that representations of the individual's experience would be realized from face-to-face or telephonic interaction, family members, government agencies such as APS and law

enforcement, and the researcher's own interpretations of the interviews. It was assumed that the proposed sample size of 15–20 adults was sufficient to enable rich contextual descriptions.

### **Strengths and Limitations**

The strength of a qualitative phenomenological study is in the ability to gain the individual's perspective on events and, in this study specifically, the ability to affirm or disprove the theory of cyber-enabled financial abuse of the elderly.

The use of a small sample of 10–20 people limits the inferences and outcomes possible between the study's findings and the larger population of victims. A nonprobability nonrandom sampling technique was chosen for a couple of reasons. First, the entire set of victim cases is unknown and perhaps unknowable, since it is estimated from only a small population of people who report victimization. Second, a probability sampling where all victims had an equal chance of being selected was unprovable. Third, nonprobability sampling, such as convenience sampling, is often used to examine real-life phenomena when it is not necessary to make statistical inferences in relation to the wider population (Yin 2014). As the name implies, convenience sampling is obtained by selecting whoever is conveniently nearby and willing to answer a questionnaire. However, in a process-tracing methodology, each case is unique and is not generalizable, therefore there are no statistical inferences in relation to the wider population. The interviews and surveys provide insight into an understudied real-life phenomenon; therefore, their biases do not affect the study.

## **Results**

This chapter reports results from the collection of several streams of data: information gathered from the Internet Crime Complaint Center (IC3) regarding the growth of cyber-enabled financial abuse, a survey to assess the understanding of internet content and attitudes toward scamming of older Americans, case studies of victims based on the interviews, the results of adjudicated criminal court cases perpetrated against older Americans, and an examination of the laws surrounding cyber activity and criminal court cases of cybercrimes perpetrated against older Americans.

To accomplish this task, the chapter is divided into sections. The first section summarizes IC3 data. The second section presents the survey results. The third section examines the interviews with victims, family members, victim's friends, law enforcement, and social workers. The fourth and final section analyzes criminal cases and laws.

To ensure a full accounting of relevant documents, the researcher used a document collection matrix for each of the data and information streams: victims, criminals and laws, IC3 data, and survey results. Process-tracing required the explanation of key concepts derived from existing literature to develop the theory. The theoretical concepts, represented by variables, indicate the possible underlying causal mechanisms among the variables. The link between the indicators and variables builds the theory of cyber-enabled elder financial abuse. This multistream investigation includes a discussion

of the analysis and how it ties back to the original research question: How are cyber scammers so successful against older Americans? To reach the fundamental issues of this question, the research will examine the following key questions:

- What are the grooming mechanisms leading to victimization?
- What are individuals' perspectives of victimization?
- What policies, laws, or other mechanisms are needed to help protect against the grooming process that result in victimization?

### **Internet Crime Complaint Center Results**

The IC3 provides a portal for reporting cyber-enabled financial crimes, and according to the IC3 (2019) it has received 4,415,870 complaints since 2000. This compilation of victim-supplied cyber-enabled crime complaints includes illegal activity involving one or more components of the internet, such as websites, chat rooms, and/or email where intentions to defraud are communicated (IC3 2019). While not every year is represented, because of variation among reporting mechanisms, for a purely contextual perspective, the data from the IC3 provide tremendous volumetric insight to the problem.

Table 4 reflects the dollar value of the complaints received by the IC3, which the Federal Bureau of Investigation (FBI) indicates may be as little as 15% of the actual loss for a myriad of reasons, including victims not knowing where to report the crime, victims blaming themselves, and victims being embarrassed.

Table 4. Loss of funds reported to the Internet Crime Complaint Center in 2012 and 2014–2018

	Complaints	Funds	Funds by age group					
			< 20	20–29	30–39	40–49	50–59	> 60
2012								
Florida	18,903	34,419,348.21	409,542	3,231,049	5,021,487	8,696,355	7,268,943	9,791,971
Maryland	6146	9,763,989.79	102,218	1,447,275	2,083,692	1,835,062	2,411,650	1,884,093
Virginia	7812	12,111,084.23	108,023	1,186,651	1,255,665	3,016,073	3,121,927	3,422,746
US total	236,994	413,543,115.07	4,020,853	35,837,082	62,266,882	93,711,999	115,146,596	99,933,198
2014								
Florida	18,637	52,544,107.00	326,966	3,417,802	6,805,746	10,352,524	16,980,579	14,660,491
Maryland	5677	9,009,877.00	146,320	850,223	1,622,351	1,802,856	2,592,475	1,995,653
Virginia	7112	16,571,859.00	120,854	950,723	3,187,823	4,292,038	4,018,075	4,002,346
US total	223,113	641,369,215.00	4,389,942	38,755,681	109,524,072	147,110,762	174,610,699	166,278,074
2015								
Florida	20,306	94,526,977.00	290,217	2,686,216	10,409,726	26,610,063	17,083,620	37,447,134
Maryland	5944	16,071,212.00	99,496	849,365	1,228,174	2,719,743	5,369,210	5,805,224
Virginia	7534	20,098,497.00	106,494	1,219,284	2,546,170	4,455,484	6,552,698	5,218,367
US total	239,811	898,639,674.00	6,904,194	52,019,481	112,206,388	223,829,985	251,385,869	252,293,758
2016								
Florida	18,890	79,806,106.00	387,232	3,895,689	15,198,523	18,918,834	18,871,419	22,534,409
Maryland	7176	22,072,669.00	118,989	928,791	2,403,538	3,694,587	11,113,811	3,812,953
Virginia	7137	47,274,220.00	151,736	1,364,861	28,030,796	4,461,526	5,735,006	7,530,295
US total	230,450	969,354,172.00	5,868,335	48,062,651	158,408,530	179,055,593	255,206,557	314,857,029
2017								
Florida	17557	84,817,598.00	379,944	4,932,068	11,140,213	16,142,947	23,321,944	28,900,482
Maryland	4383	25,172,078.00	608,566	782,095	1,258,126	8,506,127	5,155,139	8,862,025
Virginia	5964	29,436,754.00	142,300	1,115,340	2,536,437	4,602,034	12,436,899	8,603,744
US total	214,226	968,421,004.00	7,131,049	56,150,203	130,281,109	216,793,427	247,722,771	310,342,345
2018								
Florida	18,480	151,079,348.00	399,158	7,742,434	16,162,119	23,479,464	54,170,691	49,125,482
Maryland	4705	26,908,854.00	146,941	1,297,546	2,328,332	7,170,652	6,249,771	9,715,612
Virginia	6548	34,167,640.00	144,718	1,421,617	3,033,899	8,504,840	7,374,062	13,688,504
US total	234,365	1,781,496,466.00	10,953,492	117,214,302	236,404,411	357,750,340	451,280,452	607,894,469

The total loss to individuals has increased for every age group. Seniors absorbed the largest increase in 2018, while the number of complaints did not increase comparatively. Figure 5 shows the median amount loss per referred complaint across the years for individuals aged 60 years and older. The figure shows the rise in the loss per complaint.

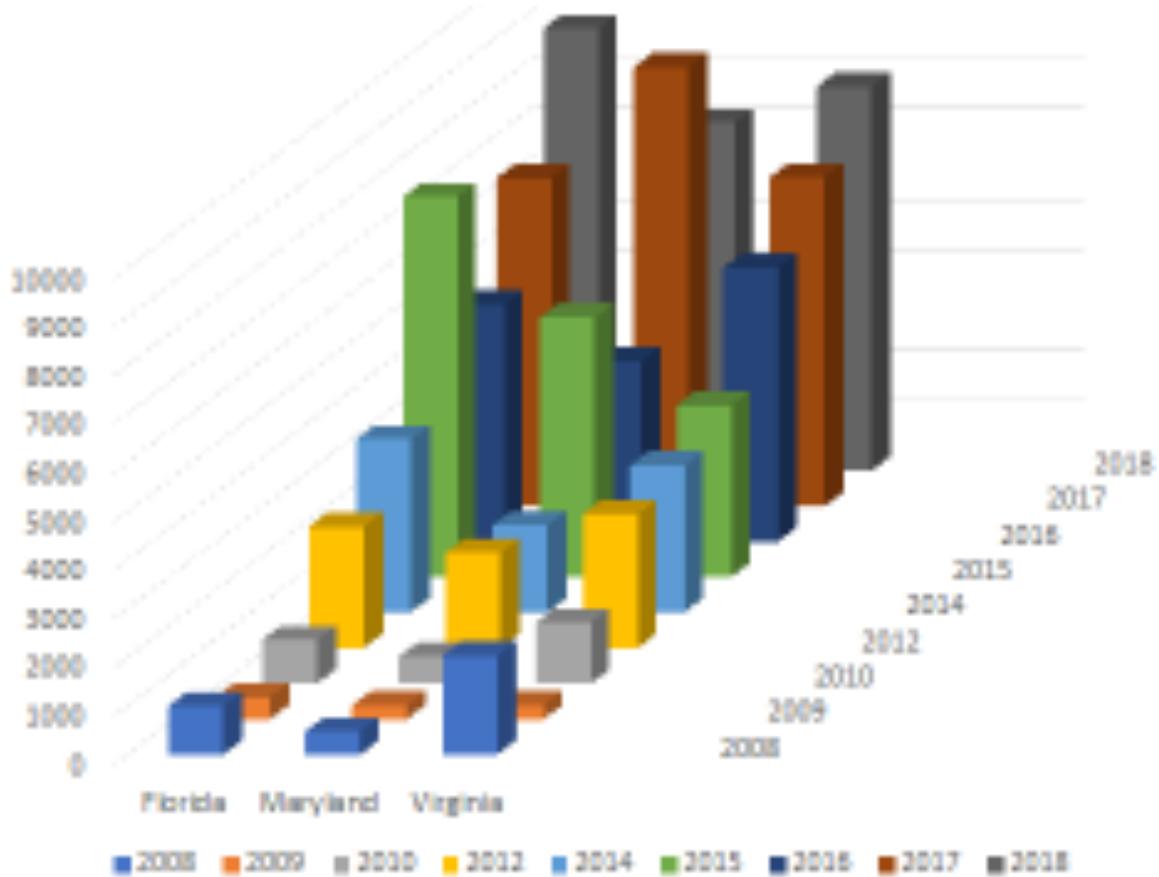


Figure 5. Median amount lost per referred complaint for Florida, Maryland, and Virginia. Data from the Internet Crime Complaint Center.

In other words, the total number of complaints did not rise in step with the total monetary loss. For seniors over the age of 60 years, the number of complaints fell from 2012 to 2018, but the reported loss for this age group increased by close to 21% over the

same period. Figure 6 shows the stability of the number of complaints for the three states studied and the entire United States.

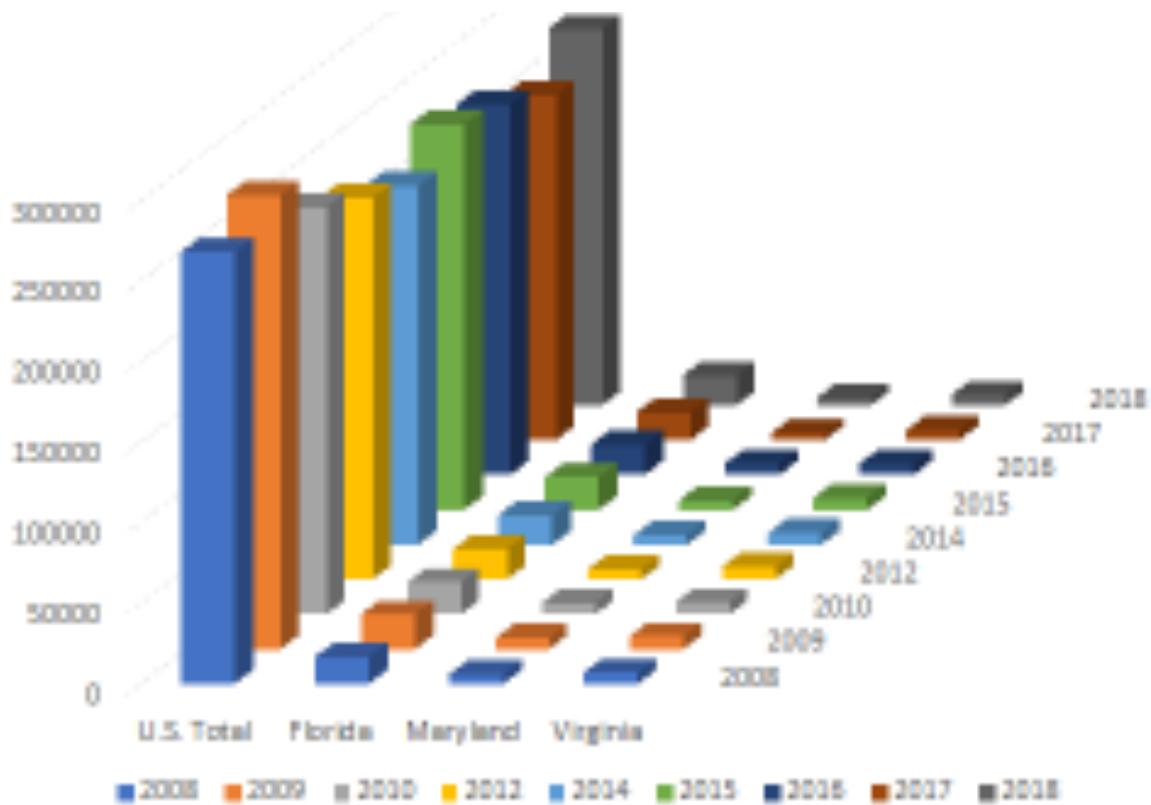


Figure 6. Total number of complaints regardless of age for Florida, Maryland, Virginia, and the United States. Data from the Internet Crime Complaint Center.

Figure 7 is a depiction of the total number of complaints, in thousands, against the total losses, in millions of dollars, across all 50 states for each year over a single decade. Each of the reported years shows approximately the same number of complaints made to the IC3, while the financial loss per year increases substantially throughout the decade.

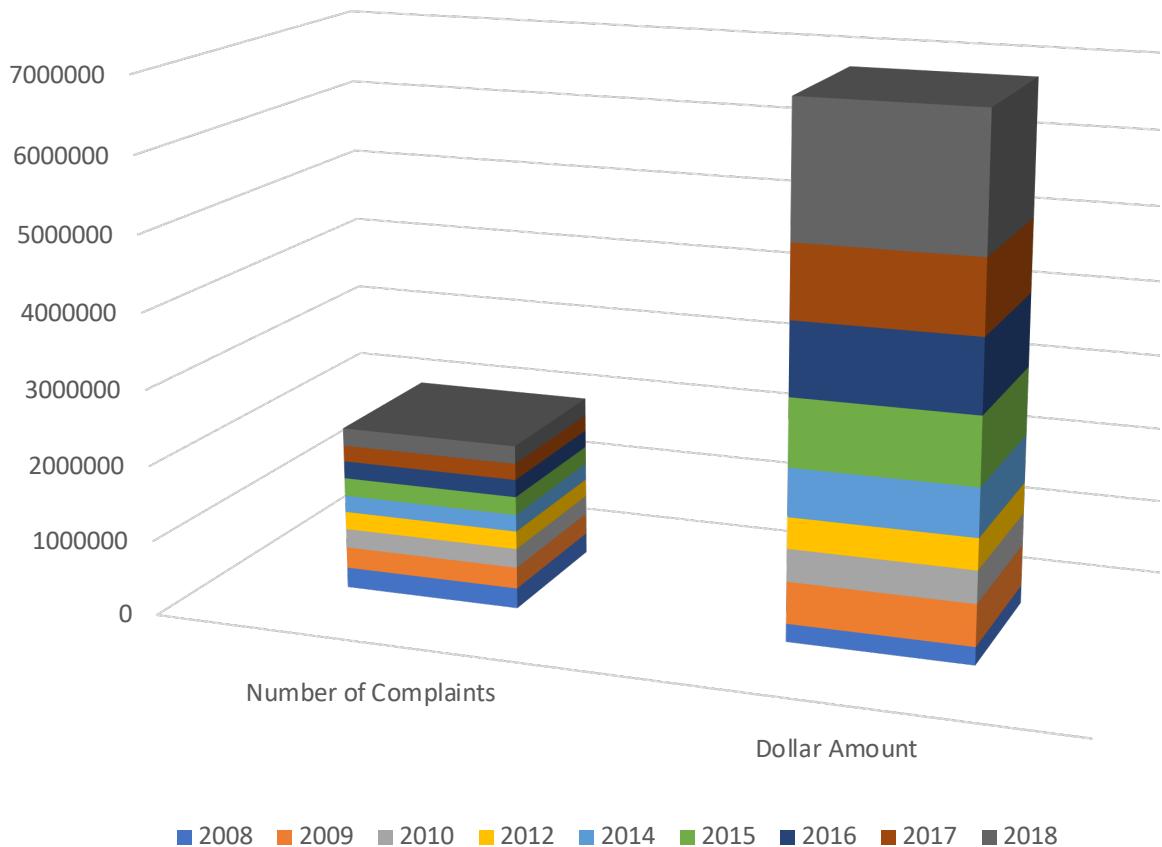


Figure 7. Dollar values in millions for all age groups across 50 states. Data from the Internet Crime Complaint Center.

In the last decade, the IC3 received an average of 900 complaints each day, making the internet a web of profit for criminals (IC3 2019). While there was an increase in the number of complaints received by the IC3 over the last decade, the substantial increase in financial loss attributable to abuse is indicative of a successful, sophisticated, and systemic cybercrime problem perpetrated against the American citizenry.

### **Survey Results**

The survey helps to assess the opinions, attitudes, and knowledge of cyber-enabled elder abuse across a wide age spectrum of adults over 18 years of age. The purpose is to extract specific data to increase understanding of the phenomenon of cyber-enabled financial abuse. Surveys were administered between February 2019 and March

2019 to residents of Virginia, Maryland, and Florida aged 18–90 years. The surveyed Florida, Maryland, and Virginia residents resulted in 168 responses to a subset of the predetermined set of interview questions sanctioned by the institutional review board. The questionnaire was provided at public events without prequalification or restriction of participation other than that the survey taker needed to be over the age of 18 years. It was not practical to randomly select a representative subset of all Florida, Maryland, and Virginia residents so that every resident had an equal chance of selection.

The survey investigated whether individuals believed the following information about citizens was on the internet: name, address, age, telephone number, social security number, income, marital status, names of family members, favorite TV show, favorite web sites, credit score, home value, education level, employment status, political affiliation, criminal history, tax history, books read, and photos. Participants were given the opportunity to provide written comments for the three open-ended questions at the end of the survey. As expected, the comments ranged in length from a single word to several paragraphs.

SPSS software was used to analyze the results of the survey. Crosstabulations were conducted to explore bivariate relationships between age and perception of data available on the internet.

### **Characteristics of Respondents**

No demographic information other than age was collected.

Figures 8 and 9 show the age groups of the survey participants. Approximately half of respondents were in their 50s or 60s.

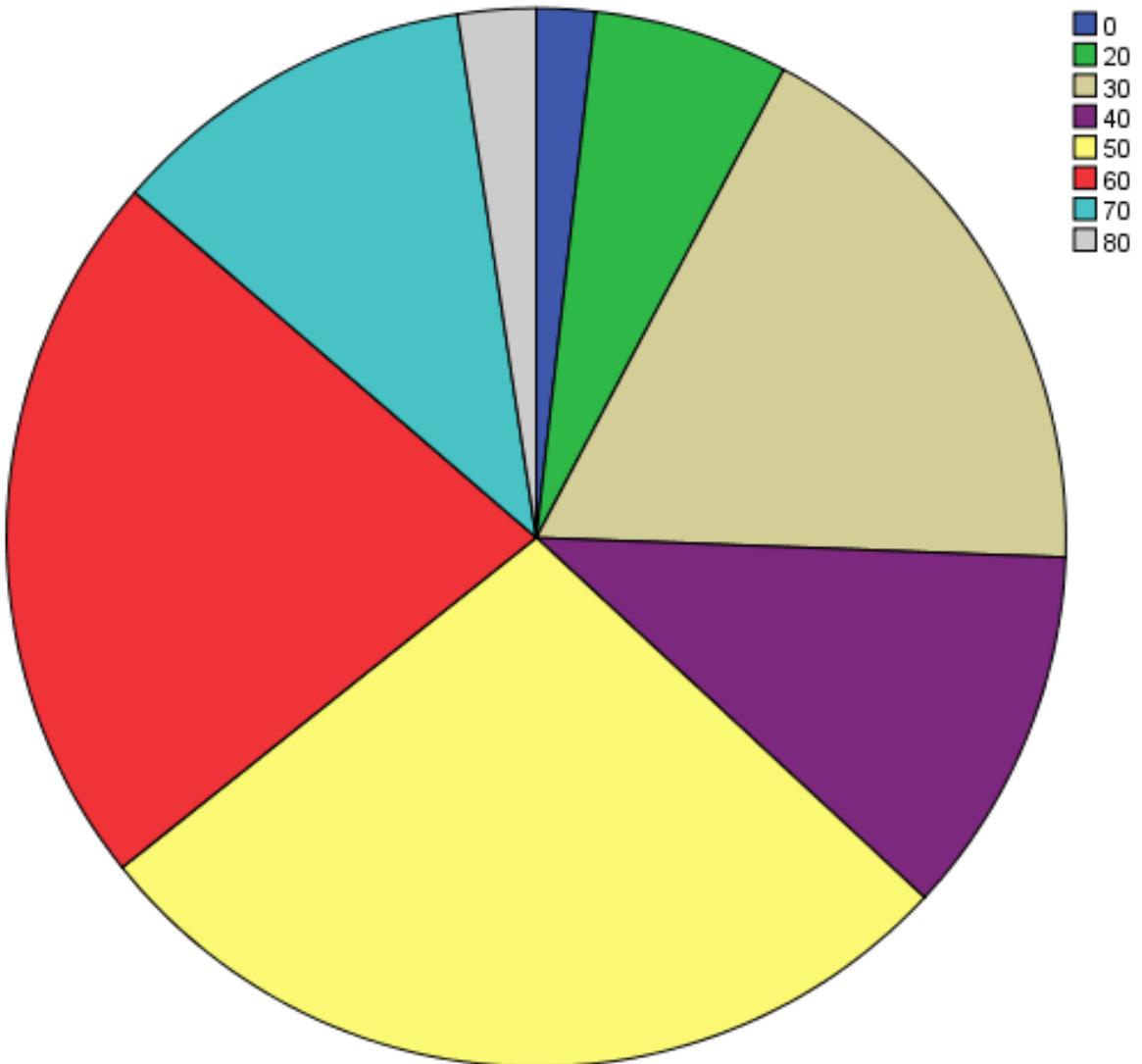


Figure 8. Age groups of survey participants.

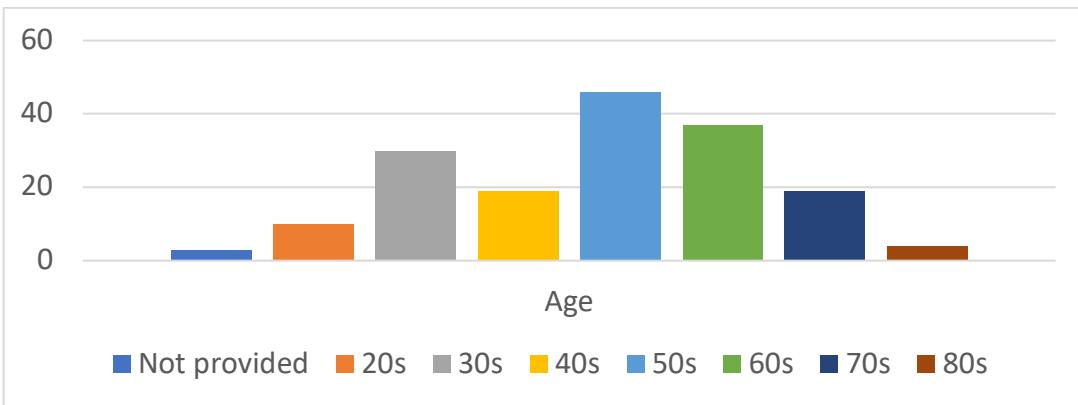


Figure 9. Age groups of survey participants.

The first set of survey questions addressed what types of information the respondents thought were legally<sup>55</sup> available on the internet.

The ordinal variable *age range* was reduced to a dichotomous variable—ages 59 years and younger were recoded into the numerical representation 1, and ages 60 years and older were recoded into the numerical representation 2. Crosstabulations allowed for the exploration of specific characteristics about the relationships between the data categorized as a dichotomous variable.

The survey data shows few differences in perspectives between respondents aged under 60 years and those aged 60 years and older. Figure 10 denotes the percentage of 108 respondents under the age of 60 years and the percentage of 59 respondents aged 60 years or older who responded in the affirmative for each category of information. Interestingly enough, the proportion of those who thought that their employment status, credit rating, income, tax history, and social security number were on the internet was higher among the older respondents than among the younger respondents.

---

<sup>55</sup> As an example, child pornography is not legally available on the internet.

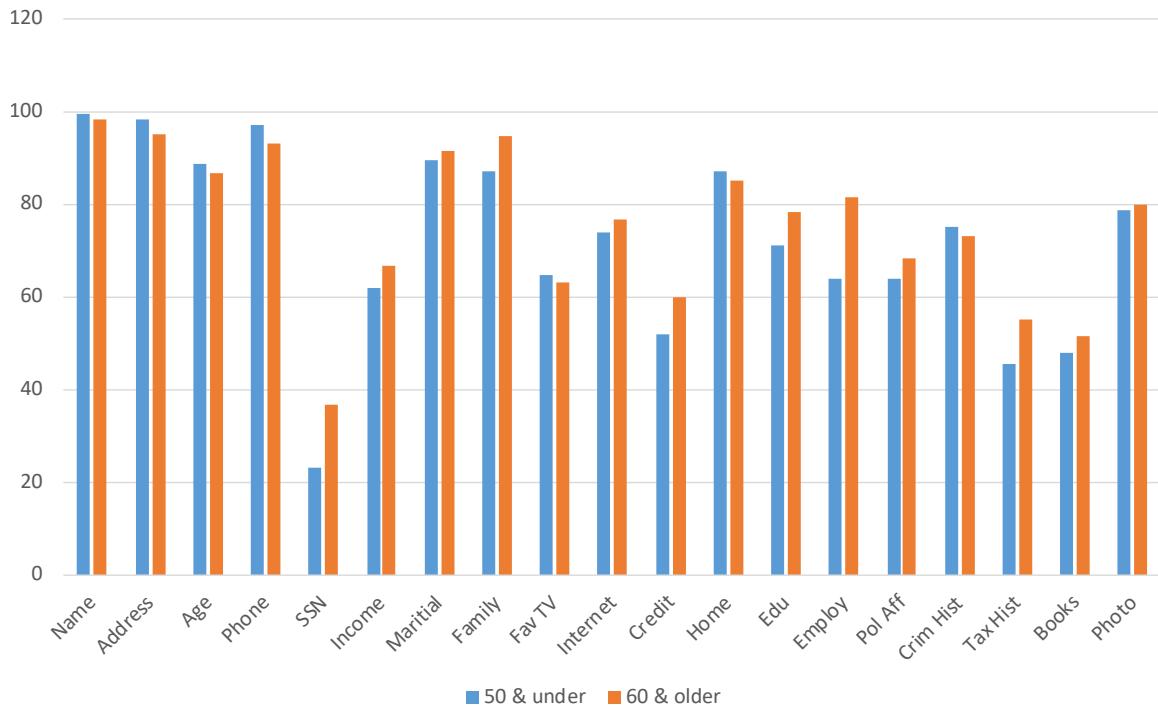


Figure 10. Percentage of different age groups responding yes to questions

Figure 11 shows that the proportion of those who believe people aged 60 years and older are vulnerable is similar between the younger and older groups, but the proportion of those who believe people aged 60 years and older are highly vulnerable is higher among the younger group than among the older group.

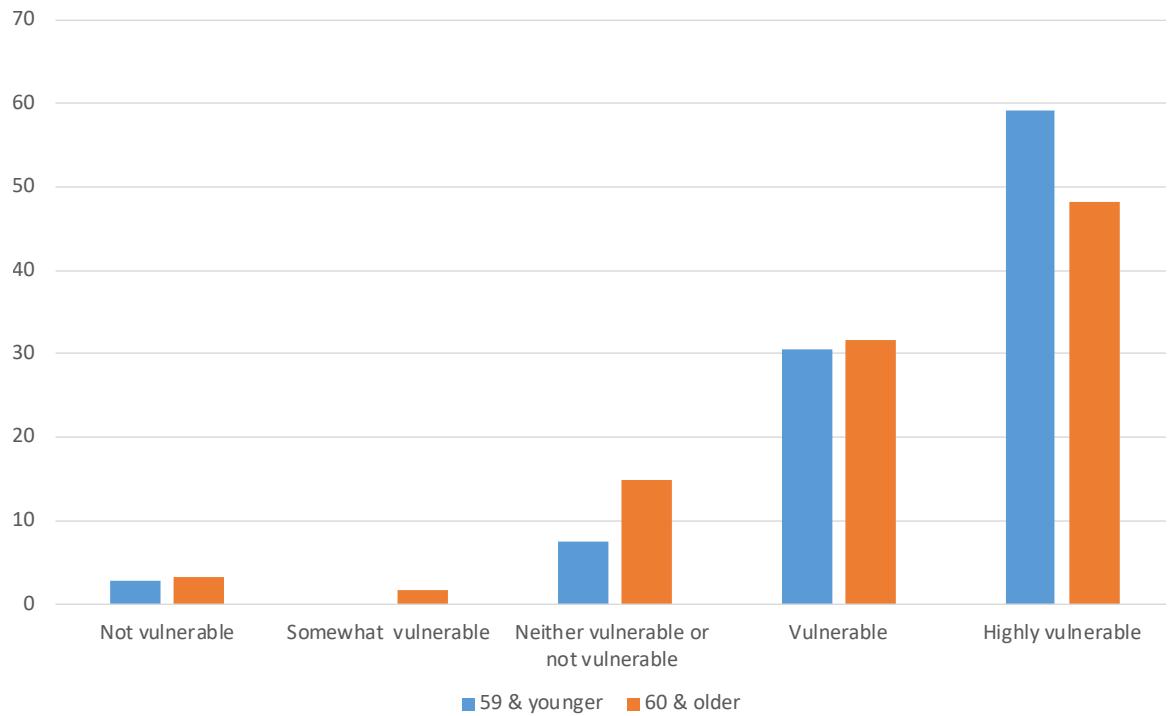


Figure 11. Perceived vulnerability by age group

Regardless of age, most respondents recognize the danger cyber-enabled financial abuse.

Participants were asked, How does no longer participating in the workforce contribute to the likelihood of victimization? One hundred five of those aged under age 60 years responded to the question, as did 58 of those aged 60 years or older. Figure 12 shows the percentage of respondents within the two age groups who perceived that older Americans' status as not being part of the workforce contributes to their likelihood of victimization.

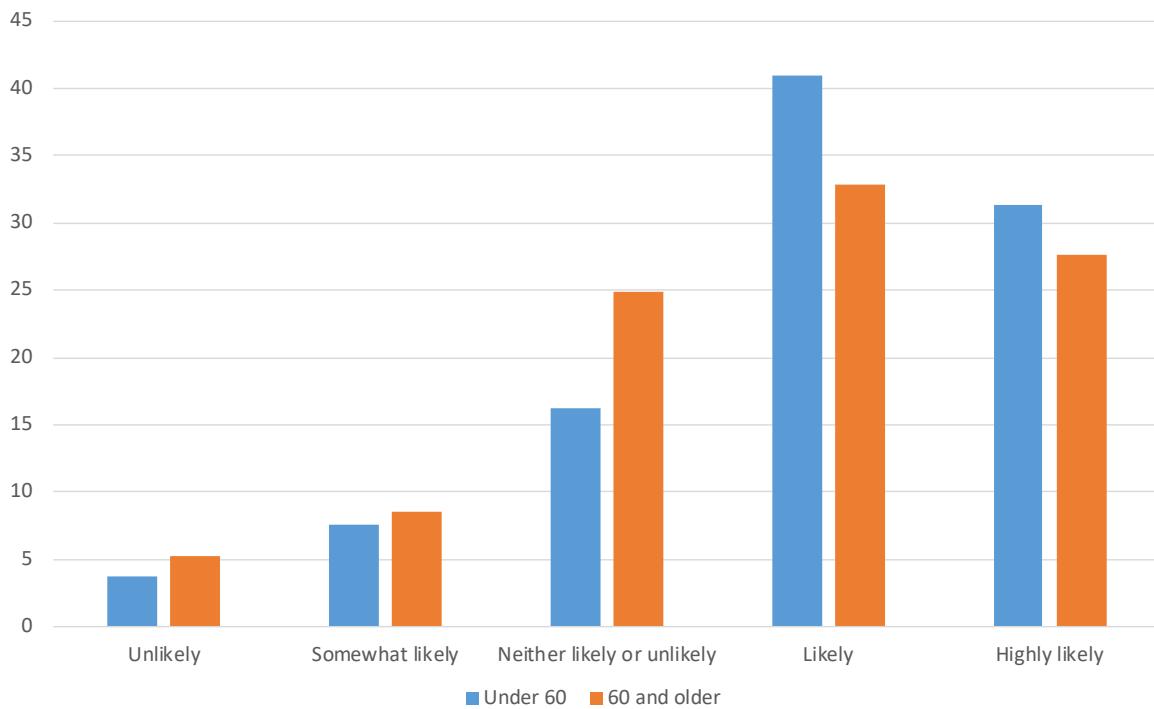


Figure 12. Not being part of the workforce by age group

The last question asked, What is the likelihood of an older victim losing their entire financial savings and requiring public assistance? One hundred six of the respondents under 60 years of age responded to this question, and 59 of those surveyed aged 60 years and older answered this question. Figure 13 shows that there is a wide disparity in the answers.

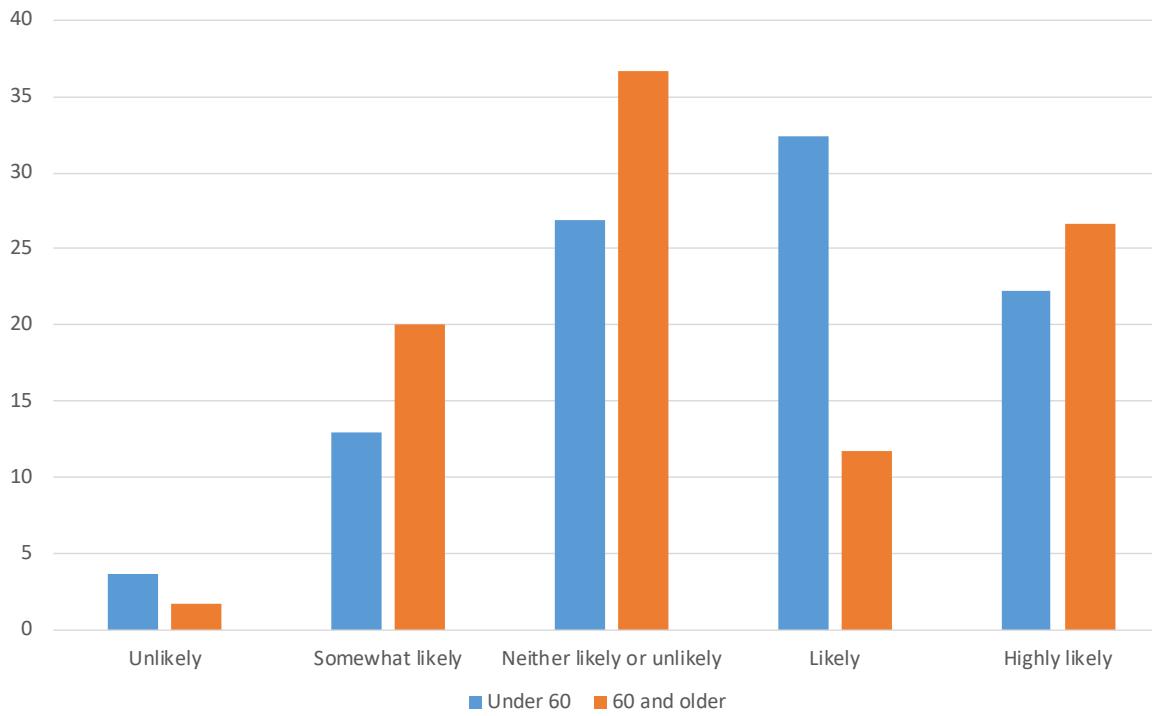


Figure 13. Victims who may require public assistance by age group

When the data are limited to a three-point rating scale, it is clearer that those aged 60 years and older do not believe public assistance would be as necessary as those aged under 60 years would (figure 14).

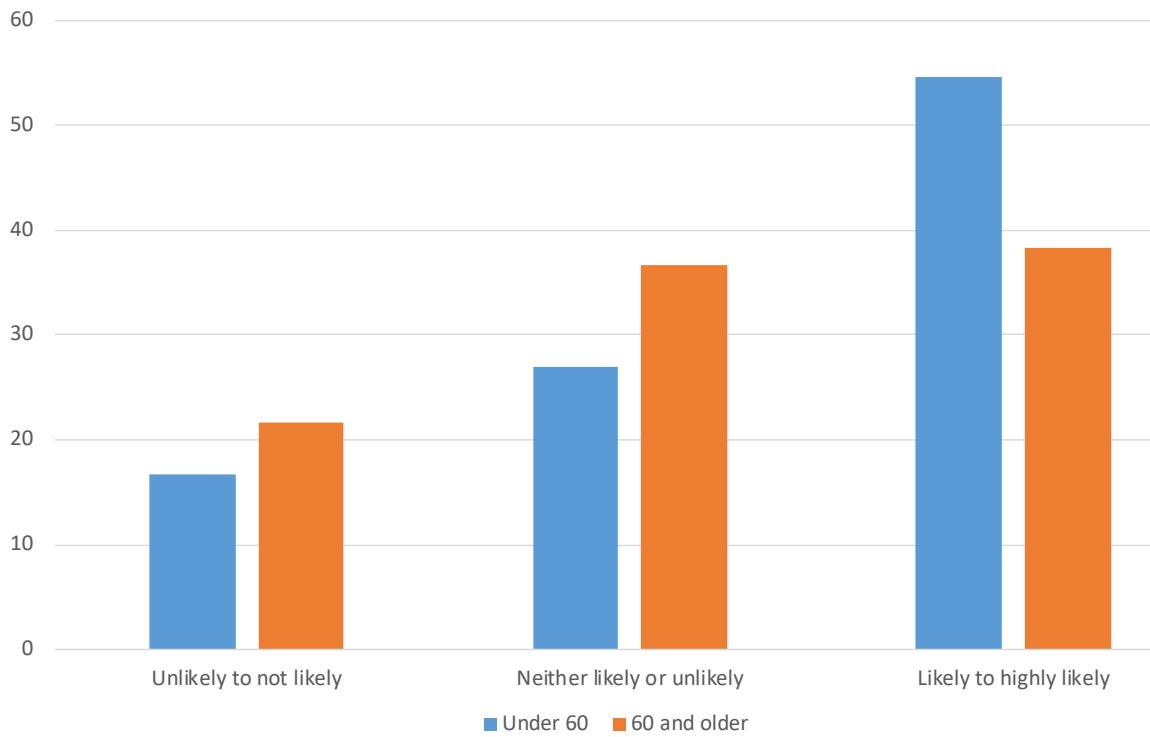


Figure 14. Three-point rating scale by age group

Figures 15 and 16 indicate how significant the perception of vulnerability is in terms of either not being vulnerable or being highly vulnerable to cyber-enabled financial abuse. Individuals were asked to evaluate quantitatively how vulnerable people aged over 60 years were to cyber-enabled financial abuse. To help capture the intensity of agreement or disagreement with the statement, a five-point rating scale was used. Figure 16 shows the age distribution of the respondents answering the question concerning vulnerability of citizens over the age of 60.

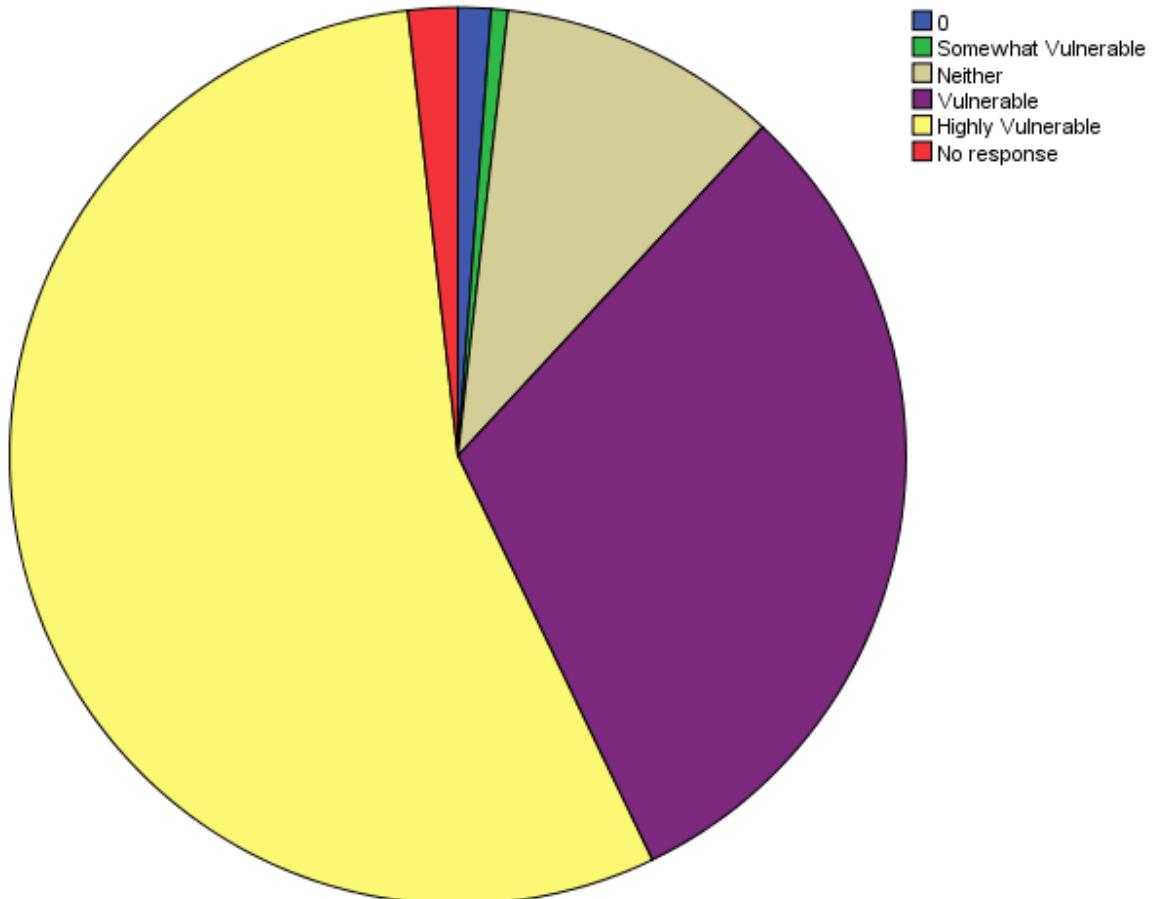


Figure 15. Vulnerability

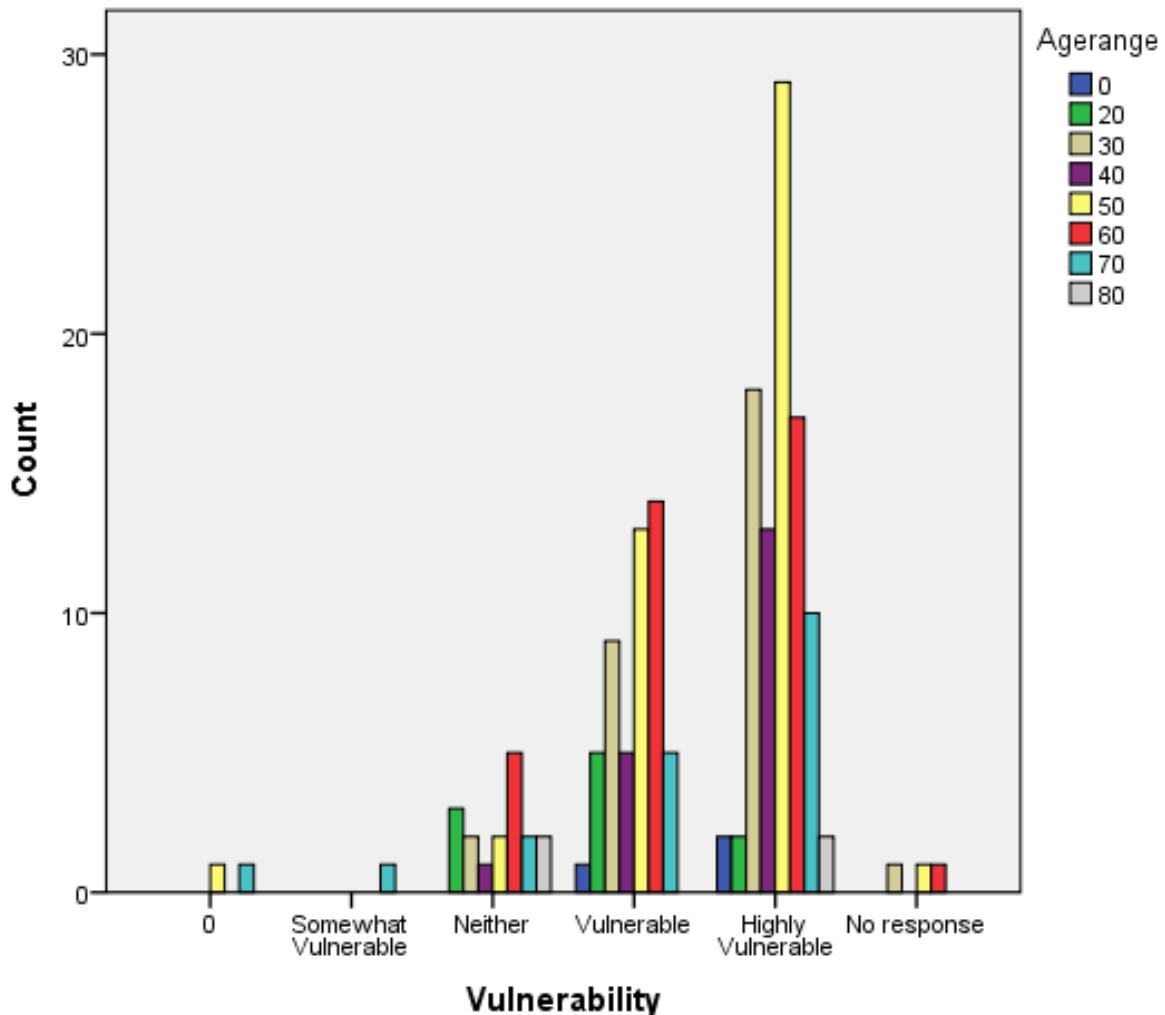


Figure 16. Vulnerability by age range

Participants were given the opportunity to provide written comments for the three questions at the end of the survey. This visual expression of this in figure 17 is referred to as a *word cloud* or *text cloud*, and it is used to provide insight into the themes which emerged from text survey's responses. The survey data revealed responses that represent the opinions, beliefs, and perspectives of a group of individuals comprised of both men and women aged 18 years of age or older from Florida, Maryland, or Virginia. The word cloud is useful for visually identifying the commonality of word themes associated with the responses from survey participants. The words represent those most frequently expressed in the text of the survey responses. While the placement and angle of each

word has no significance, the font size of the word is significant in that it shows how often the word appeared (common words such as *the, a, and, he, she*, etc. are excluded). This data visualization depicts the emphasis on certain key words: *victim, money, scam, call, bank*, and *on-line*. There was lesser, yet still important, emphasis on words such as *card, family, scammer, account, wife, help, sent*, and *claim*. Those most frequently used words construct a clear theme from the respondents' sentiments of what is most important to the entire group of respondents in their combined thinking.

## Sentiment from the Survey



Figure 17. Word cloud

### **Interviews and Case Study Analyses**

A rigorous human subject research plan was established to afford protection to all those involved in the conduct of this research. The researcher has a responsibility to conduct research involving human subjects in an ethical manner. Therefore, this study was conducted in accordance with the common rule (DHHS 2009) and *The Belmont*

*Report* (DHHS 1978). This research was approved in September 2018 and complies with the pre-2019 requirements of the common rule (DHHS 2009), with regard to research involving human subjects. However, one important feature of the new standards included in this study is that the text at the top of the informed consent form provides important information regarding the study. There are three fundamental ethical principles required by *The Belmont Report* for human subject research. The first principle is to respect the individual by protecting the rights and welfare of the participants, which incorporates the ethical requirement to treat individuals as autonomous agents and allow them to make their own decisions with regard to their personal information; in other words, respect for privacy by means of confidentiality and anonymity. The principle of beneficence requires the researcher to minimize harm while maximizing possible benefits. The principle of justice requires fair treatment in which vulnerable populations are not exploited. To ensure this research met these requirements, the researcher's study was approved by the University of Baltimore's institutional review board. The second step was to obtain informed consent from all interviewees. As part of the informed consent, the participants were given the researcher's name and telephone number as well as the name and telephone number of this dissertation's committee chair. The time and location of the interviews were at the discretion of the interviewees. All participants were informed that at any time they could stop the interview or refuse to answer any specific question without condition.

As demonstrated in the body of this research, reconstructing who the victim is depends greatly on the level of demographic material provided. Because several of the actual victims' families do not know the extent of the scams, the biographical information

on each individual in this report is limited. This is in keeping with the researcher's pledge to the victims, social workers, law enforcement, friends, and family members to restrict the demographics provided on individual cases so as to prevent reconstruction of their identities and avoid potential harm or discomfort. The interviews were conducted with members of law enforcement's fraud department, social workers who work with victims, family members or friends of victims, and victims. The victim group was chosen due to the potential severity of the impact to financial well-being, in that citizens over the age of 60 years have a reduced ability to obtain employment or other means of compensating for the financial loss. Victim interviews were conducted on a one-on-one basis, and the interviewer captured detailed notes, which were shared with the interviewee after completion of the interview to ensure accuracy.

### **Characteristics of the Victims**

There were 28 interviews, representing 23 instances of abuse and one case of foiled or averted abuse. The interviews exposed issues related to the process of abuse and reflect the experiences of the victims. Victims lived in Florida, Virginia, and Maryland during the time of the scams. There were 14 females and 14 males; four of the 28 were couples. While some victims and their families are not sure of the total financial loss, those financial losses that are known range from \$4,000 to \$1.5 million. In many cases, the size of the loss is less important than the end result, which is financial desperation for the victim and, often, their family.

Figure 2 illustrates the theoretical framework. Financial abuse is a process of the often-offered explanation of a single cognitive mistake on the part of the victim. The phenomenon is more complicated as shown by the below eight selected interviews of

what Denzin (2001) referred to as a *thick description*. Each victim's experience is different enough so as not to be generalizable, but the categorization of the variables provides insight into the process. The key data from the interviews were identified and coded. The grouping of the codes provided insight into several concepts that were categorized in groups supporting the theory of cyber-enabled financial abuse of older Americans.

Section 1 is comprised of a synopsis of the eight interviews with the interviewer's insight provided first, followed by a depiction of the process in a diagram of the ontology of grooming, and last part is a description of the interview. Section 2 contains the sole interview of someone who was almost a victim. Section 3 has the rest of the interviews, which, while emblematic of abuse, were not robust enough in detail to be included in section 2. Table 5 depicts the case moniker or coding scheme name, type of scam, and the amount of the loss, if known, for each case.

**Table 5. Moniker, type, and loss for each case**

Moniker	Type						
	Romance / companionship	Technology help	Parent / grandparent	Business / investment	Ancestry.com / family / friend in need	Lottery scam	False ID / theft / blackmail
	Loss (\$)						
Section 1							
N1		X					> 30K
O1				X			> 300K
F1	X						1.5M
P1	X						-80K
E1			X				7K
A2	X			X	X	X	> 50K
H1		X					-4K
G1	X						~600K
C2		X					> 41K
Section 2							
J1		X					0
Section 3							
A1		X					— <sup>a</sup>
A3					X	X	2.5K <sup>b</sup>

					Type	Ancestry.com / Romance / Moniker companionship	Business / Technology help	family / friend Parent / grandparent investment	Lottery in need	False ID / theft / blackmail	Loss (\$)
B1			X								27K
B2			X								-9K
B3					X						126.5K
B4			X								10K
B5									X		752K
C1	X										> 100K
D1	X										-110K
I1				X							-1M
I2	X										— <sup>a</sup>
K1	X				X						-80K
L1	X				X						— <sup>a</sup>
M1	X										> 50K

<sup>a</sup>Unknown. <sup>b</sup>Partly unknown.

## Section One Interviews

Cyber-enabled financial abuse is a criminal process perpetrated by a criminal vice with the often-assumed explanation of a cognitive mistake on the part of the victim. The phenomenon is shown in this section of eight individual interviews in what Denzin (2001) referred to as a *thick description*. Each victim's experience is different enough so as not to be generalizable, but the categorization of the variables provides an understanding of the process. The key data from the interviews were identified and coded. The grouping of the codes provided insight into several concepts, which were categorized in groups that support the theory of cyber-enabled financial abuse of older Americans. Interviews in this section were conducted with social workers from Montgomery County, Maryland, Adult Protective Services (APS), members of the fraud department of Maryland's Montgomery County Police, victims' family members, victims' friends, and victims.

## **N1**

N1 is a retired widower who lives alone and was scammed out of at least thirty thousand dollars. He has a caring family, some of whom live near him.

This victim received a pop-up message when he was on a website on the internet. The message indicated his computer was infected with a malware, needed immediate attention and provided a phone number for him to call, which he did. The pop-up looked very professional, as though it was coming from a legitimate technology company. He felt compelled to follow the “technician’s” instructions as it was too hard to close the window with the pop-up. The “technician” was professional, extremely knowledgeable, and very nice, especially offering a significant amount of information and spending a great deal of time with him on the telephone. During the many conversations, the criminal was able to gather information about the victim’s understanding of the technology and his need to have his computer work properly again, since it was a major source for his entertainment. The conversations lent themselves to the criminal ascertaining the victim’s financial status and ability to provide funds and draw on other assets he had available to him. Through their data gathering process, the scammer was able to earn the victim’s strong trust and learn about his belief in others and his cognitive ability to follow and accurately discern the quickly changing elements of the scheme. For example, the scammer used the over/underpayment fraud scheme where the criminal claims the victim has to pay and then claims they paid too much and need to be refunded. The victim became overwhelmed trying to calculate his finances, and he eventually provided the scammer with his bank account information including the passwords. In addition, the scammer captured other personal information regarding the victim’s

computer use, which indicates they may have installed spyware on his computer. The family believes the scammer learned, during the information gathering phase, that the victim was either frequenting a pornography site or was online with someone discussing pornographic content. The family also believed the scammer was blackmailing him. The scam became known to the rest of the family when the victim's sister demanded to know why he was repetitively making requests from her for money, which amounted to several thousand dollars.

The victim admitted to being embarrassed by the scam, and he felt helpless to remedy his new financial dilemma. While he did not say he was scared, he admitted he was concerned the scammers knew where he lived.

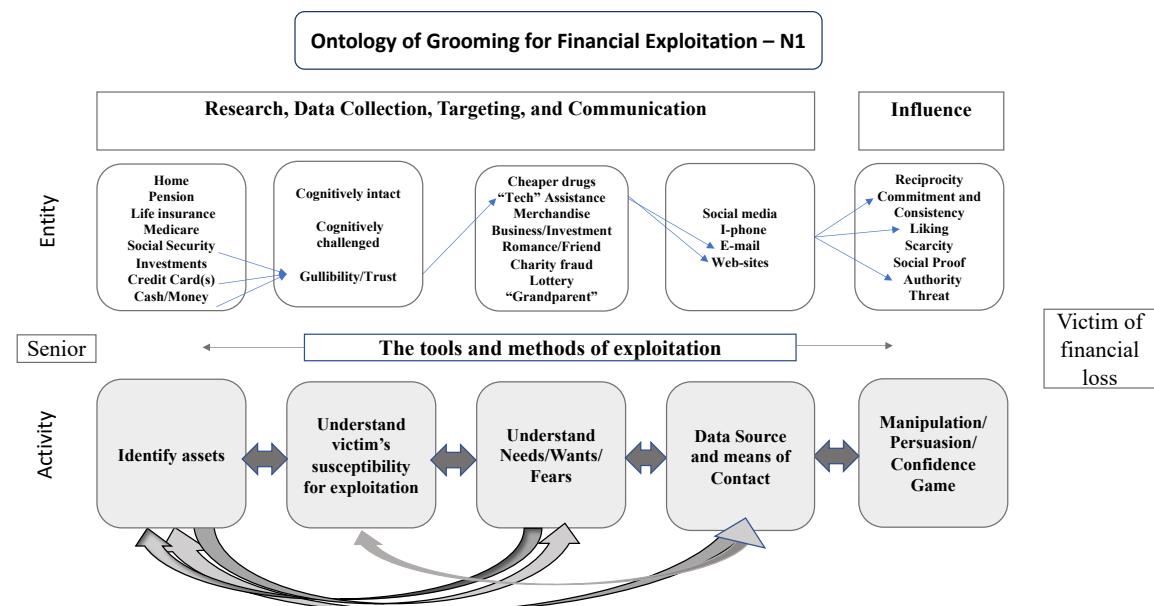


Figure 18. Application of the theoretical framework to case N1

#### *Victim Interview*

The interview lasted about two hours. He uses the laptop computer to go onto the internet daily for news and weather, although he gets most of his news from television. In addition, he occasionally is active in reading and sending emails. He does not

communicate with others in chat rooms or use any form of instant messaging. He does not participate in any online groups such as Facebook, Twitter, or any other types of social media. He does not request any assistance or information online for his household needs, finances, errands, or pet care. He does not use the internet for banking, but he does use the internet to correspond with his doctor and the doctor's office services.

He was contacted online and then by telephone calls. He was told this company, 360 Tech, was monitoring online hacking activity and that his computer was being hacked. The company representative offered to help protect the computer with software and a service. He said they found things in the computer that caused it to be vulnerable to hacking. They would speed up the computer and get rid of any "bug-a-boos" that caused any problems. The company representative appeared to be very knowledgeable and competent, and they seemed to know a great deal about his personal computer. He never met anyone in person, even though the business relationship spanned approximately six months.

During the course of the scam, he spoke with two individuals, Alex and Peter William, who were very professional sounding. On June 14, 2018, the victim received nine calls insisting that he purchase \$4,000 in gift cards to pay for the computer service. On June 15, 2018, Alex called instructing the victim to send \$4,000 more, and he informed the victim that he would receive a refund of the first payment because there was some mistake. According to the victim, the calls were nonstop, even claiming that the FCC had been called and he was threatened with jail. One of the scammers continued to call until 12:30 a.m. on June 16. At 12:57 a.m., the victim was informed he would receive a refund. He needed to give the company his bank account number so they could deposit

the money. Instead the victim discovered later that \$4,000 was removed. On June 18, 2018, the victim received three calls from Alex. This scam lasted until November 2018. During this timeframe, the victim was required to read information from 14 gift cards to the scammers to pay for the service. He bought eight Target cards totaling \$8,000, two Best Buy cards totaling \$4,000, and four Apple cards totaling \$8,000. At some point he was told his computer problems were very complex and needed significantly more time to repair.

These calls were a system of over/under payment beginning when he gave permission to the company to take the agreed-upon amount of money out of his account. This confusing scheme of over/under payment for a service resulted in an average of \$4,000 removed from his bank each time.

Finally, he let a sibling know he had been scammed. He was embarrassed and could not believe that he let this happen. Initially, he worried about getting out of the scam and did so by cancelling all of his bank accounts. The financial stress has been the hardest part of the incident for him, along with the embarrassment.

He contacted the local police, who collected the data. They left with a promise the fraud department would be in contact. However, that has not come to fruition in the last three months. The victim did not contact the FBI, and he did not have any knowledge about APS, IC3, or the FTC.

#### *Relative Interview*

The relative interviewed was the spouse of the victim's adult child who lived close by. The interview lasted about one hour.

According to the relative, the victim was online several times a week to email and to get medical information via a search engine. He told the family he had received a phishing email that offered to help him with his computer. However, this family member believes he may have been blackmailed. They believe that he is too frugal a person to willingly part with so much money. He admitted to being embarrassed from the scam, but he also seemed to be fearful. His family thinks there is the potential he was being blackmailed. This is because he may have been looking at a porn site or he may have been in contact with someone who threatened him. The family gave the victim some money to help him.

#### *Sister Interview*

The victim's sister lives about three hours away. The interviewer and the sister met during the timeframe of the interview with the victim. However, the sister's interview was conducted over the telephone in order to prevent any victim discomfort. The interview lasted about one hour.

The victim's sister was the first person he confided in. This was after she questioned why he asked her for some money numerous times. During this timeframe, she sent him several thousand dollars. He did not want to let his kids know. According to the sister, he was frequently online daily on his laptop and iPhone. He used both for entertainment. She was unsure how the scammer contacted her brother and how long the relationship existed. She did know that the scammer eventually asked for his account number so he could be reimbursed and that her brother gave it to the scammer. In the beginning it was credit card payments and repayments, but then it was "way beyond credit cards, they got into his bank accounts."

She believes his ego would compel him open his wallet, and she is concerned he met a female online and was or is still involved in a relationship. She believes he may have been on a website offering female companionship and that is how he was lured into the scam. She acknowledged he is “not worldly.” She also said he has no social or business awareness and that he is a bit of a loner. He is a very curious person and did not understand what he was doing online. She worries that he may still be involved because he often does not have sufficient funds, even though he earns enough to support himself through his retirement and social security.

He has a history of giving money to people who were not necessarily honest with him. For example, his second wife, who passed away a few years ago, took advantage of him financially to buy drugs. His sister also believes that the victim feels guilty regarding his daughter’s past and that his stepdaughter manipulates him for funds. He admitted to feeling stupid and embarrassed. He needs to see some level of justice in order to feel whole again.

## **O1**

O1 is victim of a business investment scam and intellectual property theft.

This victim is 68 years old and her husband is also in his late 60s. She is self-employed, and her husband is intending to retire within one year of this interview (2019). She uses the computer for her daily work. During this 6.5-hour interview she revealed that she is afraid of what her husband will do when he learns the full extent of the scams. To begin the interview, she wanted to communicate her savvy understanding of scamming and how she foiled an attempt when someone claimed she owed money for

clothes she did not buy. She was clever enough to close the account because the scammer knew where she had a bank account.

She is the victim of two, possibly three, scams. The most concerning scam was what she termed a theft of her intellectual property, which appears to have one-tenth the financial implications of the other scam. She claimed her LinkedIn account, where a lot of information regarding her business interests is located, was hacked. However, her focus of concern was on the first scam. She directed her anger toward the credit card company for refusing to remove a charge. The charge was for an advertisement of her decade-old book. She explicitly did not wish to advertise with the company that charged her credit card. She expressed anger and helplessness toward the credit card company for allowing an unauthorized charge.

The second scam involves a fake e-commerce business opportunity. She was in the middle of a webinar<sup>56</sup> class, taught by a financial company, to learn how to start a brokerage business and trade stocks and bonds. During this time, an individual called her home phone. As soon as she answered the phone, the individual took control of her computer. The scammer produced a contract, demanded she touch her screen, and added her digital signature when she complied. He knew she had assets in the form of 27 credit cards. He also knew she had a desire to earn money and that she was confused and frightened by the real-time access and technological takeover of her computer. She told the interviewer that she was unaware of the total amount charged to her credit cards and believed the credit card company would return her money. She indicated that she felt helplessness and angry.

---

<sup>56</sup> A webinar or web-based seminar's key feature is the ability to interactively conduct conversations in real time.

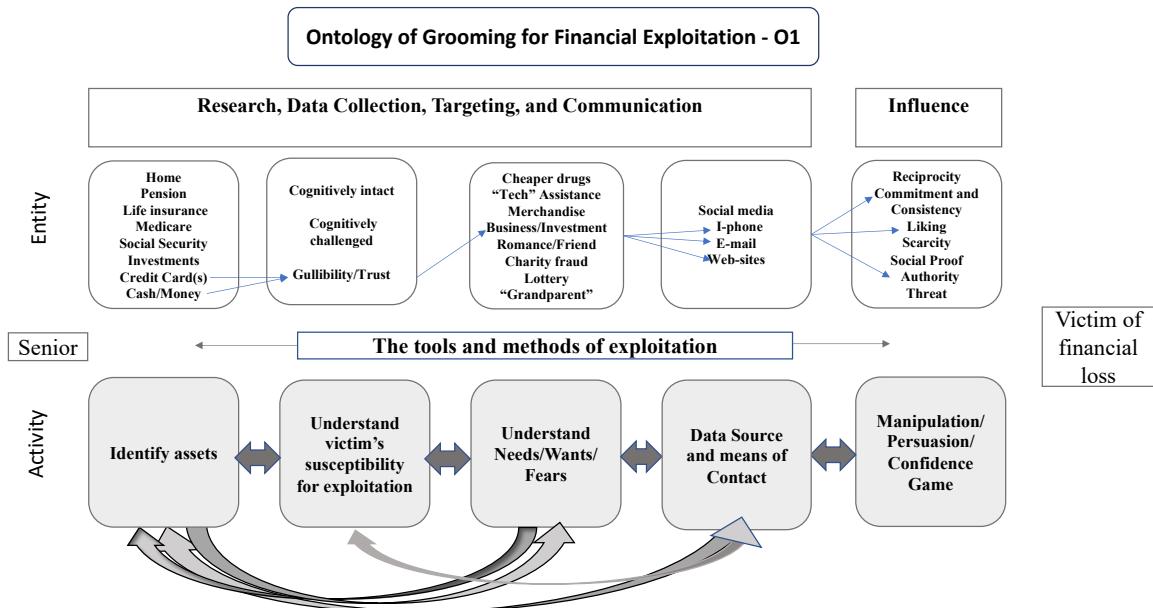


Figure 19. Application of the theoretical framework to case O1

#### *Victim Interview*

**First Scam:** In 2017, victim received a daily call from someone with a Middle Eastern accent demanding she go to the CVS parking lot in Burtonsville with money from her Sun Trust account. During a call, the phone was passed to a woman who stated that the victim bought software and clothes and that she needed to pay. The victim asked what size the clothes were but the scammer did not have the right answer. The victim then called her a scammer. The victim closed her bank account.

**Second Scam:** the victim believes her intellectual property was stolen by a company that provides services to self-publishing authors. She was charged \$3,180 for an advertisement in a brochure that she did not want or authorize. The caller from the magazine claimed they wanted to publish her book, which was already in print. The caller told her he had blown up her picture. He also made several complimentary, but unwanted, remarks about her looks. She says she did not agree verbally or in writing for the company to advertise her book. She is disputing the charge with the credit card

company. She believes the credit card company is not helping. This is because they believe she received something of value, regardless of the actual value. Her contention is that the company, which is not endorsed by the Better Business Bureau, had greater influence over what happened with her book than she did.

Third Scam: On September 18, 2018, the victim was participating in a webinar conducted by a financial company on brokerage business. She had researched the topic online, watched brokerage news, and thought this specific company wrote good financial articles. She was impressed with this company, signed a contract with them, and was excited by the prospect of starting a brokerage business. Her phone rang during the webinar. She thought the call was associated with the webinar. A man with a “salesy” type voice said, “Hi, Susan. This is Mike Winters.” He stated he was from Market Success, a group that worked with the financial company. He asked questions about her home. He also asked other intrusive questions such as how much she earned and about her liquid assets. She stated she did not have any liquid assets. Then he stated she had 27 credit cards and they were liquid assets.

He told her she would be perfect for an e-commerce store. He asked if she had any interest in opening a store and, if so, what type of store would interest her. She said health and fitness. He replied that was a brilliant idea, and he claimed she would be wonderful as the head of one of the stores. As soon as he said that, a contract appeared as a pop-up on her screen, wiping out the webinar. He said she should sign it in a demanding voice. She refused. He told her that he would sign it for her and convinced her to touch her computer screen (a nontouch screen), and when she did, her signature appeared. She reiterated that she was not interested and she wanted him off the phone. He

stated he wanted to offer her two scholarships. Each was of \$4,500, for a total of \$9,000. She asked how he obtained her email address and phone number. He said that he “bought it under the table from someone who worked at the company.” He stated that Megan Rogers was her coach and would be in touch. She did not give him her credit card number, but he was able to charge her card anyway. Megan did call, but only said one word and hung up.

The victim spoke with Chanel (not further identified) to complain about paying salaries for Mike and Megan in addition to all the office supplies. Chanel affirmed the victim’s feelings and told her “you are right, I’ve got your back.” Because of this conversation, the victim believes she will be able to get her money back from the company.

In November 2018, a detective noted three charges totaling \$100,000 on her credit cards. The victim stated she needs the 27 credit cards to feel financially safe. The victim does not know how much is owed on most of the cards. She stated she feels angry and helpless. She is very nervous about telling her husband.

#### *Husband Interview*

Her husband knew very little about any of the scams and insisted on sitting in on the interview. When he left the room to answer phone calls, she would then tell the interviewer more details. He wanted her to freeze all the credit cards and to know how much was owed on all the cards. Her husband is worried that this has thrown his wife’s life into turmoil, and he is afraid of the financial impact. He is frustrated by not knowing what is going on, and this has caused him to be stressed.

### *Information regarding the corporation*

This financial corporation is not accredited by the Better Business Bureau and has a long list of online complaints. Learning the cost of a particular feature requires the viewer to enter their credit card information. Several people stated that they did not press enter, but their credit cards were charged anyway. Most features are nonrefundable. In addition, several complainants indicated their information was made available to other “investment” companies. The company appears to act as a listserv and sells the roster of interested investors to other online companies. Reportedly, the company provides a consolidation of readily available (free) information from other companies.

### ***F1***

F1 was victim of a sweetheart scam.

The interview with the victim lasted about 2.5 hours. The victim is a soft-spoken widow who admitted to having had suicidal thoughts. This is what brought the police into the situation. Her neighbors used the same dating website and were now happily married. She did not want the neighbors to know she had been scammed. They knew how lonely she was, and they had encouraged her to use the website. She did not want them to feel guilty.

The fake romance partner had all the same interests as her. She was unaware of how the scammer knew so much about her and the things that she liked and wanted to do. She did admit that during the online courtship she shared personal details with the scammer. However, he seemed to express the same interests before she shared her interests. She suspected that she was a victim of a scam. She spoke with the scammer on the phone and she confronted him. She realized he was not an American. He made

comments about seeing the inside of her home, which was frightening. She suspected he hacked into the webcam on her computer. She sold her large home, moved into a modest home, and no longer has a computer.

She felt very sad due to the loss of her money and also due to the loss of a potential life partner. When she discussed the scam with her friends from her country of birth, they wanted to know how she could be so stupid. She feels alone, embarrassed, scared for her future, and, in some sense, isolated and helpless.

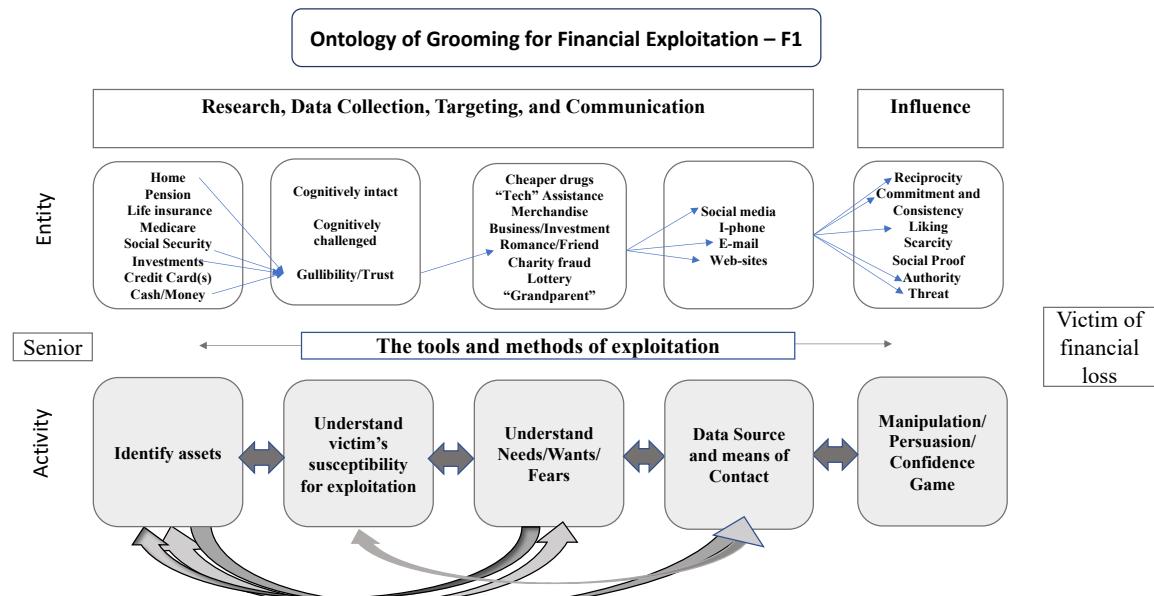


Figure 20. Application of the theoretical framework to case F1

In October 2012, a 69-year-old widowed physician, not native to the United States, met an individual online through a seniors' dating service. She had used the dating service previously. However, she disliked the first man she met online and discontinued contact after he asked for money. A close friend and neighbor met her new husband through the same seniors' dating site. The friend recommended the victim try again, knowing she was lonely after having been happily married.

The victim tried the seniors' dating website again and met someone. The relationship lasted about one year with the two corresponding exclusively online several times per week. He said he was from the Midwest. She substantiated his identity and some of his past addresses. He claimed to be a retired commercial airline pilot. She said he created a "psychological projection" that resonated with her and reminded her of her husband. They both liked travel, music, and a whole range of topics. He sent her his pictures and his passport information. About three months into the relationship, the pretend lover requested money to address some personal misfortunes. His mother died, then his beloved dog died. He would promise to come visit, and she would make local hotel reservations for him, only to be disappointed when he failed to arrive. He would send flowers to make up for not coming. Once, he was reportedly boarding an airplane and claimed he had an accident. He then requested money for medical bills. She said, "Whenever someone is in need you just want to help. You don't have an idea that there is something evil, you always help, don't have anything in mind, you just want to help."

He continued to ask for money. She gave him her investments of approximately \$1.5 million. She became suspicious when he started to use the same language (exact sentence) as the first person she met online. In October 2013, she told the individual that she had no more money. Then someone called her and told her that he "saw the inside of your nice house through Skype." The caller did not have an American accent. She realized she had given away most of the savings. Since she did not work in the United States, she lived on her husband's investments and spousal social security based on his 10 years of nonfederal work. She was very happily married, but she feels her husband was very protective and that resulted in her being very naïve.

When she fully woke up, she felt as though the roof was falling-in. She lost sleep, lost weight, stopped taking care of herself, and contemplated suicide. The police were called for a welfare check and transported the victim to the hospital. She told the police she only had a few dollars left in her bank account and felt that suicide was the only resolution. She informed the dating website of the scam. She sold her home and moved into a modest residence to live within her means. She never suspected anyone could do this and only shared her situation with her childhood friend. The friend asked, “how could you be so stupid?” She has not shared any of this with her current friends. She said this researcher is the only person with whom she has shared this level of detail. She asked, “What did I do wrong to get this?”

According to conversations with the police, some of the money transfers went to another victim. They were an unwitting money mule who sent the funds to Nigeria. Another three bank accounts were located in Taiwan and Hong Kong. All of the IP addresses were located in Nigeria. The scam also involved elderly victims in two other states.

At the date of the interview, the case remained open and the police were working with the FBI.

### **P1**

P1 is a widow in her mid-to-late sixties.

This victim is surrounded by loving family. Her adult daughter, son-in-law, and two granddaughters live with her. Her husband died in 2005, and they had had a wonderful, loving, caring marriage. Afterwards, she dated a man with whom she had a

wonderful loving relationship. However, he became ill and died in 2015. She is self-employed, does volunteer work, and is very involved in the community.

She met her scammer through an online, cross-platform, multiplayer game application where she was challenging others to the game. They struck up a conversation, and he seemed to have all the same interests she had, including grandchildren. His deployment on an oil rig meant he had hours of lonely time to spend chatting online with her. He needed help with little things.

Once he realized that she recognized the situation as a scam, the second scam erupted. Another criminal intimidated her, threatening to tell her family. She is hurt by the loss of someone she thought would be a future partner and the loss of her money. However, she is most worried about repaying her mother, since her mother resides in an assisted living facility. Beyond financial loss, she is angry at the lack of legal recourse, and she feels helpless.

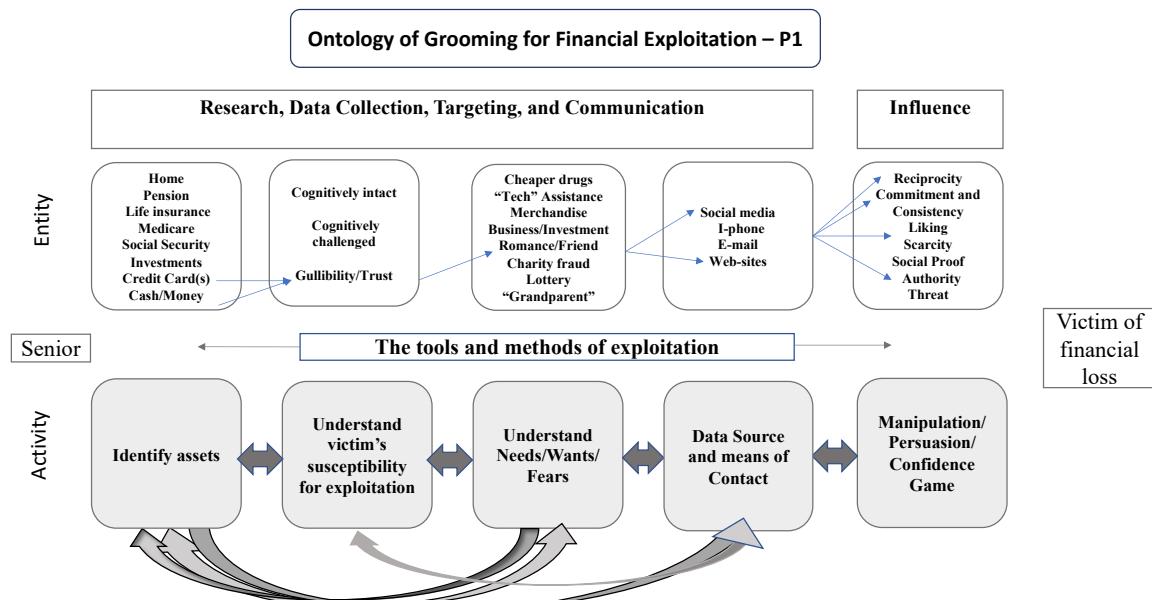


Figure 21. Application of the theoretical framework to case P1

The interview was conducted at a coffee shop of the victim's choosing and lasted about six hours.

She owns a computer, is online daily, texts, instant messages, and emails. She also uses a smartphone. She uses the internet occasionally to get health advice or medical services. She is on Facebook and often uses the internet to play games. She met an individual claiming to be a male through the game Words with Friends. He started a game with her, and they began talking through text messages, instant messages, and emails on August 9, 2017. He claimed to work on an oil rig in the North Sea.

Like her, he had grandchildren. He claimed to have custody of his grandson, Alvin, who reportedly was in school in London. He wanted to send him a card at Thanksgiving, but was unable to find his address.

He played on the fact she was looking for a relationship. She was very lonely despite having a house full of family. She met him through an innocuous online game, but she asked him a lot of questions before feeling comfortable enough to continue the online relationship. He did not have a Facebook page after his wife's fatal car accident. It would bother him. As the relationship went on, he asked her to find a place for the two of them. He had fallen in love with her and wanted to get married. He sent her loving letters and hinted at being married on her birthday. He sent her pictures of himself on an oil rig and with his grandson. He claimed to live in Redwood City, California. She searched his picture on Tineye. She found the picture that he sent was the picture of an individual that appears on a Christian dating website.

He told her he had investments in diamonds in Taiwan. The warehouse was due to be renovated, and so the diamonds needed to be moved immediately. The diamonds were

to be sent to her for safekeeping until he was off the rig. His time on the oil rig was extended. Since he was unable to get off the rig or get to a bank, he asked for money. She sent \$2,500 on September 5, 2017, and \$6,000 on September 8, 2017—eventually a total of \$82,000. In January, his time on the rig was extended again, so he was unable to come to her just yet.

In November, she realized she was being scammed after her daughter gave her articles about oil rig love scams. When he asked for more money, she faked sickness, claiming she was in the hospital. He claimed he wanted to pay with two of the credit cards. She called the card company and told them. He insisted on getting the passwords to be able to pay. He got the information about the accounts – they were already closed.

An alleged informant told her that he knew who the scammer was and could help her for a price. The scammer then sent an email to the victim stating he would tell her sister-in-law about how much she was scammed. Her sister-in-law, daughter, and son-in-law know she was scammed. However, none of them know how much. The victim went to the police, who were able to retrieve \$18,000 because this money had been sent to an account of another victim, who was an unwitting money mule.

While she admitted to being embarrassed, her biggest concern is the money she borrowed from her mother. She borrowed \$50,000, which was money earmarked to help pay for mother in assisted living.

She said, “How was I so stupid? We need to get people involved who can work through the maze to figure out who these people are. Need laws to protect people.”

## **E1**

For E1, the interview is with a family member of a victim of a grandparent scam.

The interview was held in a room of the interviewee's choosing and lasted over one hour. The scammers spoofed the "kidnapped" grandson's telephone number so the victims who recognized the number assumed the person on the other end of the telephone was their grandson. In addition, the criminal knew the name of the grandson's dog and fiance. The family believes all of the data was obtained from his Facebook page. The victims, grandson, and other family members are angry. However, they could not do anything to obtain redress.

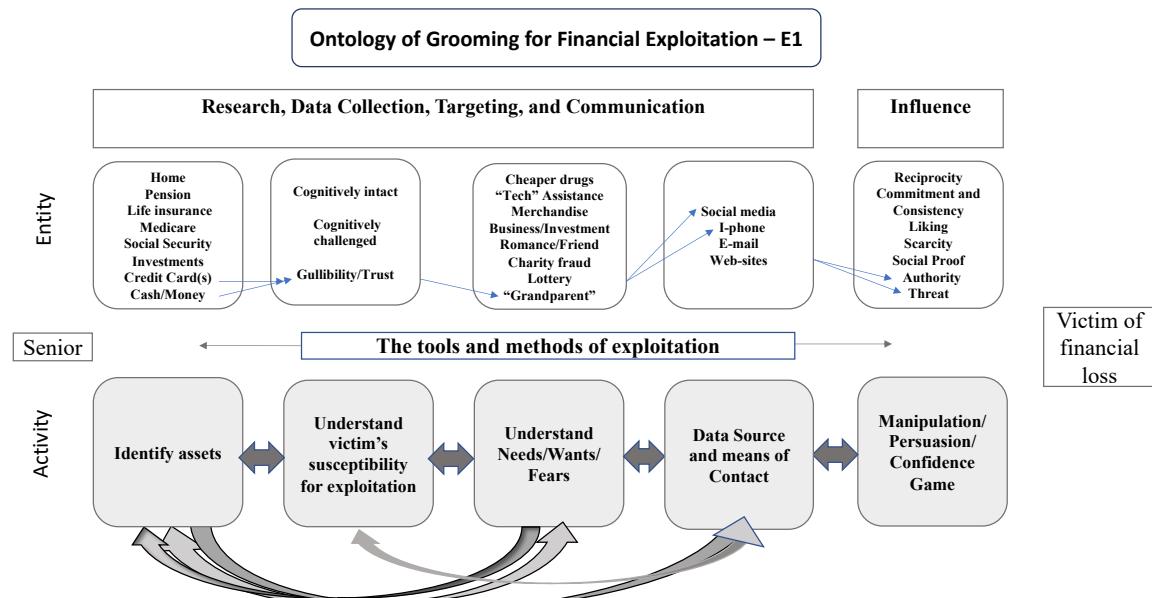


Figure 22. Application of the theoretical framework to case E1

Around 2016, a husband and wife, both 77 years of age, were victims of a grandparent scam. The husband had been an electrical engineer with a master's degree and the wife had a bachelor's degree in nursing. They received a call from someone whose voice resembled that of their grandson. He said, "Hi Grandpa." The scammer then said, "Things are tight and I could use some money," requesting \$7,000 be sent to a bank account. The individual masquerading as their grandson indicated he was in Mexico, had a problem, and desperately needed the money. There was a sense of urgency and

desperation. The criminal knew credit level detailed information about their grandson, including the names of his then finance (now wife) and dog.

Unbeknownst to the victims, the grandson's phone was unreachable during this crisis time for a return call. His phone was shut off, as he was in a prenuptial session in church. The urgency influenced the victims emotionally. They reacted out of fear for their grandchild, without consultation with other family members.

Subsequently, the grandson noted his computer had been hacked. After talking with the grandson, the family believes that a lot of the personal social details may have come from the grandson's Facebook account. The wife who sent the money was embarrassed at being duped. She stated that she was ashamed for being that 'stupid,' and she was mad at herself, as she had heard about the grandparent scams before. Although they called the police, there was no trail of the scammed money.

## A2

Victim A2 is a deceased widower, and the interviews are with two of his adult children.

The interviews were conducted over the telephone. Additionally, a letter the victim left with his family outlining the events leading up to his losing his home and declaring bankruptcy was used. After the death of his wife, the victim started to visit several dating websites. According to his family, he was lonely, wanted to have a relationship, and was very susceptible to flattery. In addition, he was computer savvy and ran a computer business from his home. Unfortunately, he was not business savvy. He believed the people with whom he was working were equally honest. The family can recount eight times the senior was scammed out of money. One happened prior to his

wife's death . The couple were issued a predatory mortgage, but because they had also taken out money to pay bills, they had no legal recourse. After his wife's death he experienced multiple scams. Of these scams, two were romance, one involved his banking information and a dating website, one was friendship based, one involved his computer business, one was related to an alleged kidnapping, and he was also convinced to buy gold in Ghana. Although the family was frantic to curb the scams, state laws protect the ability of seniors to make their own decisions. A visit with a gerontologist indicated he had no mental issues, such as dementia. After his death, it was noted he suffered from Alzheimer's disease. According to his daughter, the tests for dementia used by his physician were math based, which was his area of expertise. After the loss of his home and the companionship he garnered using the computer, he felt depressed, lonely, helpless, and embarrassed.

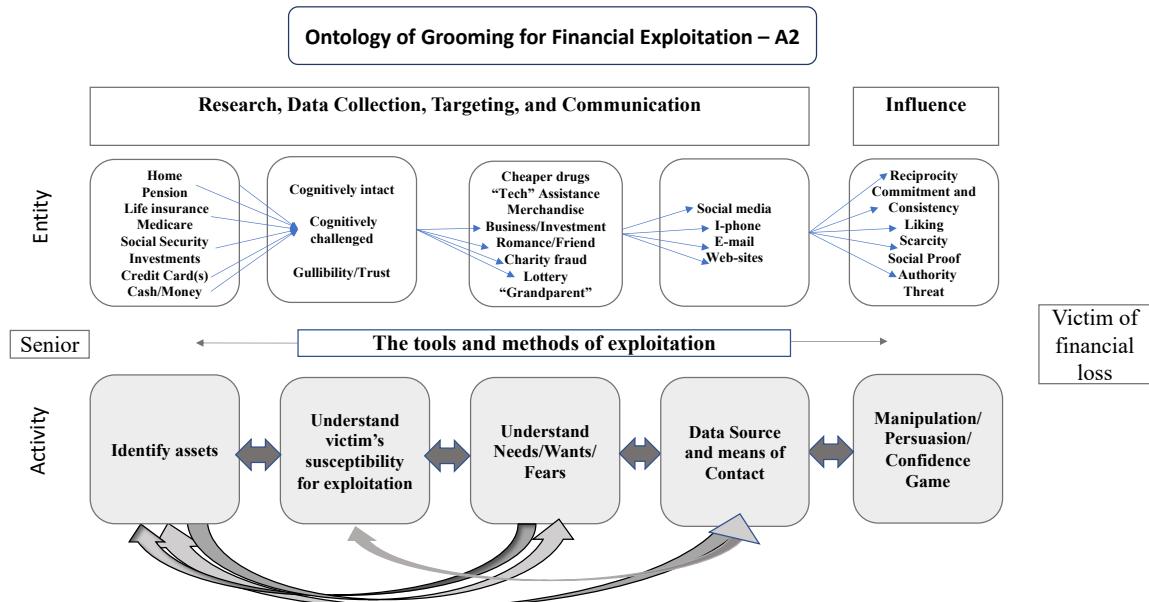


Figure 23. Application of the theoretical framework to case A2

### *Victim's Letter*

The victim was terribly lonely following the death of his wife. They had been married for over 50 years. After her death, he joined several dating web sites.

First scam: In 2008, he met “Tracy George” online, who claimed to be living about six miles from him. She told him she had gone for a visit to England. While in England, she said she had borrowed some money and needed to repay a \$500 loan. He sent her the money. Next, Tracy George next claimed the son of the woman from whom she borrowed the money was killed in a hit in run. The woman committed suicide, but the Nigerian who was driving the car was deported. He stood trial in Nigeria. Tracy George went to see the trial, but she broke her ankle prior to leaving. The other occupant in the car was a lawyer who was killed in the accident. Tracy George left for Dubai, United Arab Emirates, where she borrowed more money. She left Dubai for England. She took a flight to Atlanta, but got on the wrong plane and ended up in Deland, Florida. Because she did not have the right paperwork, she needed more money, which the victim sent her. The next time she contacted the victim, she said, that she was back in England but trying to stay out of legal trouble. While working, she followed a doctor’s orders and a patient died. At some point, Tracy George, who claimed she was born in August 1978, stopped contacting the victim.

Second scam: The victim met Sarah Smith online. He admitted that she cost him more money than any of the other scams. Sarah, reportedly born in January 1985, asked for help with her inheritance. She could not inherit any of the money from her late father unless she was married. She told him she was a medical student and needed help. However, the marriage certificate stated she was a cloth maker. The victim and Sarah

Smith were married over the phone on May 26, 2010. He admitted to sending her \$2,600 to pay for the wedding. He sent the marriage certificate to the Department of Defense's finance and accounting service (DFAS). Their marriage was recorded, and she would receive a monthly stipend if he died. This meant his monthly retirement was decreased to fund his death benefits. In total, he believed he sent her about \$11,000. He was lonely and in love with her.

Third scam: After that he met a family from Ghana online. The family was comprised of Gheieve Foli, her daughter Harriet Harrison, and her son Frank Addy. The son's girlfriend was working on culinary arts degree. The victim was sending money to start a coffee shop to earn money so Gheieve could come to the United States and take care of the victim. However, the money never got through. In the last conversation, Gheieve expressed disappointment about not getting the money, and she stopped calling.

In his letter to his family, he apologized to the family for "messing things up" and "making an ass" of himself.

#### *First Adult Child Interview*

The victim was online multiple times per day for genealogy, joke of the day, dating websites, emails, and for looking up things of interest. He responded to several phishing emails. At one point, several hundred viruses were removed from his computer.

Fourth scam: The victim ran a small part-time business. Someone from out of state made a large request for some products. The victim subsequently borrowed a significant amount of money to purchase the raw materials. The customer sent payment and the victim immediately shipped the product. He later found that the check did not

clear the bank due to insufficient funds. The customer was a scammer and the victim owed money to the bank.

Fifth scam: The victim was financially underwater for a long time because he believed others were honest in their business dealings. On more than one occasion, the victim would receive a check from a customer and the check would not clear the bank. He and his wife, who suffered from dementia, were scammed. They received a cold call regarding a mortgage refinance offer. The terms of the offer were not advantageous, with an increase in the rate, an early payback penalty, and a \$10,000 fee charged by the refinance company. His family was able to get the house refinanced. However, his wife died in May 2009 and then he stopped paying the mortgage.

Sixth scam: In late 2009 to 2010, the victim responded to the request from one dating web site, which required his banking information for membership. He took out all existing funds. The theft was just prior to his retirement and social security deposits. As such, one of his daughters was able to get to close his bank account before anyone could remove more funds. He agreed that it was “silly” to give out his account number.

Between 2011 and 2012, the victim’s son alerted the family to the victim’s suspicious behavior, particularly when he was on the computer and his son was in the room. His daughter confronted him, and he admitted he was married. The victim said that the family could do nothing about 27-year-old wife. The victim married the woman named Sarah Smith by proxy over the phone. She inherited £25 million but needed to be married to claim the funds and wanted someone older and more mature to help her. Sarah identified the victim when he was looking at dating websites for lonely singles. The victim immediately added Sarah to his military financial records as his spouse, and the

VA decreased the requisite funds every month. He hid the relationship from the family because it was “between us, it’s our relationship,” and the victim did not want to explain why he had married less than a year after his wife’s death. There was lots of romantic and sexual discussion. He truly loved her or the idea of her. She promised to come to the United States. He waited at the airport several times for her. At one point, he had family call English hospitals, because she said she was in a car accident on her way to the hospital. He was frantic and crying. He thought he lost her due to injuries from the accident. He was relieved when she called him requesting money for the doctor. The victim did not want to believe his children, who told him there were no medical bills in England. However, receipts showed that over time, he sent at least \$25,000 via Western Union.

He wanted the relationship to be true because he wanted someone to love him. The scammers would call at 3a.m. when he would be disoriented and susceptible. Once he was convinced that Sarah was a scammer, he grieved terribly. His grief was comparable to the grief he experienced when his wife died.

He was very lonely. He posted his passport, driver’s license, and military ID card (with social security number) on Facebook in the hope of meeting someone on the social media website. Once his family realized he had posted all this personally identifiable information, they demanded he take it down. He could not remember his password, and Facebook refused to remove the information. Two of his granddaughters separately reported it as pornography, and Facebook removed it immediately without further discussion.

Tracy George was another person with whom the victim corresponded. She was more vulgar and used sex as a manipulation tool. She was too nasty, and the victim realized she was not someone he would be interested in. The family had the victim's phone number and email address changed.

Gheieve's daughter corresponded with the victim. She said that she needed money for medical school. The victim felt he was supporting a starving family. There was no promise of sex, just companionship and the good feeling one gets from helping others. She told him that it was wonderful that he was "helping to feed the children." Then she said that she could come and take care of him and make him happy. She gave him companionship over the phone. He approached several members of his church requesting money to send to Ghana to help them. He also borrowed money from his life insurance plan. Gheieve's daughter would buy things online and have him go pick them up and mail them to her. They would ask for technology that was not exported, and he would buy and send it.

Seventh scam: The victim's gold investment in Ghana reflected a get rich scam. Since the victim stopped paying his bills, one of his adult children started to help with the checkbook. She found \$15,000 in recent receipts for money orders hidden in his house. He was denying himself things so he could invest in the gold, which he planned to leave to his children.

He did not believe his children's warnings. He did not think they were as worldly as him. The scammers made the "unicorn" more real. The scammers would call in the middle of the night, when he was disoriented and not thinking as clearly. The scammers

would confuse and manipulate the victim. He was told to send money, or bad things would happen.

Since he lived through the Depression era in the Midwest, he was taught to help his neighbors—“you do what you can for others.” In past scams, his motives were clear - with Sarah the relationship was sex and companionship and with Gheieve he was helping and making the world better. The gold investment was to pay off the debt and be able to leave his kids money when he died. The scammers’ calls and emails would start just prior to deposit of his retirement and social security checks each month. Calls would increase until he sent money. They would call in the middle of the night to disorient him and express a sense of urgency.

Family members stopped sending cash and only sent gift cards. Unfortunately, the victim would in turn read the numbers on the back to his friends located overseas. Finally, family members limited the gift cards to Walmart and bookstores to prevent this behavior. Finally, they had to unplug his modem. They took care to make it appear that it was still plugged in. He would constantly try to fix his computer, not realizing the modem was turned off.

#### *Second Adult Child Interview*

The second adult child said that the victim went online every day. He communicated over the Internet, chat rooms, instant messaging, cell phone, and he could be contacted by beeper. He was on Facebook, genealogy websites, played chess online, and was part of the community website called lonelypeople.com. He read news online on Yahoo and aol.com as well as listening to the TV. He banked online.

His cash register business was among the first scams. Someone ordered several systems that required he buy some materials in advance. He borrowed around \$20,000 to buy the materials and built the systems. He shipped the systems the day the check arrived from the scammers. Then he learned that the check was no good. The bank held him responsible for the loan, which put him in a bad financial situation.

After his wife died, he met several scammers on dating websites and through phishing emails. He never met any of these individuals personally. Several connections were of a romantic nature. He gave charitable money to help a family in Ghana build a coffee shop.

He met Sarah online, perhaps via [lonelypeople.com](http://lonelypeople.com) or another dating website. She sent pictures and claimed to live in England. She and the victim married over the phone, and he was given a marriage certificate. At one point she claimed she was in an accident, was hospitalized, and needed money to pay her medical bills. He was frantic and scared he would lose her like he lost his wife. He begged his daughter to find her in a United Kingdom hospital so he could ensure she was OK. She found out about the scam from a brother. The brother claimed their father was acting very secretively, particularly whenever he was there, and his Dad was on the Internet. When the victim's daughter found out he was married, she told him the certificate was a fake. He did not believe it. He wanted to believe the marriage was real. He did not want to accept the truth. From that day forward, he was always angry with his daughter. He gave his daughter Sarah's phone number. He demanded that she call Sarah and tell her the marriage was a scam, but the daughter could never reach Sarah. A year later, when her father was presented with overwhelming evidence that the marriage was not real, he refused to speak with his

daughter about it. He was a very lonely widower and the scam ran for about 1.5 to 2 years.

Eighth scam: This scam was from Nigeria. The individual claimed her father's former neighbor's daughter was kidnapped and needed money to be released. This Nigerian had tried to save her, but they still needed the money. He said he was afraid that if anyone found out about his attempt to help her escape, she would be killed. The criminal stated that authorities could know because the Nigerian Government may take draconian measures, which could cause the kidnappers to "dispose" of the girl. Several times money was sent, but the victim was told that the money did not arrive, that it was stolen, or that it was not enough ransom money. The victim sent money via Western Union at the local Walmart. His daughter reported the scam to the FBI, but she was told that because it was an international case that nothing could be done.

He was scammed by several other people who he claimed were his friends. He invested in what he claimed was gold in Ghana. The investment was \$2,000 each time. He sent money, a 55-inch TV, his own computer (with personal data on it), gift cards, etc. He would take cash out of the bank, and when his daughter paid bills from his account, the check would not clear due to insufficient funds. He blamed her for losing his house because he believed the daughter was stealing from him.

The victim was an easy-going guy and made friends easily, but he was also very gullible. He was willing to help anybody. Whenever anyone asked for help, his response was "what do you need?" Scammers contacted him several times a day, leading his daughter to change his phone number. However, he then gave his phone number to the scammers so they could reach him. They maintained consistent contact with the victim and

continued until he had no more money to give. He had to declare bankruptcy and he lost his home.

The hardest part for him was the embarrassment and loneliness. He was heartbroken over the loss of Sarah. He never admitted to this daughter that he was scammed. He was too embarrassed and did not want to talk about it. The victim's daughter believes the FBI needs to crack down on scammers.

## **H1**

The victim is a widow in her late 70s. The interview was with her daughter. The interview was conducted at a location of the interviewee's choosing and lasted about 1.5 hours. The victim is an intelligent, well-educated retiree, who uses the computer several times a week to access the internet. She has been scammed twice. Each time she was convinced to send money. Afterwards, she realized how she was manipulated by the criminal's implied urgency and her fear of losing out on a deal. The victim was truly embarrassed, and these scams have enabled her son and daughter to convince her to move into assisted living. The victim also agreed to put a governor on her accounts. Any withdrawal from her bank over \$500 will alert them. The relationship between the victim and her children is close, strong, and loving.

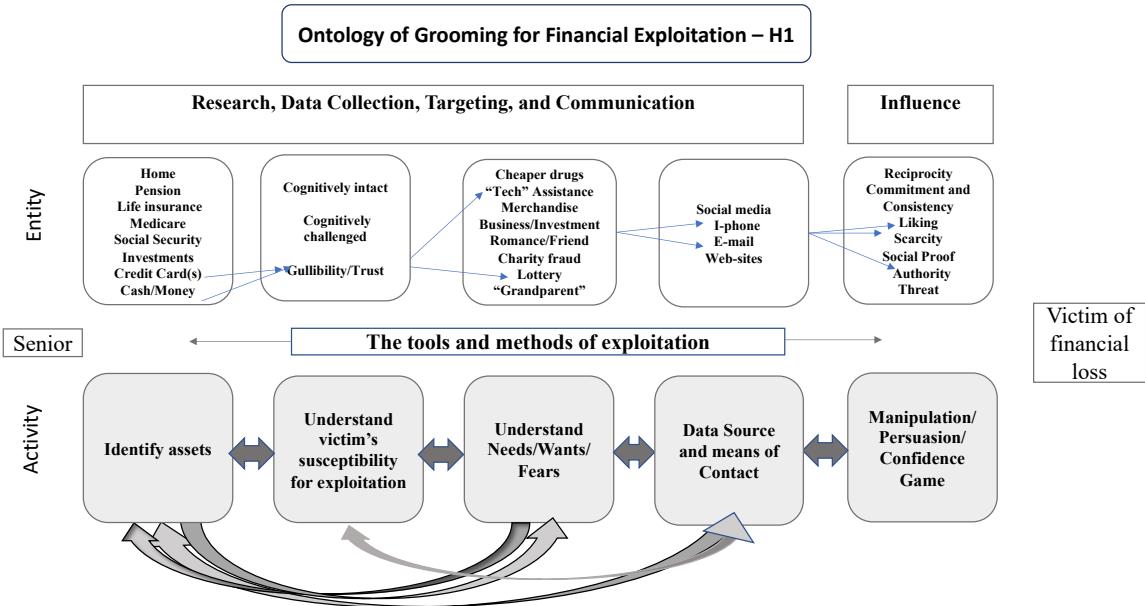


Figure 24. Application of the theoretical framework to case H1

The victim has several college degrees in several disciplines. She lives alone and is retired. She owns a laptop computer and is online two to three times a week for several hours. She is on Facebook and clicks on advertisements posted to Facebook as well as those sent via her internet service provider. She makes purchases online and checks on people she may know through paid services. She buys many items from Publisher's Clearing House. She also does some of her banking online.

First scam: She was a victim of a lottery winning scheme perpetrated over the phone. She paid \$1,000 through Western Union to an international entity. She was embarrassed by her self-described gullibility.

Second scam: In early 2019 she received an email that indicated she was entitled to a Microsoft rebate and called the number listed on the email. The caller claimed they had issued her too large a rebate, and that she would have to pay a lot of money if she went to the bank. It was supposedly \$200, but when she checked her account she was confused and said she thought she owed them \$4,000. Naturally, the scammers agreed

with her. As she wanted to avoid a bank fee, she followed the scammers' directions. She went to the drug store, bought prepaid cards, scratched off the numbers, and read them to the scammers while they were on the phone with her.

During both scams, the criminals kept her on the phone until she either sent the money or read off the prepaid card numbers. They used time pressure to make sure she did as they directed. Again, she is very embarrassed by falling victim to the scam.

Her family is taking steps to intervene. First, her two grown children are on her bank accounts, and she cannot spend more than \$500 without their knowing. Second, they are moving her into an assisted living environment, where she may be at less risk of criminal activity.

#### ***GI***

The victim is in her late 60s. The interview was with her stepson-in-law.

The interview with the victim's stepson-in-law was conducted in his office and lasted about an hour. The stepmother-in-law is a victim of a romance scam and an investment scam. While the family is upset at the scam, they are equally upset at her lack of openness about the scam. She is not close to either her son or her stepdaughter. She has recently shown indications that she realizes the scam's financial impact. The victim has subsequently asked for full ownership of a piece of property, claiming it would be what her late husband would want.. The property is currently co-owned by the daughter and by the victim. They are hesitant to enable her to make independent financial decisions.

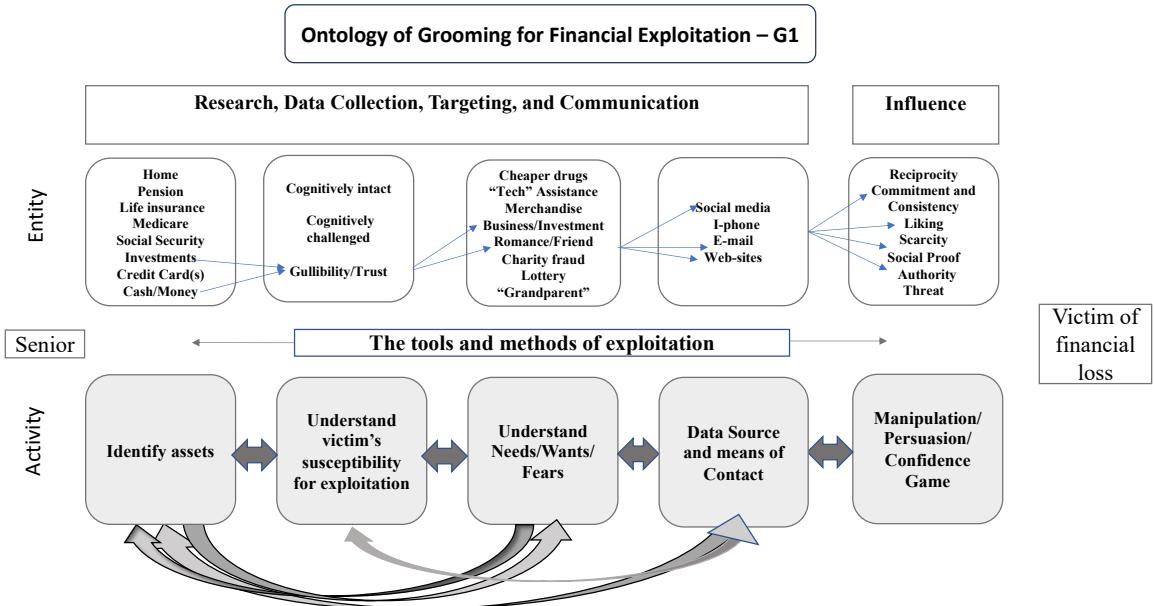


Figure 25. Application of the theoretical framework to case G1

The victim was significantly younger than her late husband. They been happily married, but she had been the care giver for many years. The husband, who suffered from cancer and died in February 2018, lived frugally and had invested wisely in stocks, bonds, and mutual funds to in order to leave a sizable “nest egg” for his wife. She married her husband years after his daughter was grown and on her own. She has a son from a previous marriage. He is not in a position to assist finaically. His relationship with the victim, while not adversarial, is not close.

The victim was alone and lonely. She spent at least four hours per day online. Following the death of her husband, she joined a dating website specifically designed for seniors aged 55 years and older. In September 2018, she met someone online who was reportedly a German engineer. The scammer claimed to know about the United States as he was a Stanford University educated engineer.

First scam: In October, the victim told the family she was dating again. Her stepdaughter was shocked, and she perceived the victim dating to be inappropriate due to

the short period of time since her father's death. However, the victim's stepdaughter began to recognize that she had underestimated the caregiver burden experienced by the victim. The victim admitted that she had never met her new love interest in person. That was due to his work in the United Kingdom. By Christmas, the victim still assured her family she was in love, and everyone would meet together in the spring.

Since the stepdaughter was concerned, she tried to convince the victim that this could be a scam. However, the victim was adamant so the family "soft-balled" their nervousness. Then the victim's neighbor called the stepdaughter to let her know there were financial problems. Through the Financial Industry Regulatory Authority's (FINRA) trusted-person notification program, the neighbor had been called by the financial institution. There were significant withdrawals from all of the victim's accounts. The neighbor did not wish the victim to know she had contacted the stepdaughter for fear of angering the victim, and she was very careful with the amount of information she was willing to give the stepdaughter when she called. The stepdaughter did not want to lose the source of information or anger her stepmother. Both the relationship and conversations between the victim and the stepdaughter were very tenuous, and so the family had little ability to prevent the loss of funds. It was obvious to all parties that the victim was in love, and this emotion swayed significant power over her decision-making.

As the five-month-old, online relationship developed, the scammer told the victim he needed money to start a business. She helped him financially. He then claimed to have inherited three million dollars from his mother's estate, but he needed money to pay the inheritance tax in advance. During the course of the five-month online romance, the

victim transferred \$100,000 to a bank account in Arizona six times. The funds were then transferred to a South African bank account.

Second scam: The victim made a \$100,000 investment in gold, which she believed she bought from someone in Africa.

While the victim was coy with her family by not sharing many details. However, either she, the investment company, or the neighbor contacted the police in February 2019. The police in turn notified the news to help inform others of the scam (Childress 2019; Zinn 2019).

## **C2**

Interview is with an APS social worker.

According to the APS social worker, the criminals understood the victim's financial situation along with his mental capacity, and they took advantage of him. Despite the criminals physically threatening the victim, law enforcement found no tangible evidence, nor could they claim "cyber" jurisdiction since the phone calls were ostensibly coming from overseas. The financial system, APS, and the state's attorney were able to help after the crime. They provided a safer living situation for him.

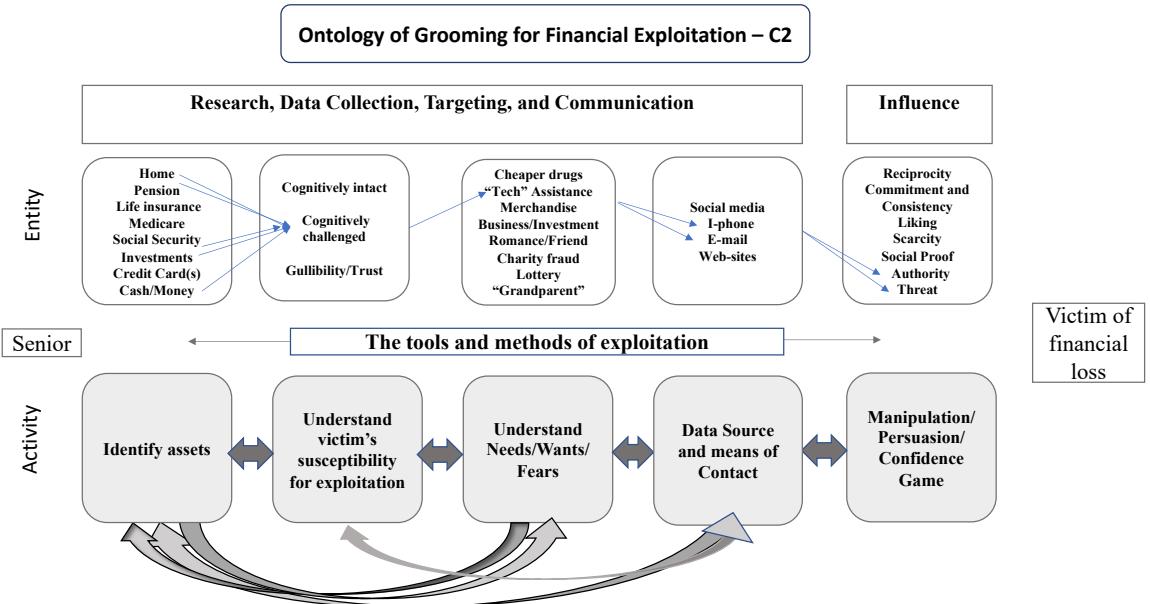


Figure 26. Application of the theoretical framework to case C2

The victim was a 78-year-old retired male who was never married and lived alone. He was a very organized individual, who knew he was not functioning as well as he had been earlier in his life. As a result, he kept notes and records of all the events. At some point, he was diagnosed with advanced dementia.

This victim was a well-educated electrical engineer who traveled extensively. Whether the travel was for pleasure or business is unknown. He was online every day and had a routine or pattern for his daily activities. He only left home to go for a daily walk in the neighborhood and to shop for food. He checked for emails and made online purchases using electronic means such as PayPal. He was an active buyer, including of electronics. However, he made purchases that he did not receive, specifically purchases from Africa.

Beginning around May 2016 his email froze due to a pop-up virus warning. He called the number associated with the warning and was promised help to solve the problem. He entered into an agreement to pay Micro-Team Solutions to fix the problem. He sent two e-checks for \$350 each to Micro-Team, and in June he sent \$400 to Charge

1. He then sent \$500 to an individual, Dennis R. S. In September 2016, he sent two e-checks for \$500 via PayPal. He would forget his password, so they would call him. Between October and December 2016, he received high pressure calls with threats of death, because he allegedly owed money to the government. He was a “boy scout type of guy” who never wanted to be in trouble. They gave him specific directions to buy iTunes cards at nine different locations to avoid suspicion. The cards totaled approximately \$20,000. He was required to buy cards in varying amounts from \$100 to \$250. In addition, he purchased gift cards totaling about \$19,000.00.

Around October 2016, charges on his credit cards were declined by Bank of America due to unusual activity of funds transferred out of the victim’s account. Reportedly Bank of America investigated, and some funds were returned to the victim. In addition, his PayPal line of credit was frozen on October 8, 2016, due to reaching the maximum limit. PayPal placed the account under investigation.

In late October 2016, his neighbors became concerned and called APS. The social worker noted the victim expressed fear as he relayed that two men had physically come to his home to pick up gift cards and had threatened him. Although the police were notified, there was no tangible evidence, and since the calls appeared to be coming from overseas nothing significant could be done. The states attorney’s office also declined to assist due to lack of international jurisdiction.

The social worker called the number that was given to the victim to call and hung up. Within ten minutes, the scammer called back and the victim answered with the speaker phone function activated. The social worker heard several telephones ringing in the background in a call center that seemed to have several highly contentious, high-

pressure conversations occurring. He gave the victim used iTunes cards and the victim read the numbers on the back of the cards to the scammer. The scammer, who had a foreign accent, continuously asked the victim to repeat the numbers, since they did not work, and demanded the victim get new cards.

The social worker had the victim's telephone number changed and provided the number only to select individuals. Although it took two months, the Montgomery County state's attorney assigned as his case manager was able to put a guardianship in place and freeze his assets. He was so organized and meticulous about his affairs. For example, he had a living will in place, had assigned power of attorney to his neighbor, and had designated this neighbor as his surrogate health decision maker. The case manager was able to get him an in-home aide. He was still able to function in his home for at least another year.

## **Section Two Interviews**

This section shows where the actions of a capable guardian helped to avert a crime.

### ***J1***

The victim is a widow in her late 60s. the interview was conducted with widow at a restaurant of her choosing. It lasted about 45 minutes. She has a loving family who are not in the area, but a great support and relationship exists with a neighbor. She is retired, lives alone, and is online several times a month. The scammer was so professional, polite, and supportive that she was ready to give the scammer money to help fix her computer issue. She did not send the money

because her neighbor came into the house and told her it was a scam. The neighbor became a capable guardian in this situation and prevented the scam from working.

The victim is online several a month via her laptop. In addition, she owns a smartphone and has Alexa in her home. She uses the internet for email and Ancestry.com. She does not conduct any banking online.

Twice she received calls from someone claiming to be the IRS, but the individual's arrogance and rudeness led her to realize it was not the IRS. She contacted the police who advised her to not answer those calls.

She was contacted by a professional-sounding cybersecurity representative who told her that her computer was being hacked. He offered to help her. He was polite, confident-sounding in his expertise, and sounded as though he wanted to help her. As she was about to give him permission to fix her computer and charge her, her neighbor walked in and convinced her to not allow the scam to proceed. She was then concerned that her computer might crash. She admits that had her neighbor not come in at the right moment, she would have given the scammer her personal information in the hopes of fixing her computer.

The hardest part for her was confronting the person. In her mind, he had the power because of his expertise. It was as though she was talking with her boss who was telling her to do certain things. She called her cable company, which conducted a scrub of her computer remotely to ensure the scammer had not done any damage to her computer.

She believes there needs to be better investment in national cybersecurity.

## **Section Three Interviews**

This section describes interviews with social workers from Montgomery County, Maryland, APS, members of the fraud department of Montgomery County, Maryland, victims' family members, and victims' friends. No interviews in this section included victims.

### **A1**

This interview is with an APS social worker regarding a computer tech scam.

A1 is a cognitively intact, divorced male with a master's degree who is over 70 years of age. The victim received a fake computer virus online and received a call immediately afterwards. The individual complied with the request for funds. At some point, APS was called to intervene on the individual's behalf.

### **A3**

The victim is a deceased widower. The interview is with his son and daughter-in-law.

The victim was online daily and active on Ancestry.com. He also did some shopping online as well as researching health issues and communicating with his physician.

In the 2014 to 2015 timeframe, the victim received a winning ticket from the Costa Rican Lottery in the mail and paid the nonresident tax fee required to receive his winnings. He was notified that he had overpaid, and they sent a check that was fake. The scammers realized he believed them at some level ,and he lost about \$2,500. During their conversations with the victim, they used the type of words he used in his business to build trust.

The victim believed his sense of self-judgment to be high. He was able to identify one scam and convinced the scammer to send a check, which he then was able to trace and report to the police to get his money back.

The family believes there is a possibility the victim received numerous requests for money, mostly from people claiming relationships overseas. The victim had visited the area many times and knew several people in the area who claimed familial ties. He reconnected with them via Ancestry.com. They believe the victim may have received requests for money from a growing community of relatives. He was very secretive about the correspondence with the local family, but he continued to mention the interest in helping relatives from “back home.” They are unsure of the amount of money he may have sent to his old/new family members.

### **B1**

This case is based on police records of a grandparent scam.

On a Friday morning in September 2017, an 82-year-old husband and 78-year-old wife were called by an individual masquerading as a Miami Dade police department lawyer. The scammer reported that their 42-year-old son was being held in police custody for a DUI. Reportedly, the son was responsible for an accident and was under arrest. To keep the son out of the general jail population would require \$5,000. The victim offered to wire the money, but she was informed that would take too long. She was instructed to purchase Best Buy or Target gift cards.

The victims were able to speak with their son. However, when they asked why he sounded so different, they were informed that he had a swollen face resulting from the stitches and injuries.

The wife then purchased a \$5,000 Best Buy gift card, providing the numbers on the back of the card to the scammer. The scammer then requested an additional \$11,000 in order for their son to be able to stay in a hotel and then leave the state of Florida. The wife then purchased a \$5,000 Target gift card and a \$6000 Best Buy gift card, again giving the numbers off the back of the card to the criminal.

The victims called the police the next day; however, there was not enough evidence for law enforcement to investigate further. The case is suspended.

## **B2**

This case is based on police records of a grandparent scam.

On a Friday afternoon in November 2017, a couple in their 80s were called by a male who asked to speak to “Grandma.” The caller appeared to be in distress. The background noise made it difficult to hear the caller. The caller asked if she knew who it was and victim replied, “Is this [name]? What is wrong?” The caller affirmed the name.

The caller claimed to be in a lot of trouble, stemming from a car accident where someone was seriously injured. The masquerading grandson claimed to have a public defender and requested permission for the attorney to call the grandparents. The scammer begged the victim to not leave him in jail and to not tell anyone. He claimed to be so embarrassed and ashamed, promising to “make it up to you.” The grandmother asked for the name of the attorney, which was provided.

With the victims’ agreement the alleged public defender called a few minutes later. The purported public defender indicated he would be defending their grandson in court. The victims were told their grandson had been driving a friend’s car and was speeding. Reportedly he drove through a red light and struck another car thereby injuring

the other car's occupant. Although the injuries were serious, the lawyer wanted to post bail of \$5,000 before the weekend. The victims were assured the return of the funds as long as their grandson was in court the following Monday.

The purported lawyer instructed the victims to fill out a deposit slip at Bank of America in a specific name. The lawyer called back and reinstructed them to use the name Green Energy Solar and told them that this is a Bank of America modus operandi to protect the privacy of arrested individuals in need of bail funds. The victims complied with the instructions.

Upon arriving home, a fictional bail officer called to inform them that the driver of the other car just had a miscarriage due to the accident. He stated that there would be additional charges as well as the likelihood of a civil lawsuit. The bail officer stated the court required an additional \$4,225 for fees and damages. The victims stated they were unable to pay additional funds. Before hanging up, the bail officer stated she understood and that the grandson would be released in an hour and a half with instructions for Monday.

The victims called a family member to talk about the incident. They immediately offered to come to their home and help. It was not until late that evening, when the grandson was finally contacted, that the victims learned he had been in church all evening. The family called the police.

The police contact a Bank of America fraud investigator who was able to freeze the account and pending account fund movement. The police fraud and Bank of America fraud investigators were able to identify another victim. In April 2018, the police fraud investigator requested funds be returned to the identified victims.

**B3**

Case B3 is based on police records of a lottery scam.

In February 2018, a victim's daughter reported to the police that her 85-year-old father had been notified of lottery prize winnings from the previous year. In November 2017, her father wired 53 payments via Western Union for a loss of \$126,550. The money orders were sent to seven payees, supposedly all located in Guinea.

Although there were names associated with the seven payees, attempts through the Department of Homeland Security's Center for International Safety and Security failed to associate additional identifiers to any individual.

**B4**

Case B4 is based on police records of a grandparent scam.

On Wednesday, May 16, 2018, an 88-year-old grandfather was called by someone claiming to be his grandson needing bail money. The masquerading grandson handed the phone to an impersonating lawyer. The attorney requested \$3,400 be sent to a Wells Fargo bank account. The victim complied with this request and an additional request of \$6,600.

Upon returning home and learning of the money demands and transfers, his wife contacted their grandson who was at home. They immediately called the police. Wells Fargo noted the money had been withdrawn from a long-standing account. The case is suspended until further leads develop.

**B5**

B5 is based on police records of a false ID theft.

In August 2018, a 70-year-old man reported to police that while vacationing in Taiwan he received a telephone call from individuals claiming to be from the Taiwanese police department. He was informed that he would be under arrest for certain Taiwanese crimes, but that he was the victim of identity theft and the perpetrator was fraudulently using his name. He was advised to wire funds to the masquerading prosecutor's office in order to clear his name and so they would not tell anyone.

He returned to the United States in May 2018 and from May until the end of July 2018, he made several wire transfers totaling \$751,980. Numerous recipients were located in China.

When he became suspicious, he shared the story with his son, who recommended he contact the police due to fraud. As of the date of this interview, this case is now in inactive status.

### ***CI***

This interview is with an APS social worker.

The victim is a widow in her late 70s, who possessed at least a bachelor's degree. She had been happily married for many years and was very wealthy. She had no children or family for emotional or physical support.

The victim used her laptop several times a day to go online. She loved ballroom dancing and had a wide variety of interests. While she had a very active and rich social life, none of her peers had her energy or intellectual interests.

She used her laptop for on-line banking, communicated using email, and was active on Facebook as well as Match.com, where she met her scammer. The scammer, who claimed to be an American businessman in Malaysia, and victim were in a four-

year-long relationship. Numerous events prevented him from returning home to be with her, including paying off corrupt government officials. He was always in need of the funds she sent, which he said were often hijacked by unscrupulous banks and so on. They spoke with each other daily, but they did not video chat, so she never saw him. She was truly in love with this man who told her all the “right things.” Over this four-year period, the victim sent at least \$100,000 to her scammer.

In 2013, APS was notified by her investment company that the victim requested to transfer \$250,000 to a man in Malaysia. The victim became concerned that investment company overstepped and demanded the money be sent. The investment company relented, but requested she send the money through the American Embassy or a contract agency there. She was adamant the money be sent, but the company agreed to delay long enough so APS could meet with the victim. Overwhelming evidence of ongoing Malaysian romance scams convinced victim that she was a victim. In the beginning of this five-month-long process, the victim was honest with APS, but she stopped being honest as more evidence was produced. Due to her high level of functioning, no sign of cognitive impairment, and exceptional physical capabilities, she was not placed under guardianship. The law limits how much APS can be involved; therefore, there has been no follow-up.

## **D1**

This is an interview with an APS social worker regarding a romance scam. The victim is a cognitively intact woman in her late sixties who is still working. She has been divorced several times and was on a dating website where she met someone. She checked his veracity online in order to avoid a scam. Her three failed

marriages made her feel unworthy, and she was anxious to make this relationship work.

He claimed to want to be married and they were quickly engaged.

She unwittingly became a money mule by handling \$61,000 of his “business funds” that were wired into the bank for him. He claimed to own a house in the D.C. area, but discouraged her from checking on it because he did not think it was safe enough for her to be there. He was working overseas as a contractor and began to have problems with his credit cards. He said that he needed money for his existence. She wound up giving him \$98,300 of her own money to help him with his day-to-day expenses. In reality, the total was nearer to \$110,000. She borrowed money from family, and she was referred by her bank when she tried to get a loan.

In March 2018, when APS contacted her, she claimed it was a mistake at the bank. At first, she was in denial, but she became more honest and accepting about the reality of the relationship. Although she never met him or visually saw him, she admitted she had an addition to the scammer. When she refused to send additional funds, he became abusive and told her, “You are a weak, vile person.” She is seeing a therapist and admits she needs help making choices about money.

## ***II***

This was an interview with an APS social worker.

Although the husband is younger than the wife, both are in their seventies. The couple were referred to APS by the bank in 2015. The wife, who has a PhD, conducted research into the possibility of starting a business online. She went to Las Vegas to take courses in starting a business. Using her husband’s IRA accounts and three computers, the wife bought into time-share schemes, losing approximately \$1,000,000. While the

doctor's assessment indicates she is cognitively intact and has capacity to take care of herself, she appears to not fully understand the consequences of her financial behavior. She knows she lost money, but she believes that she will be able to get the money back and tries to obtain bank loans.

The husband, who is not as well educated as his wife, suffers from poor self-esteem and some level of isolation due to his poor hearing. He is considered a victim of his wife's online investment in phony schemes and self-neglect, and therefore he has received court ordered financial guardianship.

## **I2**

This was an interview with an APS social worker regarding a romance scam.

The victim is a cognitively intact woman between the ages of 70 and 84. She met someone on Match.com. Her bank referred her to APS in 2013. Her friend tried to convince her that she was being scammed, but she refused to believe she was being scammed. While she did not need financial assistance, her lawyer was able to get her close friend to be a joint owner of her bank account.

## **K1**

This was an interview with an APS social worker regarding a romance and investment scam.

A retired, never married, cognitively intact county worker between the ages of 70 and 84 was online multiple times each day. In addition to seeing his doctor, he would get health advice online from someone claiming to be a Utah doctor. The Utah doctor prescribed herbs, which he bought online and used to self-medicate. In addition, he was so interested in alternative spirituality that he visited the saints in New York.

In February 2017, he met someone on Match.com. The love interest used spiritual talk and came across as someone who was helpless and needed his help. The victim assumed the caretaker role. He took out a line of credit to pay for his wife's dowry and believed he had been married in a ceremony conducted by her uncle via either Facetime or Skype.

He paid the \$9,600 tax due on the \$9 million of gold bullion she was due to inherit. In addition, between March and May 2018, he made five transfers of almost \$80,000 to a bank in Ghana. The bank notified APS in May 2018 when he tried to borrow \$9,000.

At some level he knew he had been scammed, but he was guarded about acknowledging how much. He did not believe the scam happened to him, and he did not fully accept that she was a scammer. The potential exists that he was being blackmailed due to Skype or Facetime sex.

## ***L1***

This was an interview with an APS social worker.

The victim is a retired, possibly cognitively challenged, married man between the ages of 65 and 69. His wife was younger and worked during the day. While she was gone, the victim would communicate with the scammer every day. The scammer ostensibly agreed to be his mistress due to the victim's 10-year lack of intimacy between himself and his wife. He expressed helplessness and loneliness and sent money to bring his intended mistress to the United States in hopes of continuing the relationship.

In addition, he invested in bars of Ghana gold. When he met with APS, he had no insight into Internet scams or romance scams. He was disappointed that he was unable to get his African girlfriend to the United States.

## ***M1***

The victim is in her 80s, the interview is with a fellow parishioner.

The victim is a retired Department of State employee with an almost 30-year career where she served in several countries. She lived alone with her cats and had no immediate family. In retirement, she was active on the internet, where she had pleasant conversations with someone from the African continent for at least three to six months. She grew up in a family supported by a coal miner in a small, family-oriented community, and her trust in others was very high. She and the scammer talked about her birthday, where she lived, and that she had just sold her home. She told him she put her money in a bank until she could find a smaller retirement home to buy. The scammer now had her name, birth date, and home address, and therefore the value of her home and approximately how much her government retirement paid her.

The emails were sporadic as the scammer claimed he needed to work in order to support others. A few weeks later he told her he had money problems and needed to feed his children. The scammer convinced her to send him \$100. He then claimed he had problems getting the money due to not having a photo ID or necessary codes. He then told her that it would be better to wire the funds to the bank. A few weeks later, he still had problems. Then an electronic funds transfer request at her banking institution transferred the money to an account that was closed immediately after the funds were removed.

Law enforcement informed her there was nothing that could be done. She is a very private person and told none of her friends or anyone at the church. Distant relatives were unable to have her move in with them, and she moved into a senior living community. She began to have memory issues, claiming people were doing things in her room, which turned out to be the cleaning crew. She claimed they were stealing from her. She moved to other senior living communities. Eventually, she went to a homeless shelter. She stopped taking her blood pressure and diabetic medications. Her behavior became more erratic, and she was admitted to a hospital several times. Eventually, the courts called in APS to help her.

Church members were notified and, while they visit her, she is presently living in an assisted living plus community. She suffers from dementia, receives public assistance, and lacks the quality of life she has earned.

### **Existing Law and Selected Criminal Cases**

National legislative attention to elder abuse is not recent but suffers from disjointed effort and predictable bureaucratic inertia. Elder distress gained national level recognition during the Depression in the 1930s when many older Americans experienced widespread poverty. To help alleviate the fear of old-age impoverishment, President Franklin D. Roosevelt signed the Social Security Act of 1935 on August 15<sup>th</sup> (Social Security Administration 2014). Another significant step toward elder care occurred in 1950. President Truman held the first National Conference on Aging, which was followed President Eisenhower's creation of the Federal Council on Aging in 1956. In 1958, Congressman John Fogarty introduced the White House Conference on Aging Act (Public Law 85-908) to draw attention to this vulnerable population. Recognizing special

requirements of older citizens, Congress amended the Social Security Act in 1962 to establish senior citizen protective services through the states.

President Johnson signed the Older Americans Act (OOA) into law on July 14, 1965, in response to the need for senior citizen social services. This act concurrently established the Administration on Aging (AoA) to lead a national effort under the direction of the Department of Health, Education, and Welfare (now part of the Department of Health and Human Services). Although this act has been amended 15 times, this statute has provided programs for older citizens with significant funding (AoA 2014). Two amendment examples are those of 1973 and 1978, which added a nutrition program and the long-term care ombudsman respectively.

The delegates attending the White House Conference on Aging in 1971 crafted the Supplemental Social Insurance program and the National Institute on Aging. The 1974 Social Security Act Title XX authorized the support of protective services to adults who were suffering from abuse, neglect, or exploitation. While this legislation was the impetus for the creation of state level Adult Protective Services (APS), the requisite yet challenging grant process resulted in erratic, and often insufficient, funding for adult programs. Compounding the inadequacy of federal level subsidies were the states' funding problems, as states made tough spending tradeoff decisions concerning programs for children and adults. According to Robert Blancato (U.S. Congress, Senate, Financial Committee, Elder Justice 2019), National Coordinator of the Elder Justice Coalition, funding levels declined significantly despite Congressional hearings to raise public awareness of elder mistreatment funding.

In 1981, the third White House Conference on Aging discussion was focused around the pervasiveness of elder abuse (Linberg et al. 2011). It was during this timeframe that Congress recognized the impact of overly stringent legislation and states were given more flexibility in the 1981 amendment to address needs within their communities. While The Victims Crime Act of 1984 applies to all citizens, it provides for financial compensation for medical expenses and lost wages to victims. It was a step toward reparation for abused seniors. In 1988, additional grants were added for state and community programs on aging, Hawaiian natives and Indian tribe support, and nutrition services. The reauthorization of the Older Americans Act in 1987 defined elder abuse and the requirement for the protection of residents in nursing homes. Unfortunately, funds were never appropriated. For several years, most of the funding for elder assistance was directed through the States' Adult Protective Services.

The 1992 Older American Act reauthorization was a pivotal amendment from an elder justice perspective. It included a new Title VII, Vulnerable Elder Rights Protection Activities, focused on protecting the rights and enhancing the benefits of vulnerable senior citizens (O'Shaughnessy and Napili 2006). Congressional language concentrated on the elderly who suffered deprivation and needed intervention by state agencies to "provide firm leadership" and converge advocacy on the issues affecting those who were the most socially and economically vulnerable. The twofold purpose of the legislation was to strengthen the collaboration of four advocacy programs and encourage a system level holistic, inter-program linked approach to elder rights advocacy. The four overarching programs were the Long-Term Care Ombudsman Program; Programs for the Prevention of Abuse, Neglect and Exploitation; State Elder Rights and Legal Assistance

Development Programs; and Insurance Benefits Outreach, Counseling and Assistance Programs. The 1995 Institute of Medicine evaluation of the Ombudsman program highlighted the program's inadequate resources compared to the mandated requirements and noted the top residents' complaints were rights and quality of life (Colello 2012).

The third White House Conference on Aging in 1995 helped to institute the National Family Caregiver Support Program and stressed the requirement to develop strategies for identifying, addressing and preventing abuse of senior citizens. The 2005 White House Conference on Aging resulted in resolutions sent to Congress and the President addressing lifespan planning, expanded workplace opportunities for seniors, community, health care and long-term living, civic and social engagement, innovative housing designs, caregiving, and technology and innovation in an emerging senior marketplace. It also recommended reauthorization of the Older American Act.

In 2015, the White House Conference on Aging's theme was "Empowering All Americans as We Age" (White House 2015). This conference launched Aging.gov to provide information on the resources available to older Americans, families, and care givers. There were several initiatives for better-quality nursing facilities, improved retirement savings plans, enhanced access to technology, and the ability to age in place. In addition, it provided the promise of a clarification from the Department of Justice on the Victims of Crime Act (VOCA) for victim assistance, in that VOCA funds may be used to support legal services for crime victims.

The Elder Justice Act of 2002 was the first legislation that addressed elder justice issues to receive serious consideration. It was introduced in the 107<sup>th</sup> Congress (2001-2003) by Senator John Breaux (D) of Louisiana and co-sponsored by ten other Democrats

and seven Republicans. The act amended the Social Security Act and was referred to the Senate Finance Committee, but died there. Despite not moving forward, the Act was recognized as a human rights issue of freedom from abuse and exploitation. In February 2003, the Elder Justice Coalition was formed, bringing together advocates committed to the reform of social policy for the protection of elders (Linberg et al. 2011). The Elder Justice Act was reintroduced in the 108<sup>th</sup> Congress (2003-2005), the Senate Finance Committee led by Senator Charles Grassley (R-IW) approved the bill, but the Senate did not act on the bill. In the 109<sup>th</sup> Congress (2005-2007), Senators Orin Hatch (R-UT) and Blanche Lincoln (D-AR) introduced the bill in November 2005. Again, the Senate did not pass the Finance Committee supported bill. However, in 2006 key responsibilities were added to the reauthorization of the Older Americans Act. A key feature required the Administration on Aging to develop and implement a multidisciplinary effort (law enforcement, health and social services) to address elder justice issues and to conduct an elder abuse incidence study (O'Shaughnessy and Napili 2006). This act mandated the Attorney General and Secretary of Health and Human Services to conduct a study to examine the feasibility of instituting a national database on elder abuse. Although the report was due in two years, the report was issued in 2010 characterizing the types of data required for a comprehensive understanding of elder abuse (DHHS 2010). The report considered the collection of data on victim and perpetrator demographics, risk factors, abuse consequences, and criminal actions important in order to perform data analysis and build risk assessment tools.

Senators Lincoln and Hatch introduced the Elder Justice Act in the 110<sup>th</sup> Congress (2007-2009) on March 29, 2007 and the bill was referred to the Senate Finance

Committee to no avail. The Senate Finance Committee considered the bill in September of 2008 and again supported the bill when then Democrat Senator Max Baucus of Montana submitted a bill to amend the Social Security Act. Republican Orrin Hatch of Utah and Democrat Blanche Lincoln of Arkansas in the Senate introduced the Elder Justice Act of 2009 on April 2, 2009. The House of Representatives' New York Republican Peter King, and Democrats Tammy Baldwin of Wisconsin, Jan Schakowsky of Illinois, and Joe Sestak of Pennsylvania introduced the companion bill. The Elder Justice Act was included in the Senate Finance Committee version of the Affordable Care Act. The Elder Justice Act passed as part of Public Law 111-148, 2010, the Patient Protection and Affordability Care Act. While the problem of elder abuse was identified decades ago and recognition of a need for legislation started in 1992 with the passage of the Vulnerable Elder Rights Protection Activities as part of the Older Americans Act, the change in public opinion was brought about by political activism and media coverage of the elderly who were neglected, sexually or physically abused, or were financially exploited. In the intervening years, there have been alternative proposals and enactments to amendments and laws such as the Social Security Act and Older American Act. This legislation is Subtitle H in Title VI of Public Act 111-148, the Patient Protection and Affordable Care Act (PAACA) and has several provisions that amended the Social Security Act sections under a new Subtitle A, Block Grants to States for Social Services and included a new Subtitle B, Elder Justice (Colello 2017).

During the 115<sup>th</sup> Congress Senate Judiciary Committee Chairman Chuck Grassley (R-IA) introduced the bipartisan Elder Abuse and Prevention and Prosecution Act (Public Law 115-70) to address elder financial abuse. The bill, cosponsored by Senator Richard

Blumenthal (D-CT), Senator John Cornyn (R-TX), Senator Amy Klobuchar (D-MN), Senator Marco Rubio (R-FL), and Senator Michael Bennet (D-CO), was signed by President Trump in October 2017. This bill requires the Federal Trade Commission to establish an elder justice coordinator in the Bureau of Consumer Protection. It further requires the DOJ to ensure at least one federal investigator and prosecutor in each judicial district have expertise with elder abuse cases. It also expands data collection and information sharing among agencies as well as publicizes data about abuse cases and investigations. Convictions of interstate fraud where the victim is over the age of 55, committed by marketing by telephone, email, text, or electronic message, and the fraud involves actions that induce financial profit result in enhanced penalties. Any property, money, or asset acquired from the fraud must be forfeited; unfortunately, while the Act criminalizes the use of technology to financially abuse older citizens, it is unclear how the penalties are enhanced (Goodwin and Grover 2019). The penalties aspect presents another twist in the legal system process since federal law governs elder rights yet, elder abuse prosecutions are generally at the state level (Lovett 2013).

In May 2018, as part of the Dodd-Frank revision, President Trump signed The Senior Safe Act, which encourages financial firms to train employees to identify and report suspected exploitation of older investors not younger than 65 years of age. It also protects financial professionals who ‘in good faith’ report financial abuse of seniors under bank privacy laws. While the Act does not mandate financial institutions report suspected exploitation, an employee who is a supervisor, registered representative, investment advisor, or insurance agent associated with a financial institution must be

trained in order to receive the immunity provided by the Act. The overarching intent is to ensure the reporter is not held for violation of a privacy agreement.

In 1890, two lawyers, Samuel Warren and Louis Brandeis, published an article, “The Right to Privacy,” in the Harvard Law Review to bemoan the invasion of privacy in society newspaper publications. Their argument was that individuals’ affairs and property, both tangible and intangible, were private, and that the individual should enjoy the full protection of his or her person as a principle as old as the common law. “What Judge Cooley refers to as the right ‘to be let alone’” (195).

Law review articles credit the Warren and Brandeis article with the movement to develop four torts in common law or state statutes: intrusion upon seclusion (solitude), appropriation of likeness or name, publicity of a private life, and publicity of an individual in a false light. These torts provide the liability under common law, yet not all states nor does the federal government recognize all of the torts. The right “to be let alone” with regard to the term property has come to mean both tangible and intangible possessions. While most understand what is meant by a tangible possession, intangible is less clear. An example of an intangible possession would be the value of intellectual property (IP); it is an asset if it has an associated price with the IP. For decades, the litmus test for privacy was based on the work by Professor Alan Furman Westin who believed consumers were privacy pragmatic. Westin claimed in his 1967 book, *Privacy and Freedom*, consumers were in the best position to determine what information should be given to others. In other words, consumers would evaluate the value and risk of sharing information centered on their own needs and wants (Urban and Hoofnagle 2014). His consultancy role with industry influenced much of the data sharing “rules” of the

marketplace for decades (Urban and Hoofnagle 2014). However, University of California, Berkeley School of Law Professors Urban and Hoofnagle give greater insight into the idea of pragmatic decision making with regard to privacy. They found consumers possessed a “flawed, yet optimistic perception of protections, and often did not exercise a requisite analysis because they were unaware of the “rules and practices” (Urban and Hoofnagle 2014).

Consumers tend to trust corporations while equally not trusting the government. In January 2018, almost 17 percent of American homes had a smart speaker<sup>57</sup> in their home (e.g. Alexa, Echo Dot, Siri; Perez 2018). Google as well as other companies admit they record, store, and have employees listen to personal recordings (Bensinger 2019). This is in stark contrast to the Katz v. United States court case of 1967, where the petitioner disputed the FBI agents’ authority to record his conversation outside a telephone booth that led to a conviction in violation of 18 U.S.C. 1084 (wagering information across state lines). The petitioner appealed under the Fourth Amendment protection for the seizure of tangible items (recording of oral statements). In essence, the court agreed and the opinion of the United States Supreme Court stated that “what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” While none of the smart speaker companies are the federal government, judges have successfully issued warrants for smart speaker recordings (Fowler 2019). There is the question if the smart speaker owner has an optimistic perception of protection or made a truly pragmatic decision regarding their privacy not

---

<sup>57</sup> Smart speaker – a wireless, voice activated virtual assistant using speech recognition that enables the user to control various functions in the house as well as providing time of day, date, music, weather, and requested information.

just for what may be sought by the courts by how their data is stored, transmitted, or monetized.

While tort law privacy is often interpreted to mean freedom from intrusion into personal matters, it is the legal perspective of confidentiality where an individual gives express consent whether or not to share personal information. In this regard, there are some legal protections of varying levels for specific areas of personal information. For example, The Health Insurance Portability and Accountability Act (HIPPA) of 1996 (Public Law 104-191) gives patients more control over their health information while simultaneously adjudicating disclosure in order to protect public health. This Act engenders accountability with civil and criminal penalties for violating patients' privacy rights. However, once their private information is made public, the individual has little recourse to make it private again. While 2015 and 2018 represent a timeline, there were 955 major security breaches exposing over 135 million healthcare records (HIPPA 2018). That specific information may have been collected, stored, unsecurely transmitted, sold, or used for whatever purpose the 'new' owner decided, including monetizing it.

### **Cybercrime Law Review**

There are two undeniable facts: no crime (*nullum crimen*) or resulting punishment can exist without a legal underpinning (*nulla poena sine lege*) and “[t]he individual human being is manifestly the object of every legal system” (Dinstein 1985, 206); therefore, it is necessary to discuss the legal underpinnings as it pertains to cyber-enabled financial abuse against older Americans (Cross 2005). Cybercrime is a term used to represent illegal acts committed while using information communication technologies (ICT) that include, but is not limited to theft, invasion of privacy, bullying, and

confidence scams for financial gain or to cause harm on another person. When discussing law governing cybercrime there are three overarching categories. The first is Computer Law, which includes all those laws related to the computer itself. The second is Information Technology Law, which concerns how information is collected, transmitted, and stored. The third is Cyber Law or Internet Law governing the use of the internet. The latter two are of interest for analysis.

There are three subcategories of crimes: those committed against property such as hacking, intellectual property theft, and vandalism; crimes against the government such as accessing government systems, cyber terrorism, cyber warfare; and crimes against individuals, which is the focus of this paper and includes stalking, bullying/harassment (threats of violence, privacy invasions, and technological attacks), credit card fraud, bank fraud, slander, and manipulation. While some of the victims in this research were recipients of threats and privacy invasions, the legal analysis is focused on fraud and manipulation.

There are several laws that regulate the internet as explained by Harvard Law Professor Lawrence Lessig (2006), national law in the form of copyrights, such as the freedom of speech; social norms in the form of consensus based decision-making; international law in the form of airwaves or satellite use; and code whose overarching “laws” are created and enforced by the technology creators. While these ‘laws’ provide an intellectual explanation of the internet’s laws among societies, they do not explain to the scammed individual a means of redress.

A complete review of all laws is a practical impossibility, however this research endeavors to review the most significant U.S. laws. While not all-inclusive, the collected

data represents the laws surrounding cyber that support what is generally accepted as characterizing the legal and illegal cybercrime issues. Table 6 is an abbreviated list of the most salient policies. A discussion and analysis follow.

**Table 6. Salient legislation**

United States Code	Section	Colloquial name	Actus reus (prohibited action)/mens rea (intent)
5 U.S.C.	II § 552a	Privacy Act of 1974	Restrict disclosure of personally identifiable information, grant the individual the right to seek amendment of records maintained upon showing evidence that the record is not accurate, relevant, or complete, requires the government to comply with norms for collection, storage, and distribution of records.
5 U.S.C.	§ 552a	Computer Matching and Privacy Protection Act of 1988	Amended the Privacy Act to include safeguards for individuals applying for and receiving Federal benefits in the use of computer matching on records among Federal, State, and local governments.
15 U.S.C.	§ 45 (a)(1)	Federal Trade Commission Act of 1914	Unfair or deceptive acts or practices in or affecting commerce and the injury must be substantial involving monetary harm such as coercion of the consumer; must be injurious in net effects, and the consumer could have not reasonably avoided.
15 U.S.C.	§§ 6801-6827	Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act of 1999)	Unfair sue of private financial information; pretesting, shared information without notice. Financial institutions are required to protect the confidentiality of customer's personal information.
15 U.S.C.	§ 1601	Fair and Accurate Credit Transactions Act of 2003	The FTC is charged with leading the government's development of guidelines for identity theft prevention programs with financial institutions.
15 U.S.C.	§ 1681	Fair Credit Reporting Act of 1970	Improper use of consumer information. Regulates credit bureaus, entities, or individuals use credit reports as well as financial institutions and companies that furnish information to credit bureaus.
15 U.S.C.	§§ 7701-7713	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)	"Imposed regulations on the transmission of unsolicited commercial email, including prohibitions against predatory and abusive email, and false or misleading transmission of information."

---

18 U.S.C.	§§ 2710	Video Privacy Protection Act	Violation of personal privacy from rental, purchase, or delivery of video tapes or similar audiovisual materials.
18 U.S.C.	§ 1028	Identity Theft and Assumption Deterrence Act of 1998	Whoever knowingly and without authority produces, transfers, possesses identification document, feature, or false identification document, or traffics in false or actual authentication features for use in false identification documents.
18 U.S.C.	§1028, § 1028A	Identity Theft Penalty Act of 2004	Provides for aggravated identity theft penalties.
18 U.S.C.	§ 1029	Fraud and related activity in connection with access devices	Knowingly and with intent to defraud produces, uses or traffics in one or more counterfeit devices and obtains anything of value aggregating \$1000 or more.
18 U.S.C.	§ 1030	Computer Fraud and Abuse Act (CFAA) of 1986	Whoever knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the US Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations.
18 U.S.C.	§ 2011	Wire and Electronic Communications Interception and Interception of Oral Communications	Except as otherwise specifically provided, any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.
18 U.S.C.	§ 2510-2522, 2701-2712, 3121-3126	Electronic Communications Privacy Act of 1986	Prohibits unauthorized address to obtain sensitive information such as national security, financial, and consumer credit records. In addition, it prohibits trafficking in U.S government passwords.
18 U.S.C.	§ 2520	Wiretap Act	Protect individual privacy in communications with other people who intentionally intercept communications using a device. Amended in 1986 to include electronic communications such as email.
42 U.S.C.	2000aa-5 –2000aa-12	Privacy Protection Act of 1980	Protects journalists from law enforcement requests for documents, notes, sources

---

---

42 U.S.C.	§§ 17901 et. Seq.	Health Information Technology for Economic and Clinical Health Act	“Expanded privacy and security requirements for protected health information by broadening HIPAA breach disclosure notification and privacy requirements to include business associates of covered entities.”
44 U.S.C. Chapter 35	§§ 301-3549	Paperwork reduction Act of 1995	Directed the office of Management and Budget, the National Institute of Standards and Technology, and the General Services Administration to implement policies for paper reduction that securely stored information and protected privacy.
45 U.S.C.		Health Insurance Portability and Accountability Act (HIPAA)	Exposure of certain health information
47 U.S.C.	§ 151 et seq. (et seq. = The Communications Act of 1934 and what follows)		Established the Federal Communications Commission and provided the FCC authority over domestic and international commercial wired and wireless communications. Provides protection by cable operators of information about subscribers.
47 U.S.C.	§ 227	Telecommunications Act of 1991	Amended the Communications Act of 1934. Restricts telemarketing and automated dialing systems, prerecorded voice messages, SMS text messages. It prohibits telemarketing before 8am or after 9pm (local time). In addition, it implemented the FCC's do-not-call regulations and made it illegal for prerecorded voice messages or via automatic telephone dialing system. It is further illegal for a call “to any telephone number assigned to a paging service, cellular service, specialized mobile radio service, or other radio common carrier service. Or any service for which the called party is charged for the call.

---

---

47 U.S.C.	§ 609	Telecommunications Act of 1996	Amended the Communications Act. Regulates U.S telephone, television, telegraph, and radio communications. Seven subchapters regulate all aspects of communications and broadcasting industry. It also deregulated competition for the telecommunication industry.
47 U.S.C.	§§ 223,230	Communications Decency Act of 1996	To regulate indecency and obscenity on telecommunications systems, including the Internet.

---

What is thought of as harm from a legal perspective may be significantly different from an individual's perception of harm. What is considered a violation or not a violation against an individual often is determined by the violator. For example, the U.S. Government is held to a higher standard for the violation of privacy than individuals or corporations. The laws governing the collection, transmission, and storage of citizenry data is covered by the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988 (maintenance of personally identifiable information subject to the Privacy Act), the Financial Services Modernization Act of 1999 (financial privacy), the Electronic Communications Privacy Act of 1986 (interception of communications), and the Fourth Amendment. Supreme Court Jurisprudence shows support for the privacy rights of individuals from invasive government action without a warrant. In general, the support against an invasive government stems from the Fourth Amendment:

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.

U.S. Supreme Court has assessed injury for the violation of federal privacy law with or without pecuniary harm. Privacy is a much-debated term, as noted in the literature review, since the 1890 *Harvard Law Review* article, "The Right to Privacy," by Samuel Warren and Louis Brandeis. For the citizenry, the problem is quite complicated. In his majority opinion, Chief Justice William G. Brennan stated, "[t]he overriding function of

the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.” (Schmerber v. California 1996). While some believe the Fourth Amendment, as sustained by the Supreme Court (Schmerber v. California 1996), supports individuals’ privacy rights, the right extends only from unwarranted governmental intrusion as reinforced by the Griswold vs. Connecticut (381 U.S. 479, 1965) where the Supreme Court found the state violated the right to marital privacy. While the right to privacy is not explicitly mentioned in either the Bill of Rights or the U.S. Constitution, Chief Justice Warren opined in Griswold vs. Connecticut, the right to privacy exists and is embodied in the liberty interest of the Fourteenth Amendment. In general, privacy laws are patchwork of legal protections in the form of agency regulations and individual statutes against governmental intrusion.

Since the illusive term privacy is not further defined in U.S. law where private entities are concerned, internet service providers (ISP) and Data Aggregators are enabled to collect, transmit, store, and sell individual’s personal information. The ISP is not held responsible for the content a user may post using the ISP’s service. There are a couple of reasons for this. One reason is the Digital Millennium Copyright Act (DMCA) of 1998, where ISPs successfully argued that they could not monitor every download from a user. The other is the Title V of the Telecommunications Act of 1996, the Communications Decency Act (CDA), where in Section 230 the argument was made that ISPs are not like newspapers or magazines and therefore, not responsible for the content of an internet blog, posting, or an email.

The key provision of Section 230 for digital platforms such as internet service providers states that “[n]o provider or user of an interactive computer service shall be

treated as the publisher or speaker of any information provided by another information content provider.” The origins of the Communications Decency Act of 1996 stem from the successful lawsuit for defamation against Prodigy Communications Corporation, when an anonymous user accused an investment banker and his firm of fraudulent stock offerings. Prodigy had touted itself to be an online family safe environment by assessing comments and posts for pornographic material, however, the volume of material prevented Prodigy from monitoring all postings (Statton Oakmont v. Prodigy Services 1995). Since the ISP was moderating the website, the New York judge in 1995 likened the company’s action to that of a newspaper, which could be held liable as publishers of their customers’ content. This shook the nascent industry as a previous court in 1991 sided with CompuServe who had been unsuccessfully sued when a user posted defamatory information. The difference between the two cases was in on-line monitoring of content; the decision for the industry was clear, either monitor and expose themselves to possible law suits for defamatory content or don’t monitor where they might be held to a limited distributor liability (Stratton Oakmont v. Prodigy Services 1995).

Concerns of pornography transmitted over the internet led Congress to pass the Communications Decency Act of 1996; however, a 1997 case (Reno v. ACLU) affirmed by the Supreme Court, found that the CDA’s “indecent transmission” and “patently offensive display” clauses were in conflict with the First Amendment guaranteed protection of free speech.

What stood were the two important caveats in Section 230 of the CDA. The first holds the perpetrator responsible for the content, making ISPs held harmless for the acts of others. The second caveat allows for the ISP to moderate without liability for

removing offensive postings. The effect of these caveats is, unlike publishers of physical material, the publishers of virtual printed material cannot be held liable for the content and ISPs decide what is offensive and what is not.

A marked change to Section 230 occurred in 2017. President Trump signed the controversial Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) of 2017, which amends the Communications Act of 1934 and its amended Act, Communications Decency Act, to “clarify that Section 230 of such [CDA] Act does not prohibit the enforcement against providers and users of interactive computer service of Federal and State criminal and civil law.” The Electronic Frontier Foundation dubbed it the “Frankenstein bill,” because the requirement of platforms who are “only hosting questionable content and not creating it” to censor users has the potential to “silence legitimate voices” (Harmon 2018; Jackman 2018). The detractors of the Act claim it provides draconian penalties for a person found guilty of “using a means of interstate or foreign commerce owns, manages, or operates an interactive computer service or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person [with] a fine, prison or both.” The sponsors of this Act claim it is an attempt to address the estimated 4.5 million world-wide victims of human trafficking and the 99 billion dollar per year industry (Wagner and Jefferies 2019). Supporters of FOSTA contend that the original Section 230 has enabled online what is considered otherwise bad or in some cases illegal behavior. For example, the argument from the defendants of the shuttered Backpage.com ads, “the Internet’s leading forum for prostitution ads, including ads depicting the prostitution of children online,” against the FBI’s indictment rests on “unconstitutional government censorship” and the protection afforded the platform by

Section 230 (US v. Lacey, Larkin, Spear, Brunst, Hyer, Padilla, Vaught 2018; DOJ 2018).

The Electronic Communications Privacy Act (ECPA) of 1986 amended the Omnibus Crime Control and Safe Streets Act of 1968 to protect citizens' civil rights in the interception and collection of digital and electronic communications. ECPA Title II, the Stored Communications Act (SCA), protects the citizenry's privacy from the government's access to records and other content held by service providers. The ECPA was updated by Title III where electronic communications were defined to include texts, emails, and other digital communications. The Wire and Electronic Communications Interception and Interception of Oral Communications Act prohibits any individual from intentionally obtaining another person's oral or electronic communications. U.S. citizens may be held responsible for violation of this law, but only if the victim can show they suffered a concrete and personal injury traceable to the offender's actions (Spokeo, Inc. v. Robins 2017). However, jurisdiction matters, in March 2017, the D.C. Circuit 'affirmed a lower court's decision" that the courts lack jurisdiction if the violation occurs from a foreign country (Cardozo 2017).

While the intent is to ensure individual rights guaranteed under the Fourth Amendment's protection "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," the courts have also shown the right protects people not places. This is specific to the Third-Party Doctrine and the expectation of privacy online. The courts have interpreted the limits of the Fourth Amendment when the individual has voluntarily provided personal information to a third party such as a bank, telephone company, ISP, data aggregator, etc. (Kerr 2018). To receive many federal

government benefits such as social security, the user must communicate using the internet often via a third party. While Kerr (2009) claims individuals assume risk when they provide information via a third party, there often is no practical alternative. The third party that holds the data has significant authority over the data, which often includes how it is collected, stored, transmitted, and shared. Corporations like Google understand customers and the customers' perception of governmental search and seizure. To prove to the customer that the company has the customer's best interest as part of their business modus operandi, corporations have successfully argued against subpoenas due to the potential for loss of user trust (Kerr 2009).

The Federal Trade Commission (FTC) Act of 1914 was signed into law by Woodrow Wilson in order to outlaw unfair commerce practices and also established the Federal Trade Commission. Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC §45) prohibits “unfair or deceptive acts or practices in or affecting commerce.” An amendment protecting consumers, the Wheeler-Lea Act of 1938, granted greater authority for the FTC to regulate unfair and deceptive advertising practices targeting consumers. Specifically, the Act empowers the FTC to check for false representation in advertisements including food, drugs, devices, etc. It also states the “Commission is hereby empowered and directed to prevent persons, partnerships, or corporations from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce” (para 2). This prohibition applies to all persons engaged in commerce, including banks as well as those companies using big data analytics (Ramirez et al. 2016). Under the FTC is the Bureau of Consumer Protection, which is charged with protecting consumers against deceptive commerce

practices. The Bureau has the authority to bring action against false financial products and practices, telemarketing fraud, violations of privacy and identity theft as well as seek monetary relief for injured parties.

The Financial Modernization Act included provisions to protect personal financial information held by financial institutions. Also called the Gramm-Leach-Bliley Act, the Act has three main provisions. The first is the Financial Privacy Rule, which obliges banks, investment firms, and certain types of other entities to provide customers with a privacy notice at the initiation of the relationship and annually. The customer is entitled to know what information is collected, shared, used, and how it is protected. The Fair Credit Reporting Act of 1970 allows the customer the right to ‘opt-out’ of how some of the information is shared, however, each nuanced change to the policy requires the customer to ‘opt-out.’ If a customer does not opt-out each time, the default is to share the information with whomever is listed as the company’s partner in the notification.

The second provision is the FTC Safeguards Rule governing all entities whose business is substantially involved in providing financial services including credit reporting agencies. The Rule establishes the obligation for financial institutions to assess the risks of threats from disclosure, misuse, or destruction of customer’s information. It also requires the institutions to manage and control the risk of unauthorized access, and to report to its board annually on the compliance with their information security program. The Rule requires notifying customers of the unauthorized access to or use of customer information, when doing so would not interfere with an investigation. The third provision prohibits pretexting or the use of fraudulent statements by financial institutions or its partners to gain customer information. The third provision was instrumental in the

framing of the Telephone Records and Privacy Protection Act of 2006, where an individual is prohibited from pretexting to gain customer information about their telephone records.

Other records deemed private are video rentals. In 1988, President Regan signed the Video Privacy Protection Act with the express intent of preventing the disclosure of an individual's choice to purchase or rent a video. The disclosure of Supreme Court nominee Robert Bork's video store rental prompted the Act, which has been used to sue violations related to the privacy law. In 2009, Jane Doe v. Netflix Class Action Suit claimed Netflix "perpetrated the largest voluntary privacy breach to date, disclosing sensitive and personal identifying consumer information...given away to the world freely, and with fanfare, as part of a contest intended to benefit its trusted custodian." According to the court filing of December 17, 2009 in the San Jose Division of the Northern District of California U.S. District Court, the purpose of the contest was to "improve the predictive accuracy... of filtering algorithms" for movie recommendations. Netflix provided anonymized user data to contestants. The suit claimed contestants could use "contextual and background knowledge, in addition to cross-correlation with publicly available databases" to identify customers and their video viewing choices. Researchers Arvind Narayanan and Vitaly Shmatikov were able to de-anonymize the Netflix customers and their video viewing preferences. Narayanan and Shmatikov's (2010, 24) research revealed "any information that distinguishes one person from one another can be used for re-identifying the data."

The Fair Credit Reporting Act (FCRA) was enacted in October 1970 to ensure accurate, fair credit reporting while protecting consumer's privacy. Consumer Reporting

Agencies, while not licensed are regulated by 15 U.S.C. 1681 a(f). They assemble information on consumers and evaluate the data to make determinations based on consumer's credit worthiness, financial capacity, adverse information, character, and general reputation. Then they sell the reports to third parties. Third parties may use the data for myriad purposes including whether or not to extend credit, employment eligibility, or tenant housing. FTC reported businesses and data brokers who violated FCRA were fined substantial civil penalties by collecting detailed personal profiles, hobbies, ethnicities, and religions from off-line and on-line sources (Ramirez 2016). While the law prohibits the use of the data for targeting purposes, manipulation of the data in big data sets affords the opportunity of targeting by race, religion, national origin, sex, marital status, age, financial capacity, zip code, and general character.

The Fair and Accurate Credit Transactions Act (FATCA) of 2003 was signed into law by President Bush on November 22, 2003 to improve the accuracy of consumer credit records and how credit scores are calculated. The Act amends the Fair Credit Reporting Act (FCRA) by providing a means of reporting identity theft. In addition, the amendment enables the consumer the ability to decide what information may be shared with a third party, be notified of a fraud alert, and obtain free credit reports every year from the consumer credit reporting agencies. The Act directs the FTC to produce a consumer bill of rights for remedying the effects of fraud or identity theft from credit, electronic funds transfers, or transactions with a financial institution. Consumer reporting agencies are not allowed to report information against a consumer resulting from identity theft. The act specifically limits the use and sharing of medical information in financial systems.

The U.S. Government does recognize health information requires special consideration. The Health Insurance Portability and Accountability (HIPPA) Act, signed into law by President Clinton in 1996, provides for the ability to transfer and continue health care insurance coverage, sets standards for health care electronic billing information, and requires companies and health organizations to securely collect, transmit, and store personal health information. The Privacy Rule of 2000 regulates the use and disclosure of Protected Health Information (medical record and payment history) and the Security Rule of 2003 governs Electronic Protected Health Information. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 incentivizes the adoption of electronic health records, as well as the requirement to report data breaches to the Secretary of Health and Human Services that affect 500 or more persons. In consultation with the FTC, Health and Human Services issued a HITECH Breach Notification Interim Final Rule, requiring notification to individuals when their health information is breached (HHS 2013). Several states updated the laws for data breaches, but it is a patchwork of laws that are not standardized, in terms of notification timing, types of notification, or when it is required.

In the early 1980s, Congress passed the first major overhaul to criminal legislation since the early 1900s with the passage of The Comprehensive Crime Control Act of 1984. Among the provisions of the Comprehensive Crime Control Act was the Computer Fraud and Abuse Act (CFAA) of 1984, originally written to criminalize computer-related crimes committed against government-owned computers and systems, financial institutions, and medical institutions. Specifically, the CFAA prohibits unauthorized access to financial records, defense and intelligence-related information,

and other sensitive data. CFAA has been amended six times to include protection and regulation of personal and commercial computer networks against anyone who attempts or successfully commits an offense of this act. The transmission of a program, information, or code with the intent to deny the use of the computer or compromise its use is also prohibited. In 2019, LinkedIn lost an argument in the Ninth Circuit Court against HiQ Labs, who used automated bots to scrape and then analyze information from LinkedIn profiles without authorization when they invaded LinkedIn's privately stored and maintained servers to obtain the publicly accessible data (HiQ Labs Inc. v. LinkedIn Corp 2019). LinkedIn contended that "more than 50 million LinkedIn members at some point, elected to employ the "Do Not Broadcast" feature" and who have chosen to not broadcast changes to their profiles to their connections threatens members' privacy, particularly when employees have not informed current employers they are considering a new job (HiQ Labs Inc. v. LinkedIn Corp 2019, 6-7). The Ninth Circuit argued that there is a lack of evidence the 500 million members actually maintain an expectation of privacy when they publicly post the information, which indicates the court focused on the public profiles versus private spaces (HiQ Labs Inc. v. LinkedIn Corp 2019). In an argument between Facebook and Power Ventures, in 2017, the Ninth Court, unlike the LinkedIn case, found Power Ventures to be in violation of the CFAA and Controlling the Assault of Non-Solicited Pornography and Marketing Act. Power Ventures' business model enabled users to aggregate all of their own data in one place. While scraping users' information, Power Ventures made copies of Facebook's website, a copyright and trademark infringement and violation of the DMCA (Facebook Inc v. Power Ventures

2017). This court's action was focused on the crime committed against Facebook, not on the customers whose data was aggregated, shared, or sold.

The FTC is responsible for establishing national standards for the transmission of commercial e-mail and enforcing the provisions of the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. The CAN-SPAM Act has four main components: it prohibits commercial advertisers from deceiving recipients about the source or topic of the email, it requires all senders provide a means to 'opt-out' in order to stop receiving the email, it mandates all senders of unsolicited email to give a valid physical address, as well as identification that the email is an advertisement. Recipients of SPAM have a certain level, albeit low, of redress for receiving emails with misleading sources or content by opting-out. The intent was to curtail SPAM and, most specifically, unsolicited pornography. While corporations and marketers have been occasionally held accountable for emailing unsolicited marketing, there is no evidence that this largely unenforced law has had any impact on criminal behavior. CAN-SPAM has not stopped millions of SPAM messages ensnaring the recipient into responding to charity, romance, lottery, and other illicit schemes. Criminals use spoofed email addresses of real corporations, such as banks, to lure innocent victims into responding to the request to log-on, thereby giving criminals the access code to their account. CAN-SPAM has reportedly contributed to the arrest of perpetrators; however, it also complicates several state laws, which provide greater assistance to some citizens. The majority of internet SPAM traffic are not legitimate emails, but simply "bulk, commercial, unsolicited electronic marketing messages," making up 72% of all worldwide emails (Kigerl 2016, 62). Cyveillance (2010) found that Internet hosting companies (Internet Service Providers or ISP), which

are located worldwide, aid illegal online pharmacies, as the ISPs are not held responsible for the content of the websites. In addition, the technology (secure socket layer or SSL), which encrypts end-to-end communications, makes it easier for websites to conduct their illicit business, as they are often protected from legal oversight. The focus for the law was on commercial email versus all unsolicited email and, in a study of CAN-SPAM Act prosecutions, Kigerl (2016) revealed a level of a possible deterrent effect, but not necessarily for the perpetration of fraud. Specific to this policy, is the lack of ISP responsibility for content.

In 2011, FTC issued a Consent Order, where it settled charges that Facebook deceived consumers by failing to keep privacy promises (FTC 2011). Facebook was barred, among other things, from making false privacy representations and overriding privacy preferences without obtaining consumer's express affirmative consent. Facebook was also required to protect privacy and confidentiality of consumer's information. In March 2018, FTC, again, began an investigation into Facebook's privacy practices (Kaplan 2018; Matsakis 2018). The FTC found Facebook were deceptive in their stated disclosures regarding users' privacy in direct violation of the FTC order (FTC 2019). The FTC found Facebook allowed third-party developers to collect and mine data on millions of users. In one case, Cambridge Analytica collected and analyzed data from Facebook, including users who participated in a quiz, as well as their friends (FTC 2019).

Stemming from the Cambridge Analytica admission, a lawsuit was filed on September 9, 2019, in the U.S. District Court, in the Northern District of California, against Facebook for sharing users' names, gender, age, address, photographs, homemade videos, video preferences, religious views, political views, relationships, and other

information with third parties. The privacy-based tort claim is based on the Stored Communications Act and the Video Protection Act. Facebook has filed to dismiss the suit for three reasons: 1) Users have no legitimate privacy interest in social media-posted information; 2) There were no tangible negative consequences as a result of the exposure; 3) Users consented to the sharing of their information (Facebook, Inc., Consumer Privacy User Profile Litigation 2019).

With regard to user's expectation to legitimate privacy interest, for any information users make available on social media, Facebook may be relying on the Ninth Circuit argument that there is no expectation of privacy on publicly posted information and the Third-Party doctrine, where the original owner may lose ownership over the data, once it is shared with a third party (HiQ Labs Inc. v. LinkedIn Corp 2019). Facebook successfully had a lawsuit dismissed in 2015, where Facebook was accused of using cookies to intentionally track users' browsing activity across the internet, even when the user logged off of Facebook. The court held Facebook did not intercept the communications in violation of the Electronic Communications Privacy Act or the Stored Communications Act.

In terms of Facebook's argument against tangible harm, the Ninth Circuit stated that the inaccurate conveying of personal information that affects an individual may be sufficient injury (Spokeo, Inc v. Robins 2017). However, the harm must be closely related to a traditionally accepted harm. It is difficult for plaintiffs to know the extent of potential harm, as they do not know how their data will be used and when. According to the complaint, Facebook engaged in the disclosure of private facts of users. These facts were not a matter of public concern, the disclosure was to the public, and the disclosure is

offensive and objectionable to the reasonable person, which is a requirement for a breach of privacy. The Wiretap Act makes it unlawful to listen to another person's communication or read their text, email, or other messages, and the Electronic Communications Privacy Act (ECPA) protects email messages from interception and disclosure to third parties. Arguably, the reading, sharing, and selling of emails, texts, or other messages is a violation of the Wiretap Act and the ECPA. Facebook argues that sharing information is a social norm that underpins Facebook and that Facebook did not violate that social norm by sharing users' data in a manner consistent with the users' preferences. This may be a breach of trust of the users who selected private communication (Facebook, Inc., Consumer Privacy User Profile Litigation 2019). Facebook's argument is juxtaposed to its stance in 2016, when Facebook, in Facebook, Inc. v. Superior Court, demurred to deliver a user's post to law enforcement, claiming to do so could divulge the user's private interests and affairs, as well as personal information, which may include representation of their thoughts, feelings, and intentions, and, as such, there is a significant expectation of privacy that requires a warrant to gain access (Facebook, Inc., Consumer Privacy User Profile Litigation 2019).

Facebook's third defense, users consented to the sharing of their information, is derived from the user agreement to the Terms of Service. This connotes that the consumer understood the Facebook declaration that users consented to the dissemination of their sensitive data, as noted in the terms of use user agreement. Facebook may rely on the fact that, in several states, the courts assume users read and agree to the contractual terms (Facebook, Inc., Consumer Privacy User Profile Litigation 2019). However, in 1989, Justice Stevens, Chief Justice Rehnquist, along with White, Marshall, O'Connor,

Scalia, and Kennedy, held “information may be classified as private if it is intended for or restricted to the use of a particular person or group or class of persons,” rather than being “freely available to the public” (DOJ v. Reporters Committee for Freedom of the Press 1989, 15). In Campbell et al. v. Facebook Inc., the court held, in 2014, that Facebook violated ECPA by the “interception” of private messages when it scanned the contents of private messages. Nonetheless, the Ninth Circuit dismissed a privacy suit concerning the collection of medical information because Facebook’s written policy allows for the secret collection of such data (Smith v. Facebook 2017). Lewis (2018, webpage), President / CEO Winning Technologies, Inc. (an IT services company) discovered, while the specific language varied, companies shared the same sentiment in their licensing agreements, commonly referred to as the user agreement, where, in effect, it is now the company’s data:

To the extent necessary to provide the Services to you and others, to protect you and the Services, and to improve products and services, you grant a worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools Your Content on the Services. If you publish Your Content in areas of the Service where it is available broadly online without restrictions, Your Content may appear in demonstrations or materials that promote the Service. Some of the Services are supported by advertising (Lewis 2018, para 6).

The Identity Theft and Assumption Deterrence Act of 1998 criminalizes the use of another person’s means of identification, such as an account number, Social Security

Number, or personally identifying information, with the intent to commit an unlawful activity. The prohibitions in the law range from using false identification, with the intent to defraud, to manufacturing false identification. The 2008 Identity Theft Enforcement and Restitution Act obliges the convicted perpetrator to financially compensate the victim for any damage sustained if caught and successfully prosecuted. This Act enhanced identity theft laws, where the perpetrator received economic gain through the use of an individual's personal information by fraud or deception. In July 2019, the FTC's consumer Financial Protection Bureau announced that Equifax agreed to pay up to \$700 million to settle claims stemming from the 2017 breach, where the consumer reporting agency failed to secure the personal data of nearly 150 million people (Kochman 2019).

### **Law and Characteristics of the Criminal Cases**

The criminal actors are highlighted in eight cases of cyber-enabled financial abuse of older Americans, committed by 26 individuals. All cases, but one, were reported as part of the Department of Justice's public announcement on February 22, 2018, regarding the biggest sweep of elder fraud cases in history, in which 250 defendants received criminal charges (DOJ 2018a). The selected exemplar cases met the criteria of cyber-enabled financial abuse that received adjudication by December 2018. The sources of data come from news reports and court documents obtained through the Public Access to Court Electronic Records, which is an on-line accessible means of obtaining case and docket information on court proceedings. Table 7 shows the binding authority. A discussion of the cases follows.

Table 7. Binding authority

United States Code	Section	Colloquial name	Actus reus (prohibited action)/mens rea (intent)
18 U.S.C.	§ 513	Securities of the States and private entities	Whoever makes, utters or possesses a counterfeited or forged security of a State or organization. Intent to deceive another person, organization
18 U.S.C.	§ 1028	Identity theft and Assumption Deterrence Act of 1998	Whoever knowingly and without authority produces, transfers, possesses identification document, feature, or false identification document, or traffics in false or actual authentication features for use in false identification documents.
18 U.S.C.	§ 1341	Frauds and Swindles	Whoever devises a scheme to defraud to obtain money or property by means of false pretense and in execution uses any post office or authorized carrier anything to be delivered in commission of the offense.
18 U.S.C.	§ 1343	Fraud by wire, radio, or television	Devise any scheme to defraud or obtain money by means of false or fraudulent pretenses by means of wire radio of TV communication in interstate or foreign commerce
18 U.S.C.	§ 1344	Bank Fraud	Knowingly executes or attempts to execute a scheme to defraud or obtain funds by means of false or fraudulent pretense of a financial institution
18 U.S.C.	§ 1349	Conspiracy to Commit Mail or Wire Fraud	Agreement between two or more persons to commit mail fraud or wire fraud and an overt act committed by one of the conspirators
18 U.S.C.	§ 1949	Attempt and Conspiracy	Any person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed with the offense
18 U.S.C.	§ 1956	Laundering of Money instruments	Knowingly involved in a financial transaction that represents the proceeds of some form of unlawful activity, conducts or attempts to conduct the financial transaction.
18 U.S.C.	§ 1957	Engaging in monetary transactions in property derived from specified unlawful activity	Knowingly engaging or attempt to engage in monetary transaction in criminally derived property of value greater than \$10K.

### ***Romance and Dating Website Scam***

John Pierre Mack III, Ronnie Rollard Montgomery, David Augusta Jones III, Dillion McDowell, Amaryllis Pagan, and Ashley Ferrell were charged with Conspiracy to Commit Wire Fraud and 23 counts of wire fraud. The court document states that from around August 2015 until around June 2017 the individuals “conspired together to commit an offense against the United States to knowingly...and intend to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses...in violation of 18 U.S.C §1343 and §1349 (United States v. Mack, Montgomery, Jones, McDowell, Pagan, Ferrell 2017).

The defendants created a fake internet adult dating website. They would develop an on-line relationship with the victims after the victim chose to respond to the posts, reportedly supplied by the female, whose picture was posted. The perpetrators pretended to be Homeland Security agents and entrapped the victims, accusing and ‘charging’ them with soliciting a minor. The defendant sent the charges to the victims with the official seal of the Department of Homeland Security and a judge’s name. The defendants further described themselves as assigned to the “C3 Child Exploitation Division.” Over the internet and telephone, the victims were told they could pay a fine, rather than going to court, since it was a first offense. The victims were guided to use Ria, MoneyGram, and Western Union money services to transfer money. All defendants plead guilty to the charges. The criminals collected almost \$80,000 from 61 extortion payments (Mordock 2018). However, court documents show restitution ranges from \$63,451 to over \$350K, with sentences ranging from six months to 80 months.

***Romance, Inheritance, and Lottery Scams***

Roda Taher, Hanan Jaafar, Geannis Gonzalez, Alfredo Tovar, Quiana Velasco, Jose Daniel Estrella, Pedro Reyes, Jamie Vives Castillo, and Robinson Castillo were indicted on charges of Conspiracy to Commit Money Laundering (U.S. v. Taher, Jaafar, Gonzalez, Tovar, Velasco, Estrella, Reyes, Castillo, Castillo 2017)

The court indictment states that, since 2008, the defendants conspired and confederated to commit offenses against the United States, in violation of Title 18, United States Code, Sections 1344, 1349, 1956, and 1957. There is one count of bank fraud and conspiracy to commit bank fraud, 22 counts of laundering of monetary instruments (money laundering), and 15 counts of committing transactions in criminally derived property.

Roda Taher, who reportedly works from Beirut, Lebanon, leads a global money laundering scheme that criminally scammed more than \$94 million from vulnerable victims, primarily the elderly (U.S. v. Taher et al 2017). He was charged with conspiracy to commit money laundering, conspiracy to commit bank fraud, 21 counts of money laundering, and 18 counts of transactions, in criminally derived property. His wife, Hanan Jaafar, also from Lebanon, received the scam proceeds and transferred the money to overseas bank accounts. She was charged with conspiracy to commit money laundering and conspiracy to commit bank fraud.

Geannis Gonzalez, president of two shell<sup>58</sup> companies: Trades Generation, Inc. and Worldwide Contracts, Inc., recruited and managed money mules<sup>59</sup>. Alfredo Tovar, a money mule and president of shell company ATI Global Tradings, Inc., also recruited and managed money mules. Quiana Velasco, a money mule and president of shell company QMV Atlantic Trade, Inc., recruited and managed money mules. Jose Daniel Estrella, a money mule and president of shell company JE East Products, Inc., recruited and managed money mules. Pedro Reyes, president of shell companies RP Global Sales Inc. and RP Global Sales & Logistics, Inc., recruited money mules. Jamie Vives Castillo, president of shell company JV Atlantic Trades, Inc. recruited and managed money mules. Robinson Castillo, president of shell company Castillo Global Tradings, Inc., recruited and managed money mules.

Taher offered employment to individuals under the guise that they were to conduct wire transfers for his businesses' export or import of goods. Once employed, he would use their personal information to incorporate a shell international import/export company in the employee's name (U.S.A. v. Taher, Jaafar, Gonzalez, Tovar, Velasco, Estrella, Reyes, Castillo, Castillo 2017). Under his direction, the money mule would then open bank accounts in the name of the shell company. The money mules received a 'cut' of the funds wired into the bank accounts. According to the indictment, those bank accounts received wire transfers from fraudulent schemes, ranging from \$3,381,110 to

---

<sup>58</sup> A shell company is a "purported business entity incorporated under state law that does not engage in any substantial legitimate business activity, but is instead used to perpetrate or facilitate money laundering or other criminal offenses (U.S. v. Taher, Jaafar, Gonzalez, Tovar, Velasco, Estrella, Reyes, Castillo, Castillo 2017).

<sup>59</sup> A money mule is "a person that is recruited to incorporate a shell company and open shell bank accounts in that shell company's name for the purpose of receiving, withdrawing, and transferring proceeds of criminal activity" (U.S. v. Taher, Jaafar, Gonzalez, Tovar, Velasco, Estrella, Reyes, Castillo, Castillo 2017). A money mule may also be an unwitting participant in the transfer of funds, believing they are helping a friend overseas.

\$7,177,442 that were further wired to accounts in the U.S., Asia, Europe, and Africa (FBI 2018). The perpetrators took over hacked victim's accounts, or used 'spoofed' email accounts that looked like the victims' accounts, and instructed banks, financial institutions, and corporations to wire money to the shell bank accounts.

The co-conspirators contacted victims on dating, social networking, and other internet sites to initiate romantic relationships (U.S.A. v. Taher, Jaafar, Gonzalez, Tovar, Velasco, Estrella, Reyes, Castillo, Castillo 2017). During the course of the relationship, the criminals persuaded the victims to open bank accounts, deposit checks, and wire money to the shell banks (in essence, making the victims into unwitting money mules). The perpetrators deceptively solicited and persuaded victims to wire money for fraudulent lottery and investment schemes. According to the DOJ (2018b, para 4), "there were over 400 victims...who were scammed out of tens or hundreds of thousands of dollars."

Orlando Rodriguez, a lawyer representing Robinson Castillo, claimed Judge Ungaro was as fair as she could possibly be, given that the ones being punished were not the masterminds (Hale 2018). Estrella's lawyer, Scott Sakin, claimed their defendants were vulnerable, not business savvy, needed the work, and were not responsible for the underlying frauds that acquired the transferred funds (Hale 2018). Gonzalez, Tovar, Velasco, Estrella, Reyes, Castillo, and Castillo all pled guilty to one count of conspiracy to commit money laundering. All receiving prison sentences, ranging from four years to nine years, with restitution ranging from \$1.2 million to \$3.7 million. Taher and his wife, Jaafar, sentences are pending.

### ***Grandparent Scam***

Tiffany Strobl perpetrated a Grandparent scam and was charged with fraud and identity theft for stealing \$5,000 from an 81-year-old Iowa woman by telling her that her grandson needed bail money. The victim later learned her grandson was never arrested and never called to request money. According to the indictment, Strobl opened a bank account under a false name, had the victim wire the money to the bank, and then made cash and debit card withdrawals. She was charged with three counts of bank fraud, one count of wire fraud, one count of using an unauthorized access device, and one count of aggravated identity theft. Strobl was found guilty in 2017 to one count of possession of false identification and one count of bank fraud and was sentenced to two years and ordered to pay \$9,548 in restitution (U.S. v. Strobl 2017a). Court records show Strobl has a history of scamming (U.S. v. Strobl 2017b).

### ***Investment Scam***

According to the Department of Justice, Anthony Sciarra waived his right to be indicted and pled guilty in one count of wire fraud. He portrayed himself to be an independent insurance agent and investment advisor from around 2001 until 2012. During this timeframe, he offered insurance, securities, as well as other financial products to his clients. Instead of investing the money in bonds and other securities, he used the funds for his personal use (U.S. v. Sciarra). He was able to hide the scheme by issuing partial payments to victims from monies that were obtained from other victims. Court documents indicate there were at least 12 victims who invested over one million dollars with him with a loss of over \$874K. Sciarra was sentenced to 46 months in prison (U.S. v. Sciarra 2017).

### ***Romance and Inheritance Scams***

In the indictment against Sally Iriri, the courts state that from October 2013 to March 2015 she and her accomplices, ex-husband Michael Adegoke, Richard Ugbah, and Jon Whipple, defrauded victims by creating fake profiles on internet dating websites and making false representations and promises (Forward 2016). She gained the victims' trust through strong romantic emotions and promising to move to be with the victims (U.S. v. Iriri 2015). She also defrauded victims by convincing them to help her pay an 'inheritance tax' on a non-existent inheritance, assist with personal tragedies, or invest in money-making schemes (Forward 2016; U.S. v. Iriri 2015). The schemes defrauded victims out of more than \$12.9 million, but the judge opined that the amount was likely greater due to the scope and scale of the fraud (Forward 2016). Iriri and accomplices victimized and revictimized the same people (U.S. v. Sally Iriri 2016). Fourteen of the known 21 defendants provided victim impact statements, in which one attempted suicide from the emotional and mental anguish, another lost all their retirement savings, and a third suffers from depression and general anxiety, induced by the scams (U.S. v. Sally Iriri 2016).

Iriri was charged with using a false name and address and devising schemes to obtain money through fraudulent pretenses, by means of wire in interstate (wire fraud) and foreign commerce. She pled guilty and was sentenced to 10 years in federal prison in November 2015, which was a sentencing enhancement, due to the vulnerability of the victims (U.S. v. Sally Iriri 2016). Iriri admitted she purposely targeted the elderly and vulnerable .... simply because of their age and access to money and justified her actions because she gave them what they wanted by listening to them (U.S. v. Sally Iriri 2016).

She lost the appeal of her sentence when the Court of Appeals affirmed the lower Courts sentencing and stated that perpetrators of fraud do not grow out of criminal fraud activity the way violent criminals or drug gang members tend to do. Adding that even in ten years she will be just as capable of fraudulent scheming as when she committed the crimes for which she is sentenced (U.S. v. Sally Iriri 2016). Iriri is a Nigerian citizen and the court acknowledged that she will most likely be deported once she leaves prison, but that her skills are honed enough that she has the ability to use these skills against Americans from Nigeria.

Richard Ugbah and Michael Adegoke, both Nigerian citizens, were sentenced to 12 years in federal prison. Ugbah was charged with wire fraud and required to forfeit two bank accounts and his Mercedes Benz (Superior Telegram 2017). Adegoke was charged with, and pleaded guilty to, conspiracy to commit wire fraud, but later challenged the sentence because of ineffective counsel (U.S v. Adegoke 2019). In his appeal, Adegoke's premise is that his lawyer should have objected to the amount of victim loss as they incurred, before he joined his ex-wife's schemes. He contends that he is not responsible for approximately \$600,000 of victim losses, as they were not "reasonably foreseeable," which he believes would have given him different sentencing guidelines (U.S. v. Adegoke 2019). The court disagreed.

Jon Whipple was a victim at first, but assisted in the fraudulent schemes by disseminating counterfeit checks. He pleaded guilty on February 16, 2017 to uttering a counterfeit security and received five years' probation.

### ***Internal Revenue Service (IRS) Impersonation Scam***

Moin Gohil, Nakul Chetiwal, Pratik Patel, and Parvez Jiwani were charged with wire fraud, conspiracy to commit wire fraud, and aiding and abetting crimes (U.S. v. Gohil, Chetiwal, Patel, Jiwani 2017). The four criminals perpetrated a 3.5M wire fraud, pretending to be tax officials and collecting money by threatening over 7,300 people. Court records show the runners, Gohil, Chetiwal, and Jiwani, would use fraudulent identification cards to pick up the money, while Patel aided and abetted. The scheme, which likely originated from India, consisted of the criminals calling victims and telling them to pay taxes via wire transfer, gift cards with cash value, Western Union, or MoneyGram. The false identification cards were linked to 6,530 other fraudulent transactions, with an estimated value of \$2.8 million (U.S. v Gohil et al 2018). Between January 2016 and August 2017, 784 victims sent \$666,537, as the defendants “preyed on vulnerable victims and caused significant losses, in addition to emotional consequences.” (U.S. v. Gohil et al 2018, 4. Defendants were sentenced to serve time and ordered to pay restitution.

### ***Romance, Advance Fee, Counterfeit Checks, Computer Hacking, Email Spoofing, and Check Forgery***

According to Court records, Luis Pujols, Gary Camilo, Jean-Philippe Etienne, Karina Ocasio, Randy Santos, and Cosme Vasquez enriched themselves through money laundering. Shell companies Camilo International Trading, Cosme Global Trades, Jean Champions Trade, Luis Global Investments, Ocasio Trades, Santos Global Sales, Barcelo Max Trades, DB Wholesale Prices, J Smart Connections, JG Plant Trades, JR True Connections, JR Vast Enterprises, and United Wire Metal were all Florida-based

corporations. From March 2013 until September 2014, the defendants conspired to commit money laundering and bank and wire fraud offenses against the United States (U.S. v. Pujols, Camilo, Etienne, Ocasio, Santos, Vasquez 2017).

The defendants perpetrated several scams from romance to investments (U.S. v. Pujols, Camilo, Etienne, Ocasio, Santos, Vasquez 2017). They posed as interested partners on-line to establish a romantic relationship and then would persuade the victim to send money, via wire-transfer, to one of the shell companies. They persuaded victims to pay fees and costs for taxes due on fake inheritance schemes and lottery winnings. Victims were conned into depositing checks into their own accounts and then forwarding the funds to a shell company's account before the check would be returned due to insufficient funds. According to the indictment, the fraudsters hacked into some victims' computers to install software that generated payments to one of the shell company accounts. The software also generated a forged email address to divert payments to a shell company's account. Funds sent overseas included Spain, People's Republic of China, and Singapore. Pujois was convicted of money laundering and conspiracy to commit mail fraud. He was sentenced to 121 months in prison and ordered to pay \$1.5M in restitution. Camilo pled guilty, was sentenced to 87 months in prison, and ordered to pay \$1.4M. Etienne and Ocasio were also convicted, sentenced to 40 months and 30 months, respectively, and must make restitution of \$735K and \$716K. Santos pled guilty and was sentenced to five years and to make restitution of \$600K. Vasquez also pled guilty, was sentenced to 57 months, and ordered to pay \$1.7M in restitution.

### ***Investment Fraud***

Robert Leslie Stencil, Michael Allen Duke, Daniel Broyles, Ludmila Stencil, Martin Lewis, Nicholas Fleming, Paula Saccomanno, and Denis Swerdlen were indicted for a \$2.5 million investment scam. Beginning in 2012, Robert Stencil owned, marketed, and operated a company, Niyato (U.S. v. Stencil, Broyles, Sierp, Lewis, Fleming, Duke, Saccomanno, Swerdlen, and Dearboran 2017). According to the indictment, Stencil told investors he had patented a natural gas technology and offered stock subscriptions for the initial public offering (IPO). Stencil claimed to have manufactured and sold 2,700 electric vehicles, using his patented technology, with hundreds in production in his own facility (U.S. v. Stencil 2017). It was revealed during the trial that between 2012 and 2016, Stencil and his co-conspirators sold millions of dollars of worthless stock, often to the elderly. Through high pressure, short time opportunity offerings of the limited pre-IPO stock options sales calls, approximately 140 victims were sold around \$2.8 million in stock. There was no patent, or any other product, and no stock options for an IPO. The co-conspirators knew the stock was worthless.

Kristian Sierp pleaded guilty to participating in two cases of scams. He admitted to working for Stencil and in a Costa Rican call center where he made telephone calls to the U.S. residents, masking the origin using voice over internet protocol (VOIP) to display a 202-area code (U.S. v. Nastasi, Fairchild, Mommers, Sierp, Fernandez, Finck, Sniffen, Harmelin, Woods, Del-Hoyo, Saxon, Jordan, and Dodt 2019). Sierp confessed to creating high-pressure sales to Niyato's victims. For both cases, he was sentenced to 102 months and must make \$11M in restitution. Michael Duke was the top salesperson, selling around \$1.4 million of useless stock to at least 70 victims. Both Stencil and Duke

were found guilty of conspiracy to commit mail and wire fraud, mail fraud, wire fraud, and money laundering. Martin Lewis pleaded guilty and was sentenced to three years of probation and \$1.6M in restitution. Nicholas Fleming pleaded guilty, was sentenced to five months in prison, and must make restitution of \$1.3M. Paula Saccomanno pleaded guilty, was sentenced to five months in prison, and must make \$1.9M in restitution. Dennis Swerdlen pleaded guilty, was sentenced to three years of probation, and \$1.9M in restitution. All charges were dropped against Scott Dearborn and Ludmila Stencil was found not guilty of all charges. Daniel Thomas Broyles remains a fugitive.

## **Discussion**

### **Overview of the Study**

As the Internet Crime Complaint Center (IC3) reports and subsequent research indicate, all citizens are vulnerable to scams; however, older citizens may be particularly vulnerable to being targeted, as criminals may consider them to be gullible or suffering from cognitive decline. While an individual's cognitive capacity may, or may not, play a role, the victim is never responsible for the criminal's behavior. Any misperception of contributory negligence is unfounded in these situations, since the victim is rarely attempting to participate in any illegal endeavors. The disconnect between what happens during scams and the public narrative inhibits the delivery of actual help to older Americans.

This research set out to examine the social, economic, and policy characteristics of cyber-enabled financial abuse to advance the field of public administrations' body of knowledge and to influence policies on cybercrime and older citizens. Understanding the complexities of cybercrime and older citizens' abuse are two of the most two challenging public policies areas. For any consequential policy change to occur, one must first diagnosis the problem and compare it to the existing public policy (Gaus 1947).

The streams of research into the perpetrator, victim, and laws surrounding the internet come together for a contribution to the field of public administration. While this research used a mixed-methods approach, the quantitative data was used to support the

qualitative data. This study supplements the little qualitative data that existed to help understand the process of cyber-enabled financial abuse of older Americans, where criminals convince an individual to participate in his or her own victimization. This chapter contributes to both the theory and method, as well as providing a number of recommendations for future research.

This final chapter compiles the information listed in the first four chapters. It also considers the mechanisms and analyzes the findings from the fourth chapter, in order to answer the research questions. First, the results are analyzed by restating the research questions and presenting the background of the data, in order to address the initial research question: How are cyber scammers so successful against older Americans? With the examination of qualitative and quantitative data, the proposed processing tracing outcome explaining model can be solidified and represented graphically in figure 2.

From this, it is possible to make some conclusions regarding the relationship among these process-tracing mechanisms and address the question: What are the grooming mechanisms leading to victimization? All of the entities (assets, cognitive capability, needs/wants/fears, means of communication, and persuasion/manipulation) are necessary, yet none alone is sufficient for victimization. Criminals perform research by readily collecting data, or they purchase it for pennies on the dollar and establish trusted affinity relationships. Unknown to the average American citizen, significant information is available to criminals who capably target their victims. This data includes demographic data, such as age, height, weight, and marital status, to lesser known information, such as political affiliation, sexual orientation, financial capacity, food allergies, airline seat preferences, investment inclinations, and purchasing predispositions. Algorithms are

written to understand the individual's tendencies and social media software programs are written to be both addicting and to influence decision making. Applying the conceptual framework helps address the question: What are individual's perspectives of victimization?

### **Conceptual Framework**

The Conceptual Framework, depicted in figure 1, is a model of how seniors are protected, or not. In the individual victim interviews, the victims, family members, social workers, and friends who shared their experiences allowed the researcher to gain insight into the intensity of the crimes from their perspective.

All of the interviews were conducted with known cases of cyber-enabled financial abuse, where family, law enforcement, or other authorities were notified. In some cases, the local police had active fraud departments, like Montgomery County, MD, and were able to provide some victim assistance. In one case, the fraud department was able to get about a third of the money that was lost, returned to the individual. In another case, a family member called the local FBI branch, only to be told there was nothing that could be done, as the FBI received "20,000 calls per month" and had no means to assist. None of the family members, nor the victims, in any of these cases, knew, or was told, to report the crime to the IC3, including the family that called the FBI.

The sentiments conveyed most often by the victims were shame or embarrassment at their complicity in their own victimization and the humiliation of not knowing they were being scammed. Three of the victims wanted to know if they deserved this because they "were stupid?" Two of the victims, who are female, expressed fear of the criminal knowing so much about them and the possibility the criminal may do something to

physically harm them. Four of the victims indicated severe anxiety and worried about being able to meet present and future financial obligations. Two of the interviewees indicated the scammers threatened to reveal publicly very personal information they had obtained somewhere - not from the victim. Initially, the threat of humiliation prevented the victims from obtaining help. One of the victims, while she is in the process of receiving counseling, had attempted suicide.

### **Friends, Family, and Services as Capable Guardians**

Family members also expressed embarrassment, but for different reasons. They were often embarrassed and angry at the victim for being so gullible, but also at themselves for not having a strong enough relationship with the victim, to help the victim identify the danger and either prevent or curtail the scam. In one case, the family did try to intervene, but the relationship between the victim and the scammer was so solidified that the family failed to convince the victim of, in this case, marital scam. In fact, the individual accused the family of not wanting him to be happy and accused the family of mistakenly interpreting his newfound happiness as disloyalty to their mother. At no time did this individual acknowledge he had been scammed. He wanted his new wife he had married over the telephone to come to the United States. He persisted until overwhelming evidence proved he was not married, and then he refused to discuss it further. In several cases, the scams have caused significant financial burden on family members. In two cases, the family members indicated the victim lost their home, one through bankruptcy and the other through financial distress. Too often, once the victims are so emotionally invested in the relationship, they deny to everyone, including themselves, the truth about the problem.

In the sole case where the individual was not a victim (J1), her neighbor was her capable guardian, in the form of sage advice. According to the non-victim, she would have given the scammer the money, as he sounded so professional, kind, and helpful. The scammer sounded as though he worked with the internet provider. Her neighbor, readily aware of the scam, saved not only her money, but her sense of well-being.

In another case (P1), her daughter was the one who initially told her the romance was a scam. While she admitted she did not want to believe it, she gradually came to understand that it was a scam. She revealed to the researcher that she never fully disclosed to her family the gravity of the financial loss, out of embarrassment. Her daughter acted as a capable guardian and saved her from further financial, emotional, and social pain.

Other situations, where the family tried to warn the victim (G1 and A2), the depth of the criminal's relationship with the victim was greater than the family ties. The financial impact to both families was extensive, as was the damage to the relationship between the victim and the family members. In both cases, the capable guardians were family members, who attempted to unsuccessfully save the victim.

Investment companies and banks have tried to intervene as capable guardians (C1, D1, O1), with mixed results. Like G1 and A2, the depth of the criminal's relationship with O1 was greater than the ties with the financial institution or the Adult Protective Services (APS), who tried to intervene.

In one case, C1, the victim threatened to withdrawal all funds from the investment company, if the institution interfered in her personal decisions again. According to APS, she had a significant financial portfolio. The financial investment company removed

themselves from making any more forays into her personal financial business, as did APS, since she did not display any negative cognitive issues. Situations like this often place companies, and other capable guardians, in an awkward position.

### **Laws as Capable Guardian**

Criminals are rational, economic actors, as they will always maximize their own utility where the benefits gained from the crime outweigh the probability of being caught, if caught, convicted, and if convicted, the severity of the punishment (Becker 1968). Capable guardians, such as neighbors, Adult Protective Service social workers, fraud police, family, friends, financial awareness, and laws help protect the potential victim from the motivated criminal. Hundreds of years of law-making show that laws do not necessarily make criminals law abiding; however, economic analysis shows that profitability is important and the lack of profitability drives behavior (Becker 1968). Right now, scamming is a low risk opportunity to make money. Risk is a function of vulnerability, threat, and consequences. The existing vulnerability to discovery for the criminal is low, the threat of discovery is low, and the consequences, if caught, are low compared to the chances of being caught. Financial fraud/abuse is a white-collar crime and the punishment for a white-collar, non-proximate crime is minimal compared to the monetary and emotional devastation experienced by the victim. Typical sentencing guidelines for white collar crimes are significantly less than those of violent crimes.

Unfortunately, as demonstrated in the court results, listed in chapter four, courts have difficulty calculating the optimal punishment for cybercrime. The murderer or rapist's physical detention, arguably, contributes to a safer society, whereas, from a pure economic perspective, society may, or may not, be better, or worse, off from the

cybercriminal's release. Economic efficiency is a social concern and not just a victim's justice issue. In other words, the courts weigh the proximity of the crime (no physical threat) and the cost of housing a criminal, over a period of time, against the criminal's potential of producing financial benefit for themselves, society, or the victim. This does not, however, deal with the devastating blow to the individual, older American victim and their right to the pursuit of a self-defined financial well-being.

Akhlaque Haque (2015) claimed that technology is shaping social and political order. The speed of that technology shaping the order, makes John Gaus' 1947 warning, in *Reflections on Public Administration*, that society's inability to fix human-created artifacts could lead to a citizen-collective financial catastrophe, a public administration obligation to address. In which case: What policies, laws, or other mechanisms are needed to help protect against the grooming process that result in victimization?

While the victim is the first line of their own defense, the internet is a different environment in which to experience socialization. Humans are social animals and the trust built between humans has helped society to flourish. Inventions from fire to space launches have changed how people live, work, organize, and socialize. Information communications technology has had the greatest leap in the last three decades and this exponential leap has helped fuel both social advancements, as well as crime. Today, the hand-held smart phone has more technology than that which launched John Glenn into orbit around the Earth. Information hurls around the world at the speed of light (186,000 miles per second or 71/2 times around the Earth, per second), thanks to fiber optics. With this, comes the ability to socialize on a global scale, as well as spread both false and real information and criminal behavior.

The internet is a myriad physical connection of interconnected network of publicly and privately-owned networks. Nicholas Negroponte (1995) argued that the Internet cannot be regulated and Grateful Dead lyricist, John Perry Barlow's (1996) "Declaration of the Independence of Cyberspace" is a manifesto for cyberspace, without sovereignty, where cyberspace "is an act of nature and it grows itself through our collective actions." There are arguments that the internet empowers individual rights, as a constituent with the power and the means to be heard. While this may conjure up thoughts of the wild, untamed West, the internet is owned and governed, in many ways, by private industry. Cyberspace may seem an intangible, inanimate object, however, the governments and corporations that own and operate the internet are tangible. There is a legitimate role of government, as it pertains to the safety and security of the individual citizen, and there are, or should be, social and legal responsibilities for those who profit from the using and owning the internet. It is through laws and regulations that sovereign governments rein in those with outstripped power over the masses. Yet, the U.S. government struggles in its ability to take action with the threat, as the jurisdiction covering cyber, security, and the elderly spans over 80 groups (Corrigan 2019; McDaniel 2019).

Google, Yahoo, Equifax, Cambridge Analytica, and other big data brokers help manage the lives of millions of people. As pointed out by Goodman (2015), data brokers use algorithms to determine who has wealth, who is malleable, who should be allowed to borrow money, and their predilections. Information on every American, whether large or minute, is collected, analyzed, and available for sale.

The push away from paper documentation toward digital records drives the collection and storage of information on all citizens. In many ways, this makes the internet a public utility. The requirement to provide personal information to borrow money, purchase health insurance, use a credit card, or apply for a job, imputes a level of trust with institutions that have failed to maintain the privacy and confidentiality of the information. Privacy is different from confidentiality. Privacy affects the right of the individual to control, or disclose, personal information and confidentiality is how the individual's data is collected, stored, and used by the organization (Westin 1976). The myriad of federal laws regulates how the federal government will collect, store, use, or disclose personal information. There are very few laws governing the use of individual information, in as much as individuals have ostensibly given permission via Terms of Service agreements. Even entities that collect data without the individual's permission decide the ability of that individual to qualify for loans or jobs, such as Credit Reporting Agencies, which are not accredited by a governing body. There is little change from the Federal Trade Commission, in 2014, recommendation that data brokers have greater regulation and oversight when it comes to data handling.

Internet Service Providers (ISP) have used the protection afforded by the Communications Decency Act (CDA) to shield themselves from lawsuits on several fronts. The first, is a safe harbor from online defamation judgments, because the First Amendment grants freedom of speech. The second, is the immunity from content of an email sent to the victim. This includes advertisements using false trademarks and patents. These weaken the capacity of the citizen to trust in the electronic version of the mail.

Algorithms are capable of recognizing the difference between a real and a fake company seal, as well as a false email address, to redirect an individual to a fake website.

Not a single criminal was charged with violation of communication, privacy, video, or transmission of unsolicited commercial email. They were charged and convicted under criminal codes having to do with securities violations, identity theft, fraud, wire fraud, bank fraud, conspiracy, money laundering, and engaging in unlawful monetary transactions. The suicide attempts by one of the interviewees and the indicated attempt by one of the victims in the adjudicated law cases, shows the depth of desperation for these victims. Yet, there is little to no means these criminals will pay the restitution owed the victims, either because they spent the money or forwarded the money onto their handlers in the U.S. or foreign countries. Two of the known perpetrators have yet to be found guilty, due to the lack of jurisdiction in a foreign country.

Support for international laws is critical. The Council of Europe's Convention on Cybercrime of 2001 has support from the United States, Canada, Australia, and Japan, as well as the United Nations, as part of the Human Rights concerns. The Budapest Convention addresses internet-related crimes and sets up mechanisms for cooperation, like the bilateral agreement that resulted in the extradition of the perpetrators, exhibited during Brennan's cyber hack. Cyber is a man-made phenomenon and, despite the Negroponte or Barlow' proclamations, sovereignty has a role in providing rules that allow for the safe environment for its citizenry.

## **Recommendations for Future Research; Recommendations and Implications for Public Administration**

### **Recommendations for Future Research**

Banerjee's (2011) study indicates that financial education may act as a capable guardian. Those states with a higher financial literacy, also had fewer percentage of complaints per capita. The study did not specify age of the survey, in 2011, but determining how financial education acts as a capable guardian is an area for further research.

The following are specific recommendations:

- The internet is a pseudo public utility and, as such, antitrust laws are needed, in order to help modify behaviors, with regard to confidentiality and privacy.
- Regulation is necessary for those that collect, store, transport, broker, and sell data. They need to obtain explicit permission from the creator of the data, the individual. Request for information must be written, in plain, eighth grade level, everyday language. The request must state why the information is needed, how it will be used, stored, and transmitted. It may only be sold with explicit permission and the individual may request all data be removed. Violations must be harsh enough to make the risk calculus weigh in favor of the potential victim.
- Limits to the CDA Section 230 are needed. In other words, hold ISPs accountable for the content of the email, by empowering the ISP. The ISP's terms of service agreements may establish that they have the right and ability to control their customers' posts. Real email addresses, belonging to corporations, are not unlike trademarks and need to be treated as such. Spoofed email addresses of banks and

other organizations should be considered a trademark violation. The ability to watermark real addresses allows ISPs to control this aspect of their business.

### **The Enigmatic Impact: Implications for Public Administration**

Readily accessible money, loneliness, a need to be needed and loved, a trusting nature, a desire to help another person, a longing for continued significance, all potentially contribute to seniors becoming victims. In a *Life* magazine article, Greta Garbo clarified what she meant when she told the media she wanted to be left alone, “I never said ‘I want to be alone,’ I only said, ‘I want to be let alone’” (Bainbridge 1955, para 1), which embodies the sentiments expressed by the seniors interviewed. Several victims declared they do not want to be alone, but also do not want to be managed by others, who, despite their good intentions, diminish the senior’s sense of independence. As evidenced by comments from celebrities like Garbo, intense scrutiny from others can be emotionally overwhelming or stifling. Seniors want to be independent, full participants in society, not managed or judged. The fear of judgment or ridicule at being ‘duped’ in the scam, as though it was due to feebleness or gullibility was a strong consideration for the victims not confiding in others. The melancholy during the victim interviews was palpable in terms of sadness and acknowledged soul-searching, as if their self-perceived gullibility meant they deserved to be victims.

An important role for public administration is helping solve problems, by giving political and economic voice to vulnerable citizens. The consequence for not addressing the citizenry’s cybersecurity needs, may lead to a continued senior citizen financial victimization, as well as a loss of confidence in society and the government (Frederickson 2008; Gaus 1947). Many victims have no reasonable means of redress for cybercrime.

The threat from unscrupulous individuals has always existed and this will not change; however, to change the criminals' decision-making calculus requires the victims' vulnerability to be lessened, while simultaneously enhancing the consequences. While the 2018 and 2019 DOJ recent arrests of crimes committed against the elderly are admirable, these are a small dent in the devastating financial loss experienced by the seniors, which has grown 16 percent in the last six years. The significant increase in financial loss is indicative of criminals' success and demonstrates the urgency for action.

## Appendices

## **Appendix A**

### **Consent Form**

#### **CONSENT FORM FOR PARTICIPATION IN RESEARCH ACTIVITIES**

##### **I. INTRODUCTION/PURPOSE:**

I am being asked to participate in a research study. The purpose of this study is to understand cyber enabled financial abuse methods against older citizens. I am being asked to volunteer because (either myself or family member was a victim). My involvement in this study will begin when I agree to participate and will continue until 31 January 2019. At least 12 persons will be invited to participate.

Every year cyber criminals defraud Americans, in fact the Internet Crime Complaint Center received more than 300,000 complaints for a loss of more than \$1.4 billion dollars in 2017. While all citizens are potential victims, Internet criminals target people over 60 years of age. The purpose of this research is to better understand the criminals' behavior.

##### **II. PROCEDURES:**

As a participant in this study, I will be asked to participate in an interview. I will be asked to participate by phone or if necessary, in person. My participation in this study will last for 30 minutes and notes will be taken. No personal identifying information will be written with responses to the questions.

##### **III. RISKS AND BENEFITS:**

My participation in this study does not involve any significant risks and I have been informed that my participation in this research will not benefit me personally, but will benefit others, the community or society. I further understand that I may feel uncomfortable answering some questions and therefore may elect not to answer. I also understand I may stop the interview at any time and request my information not be included in the study.

##### **IV. CONFIDENTIALITY:**

Any information learned and collected from this study in which I might be identified will remain confidential and will be disclosed ONLY if I give permission. All information collected in this study will be stored in a locked file cabinet in a locked room. Only the investigator and members of the research team will have access to these records. If information learned from this study is published, I will not be identified by name. By signing this form, however, I allow the research study investigator to make my records available to the University of Baltimore Institutional Review Board (IRB) and regulatory agencies as required to do so by law.

Consenting to participate in this research also indicates my agreement that all information collected from me individually may be used by current and future researchers in such a fashion that my personal identity will be protected. Such use will include sharing anonymous information with other researchers for checking the accuracy of study findings and for future approved research that has the potential for improving human knowledge.

Although your confidentiality in this study is protected, confidentiality may not be absolute or perfect. There are some circumstances where research staff might be required by law to share information I have provided. For example, if an interviewer has reason to believe an elderly person is being abused (or has been abused), the interviewer is required by Maryland state law to file a report with the appropriate agencies. Similarly, if I report that I have been abused in the past, the interviewer may also have to file a report. In addition, if I am threatening serious harm to myself or another person, it may be necessary for the interviewer to warn an intended victim, notify the police or take the steps to seek hospital-based treatment.

This research study is for a doctoral dissertation.

**V. COMPENSATION/COSTS:**

My participation in this study will involve no cost to me.

**VI. CONTACTS AND QUESTIONS:**

The principal investigator(s), Christine Weston-Lyons, Heather Wyatt-Nichol, has offered to and has answered any and all questions regarding my participation in this research study. If I have any further questions, I can contact:

Christine Weston-Lyons 301-332-4091  
Heather Wyatt-Nichol 410-837-6173

For questions about rights as a participant in this research study, contact the UB IRB Coordinator: 410-837-6199, [irb@ubalt.edu](mailto:irb@ubalt.edu)

**VII. VOLUNTARY PARTICIPATION**

I have been informed that my participation in this research study is voluntary and that I am free to withdraw or discontinue participation at any time.

*I will be given a copy of this consent form to keep.*

**VIII. SIGNATURE FOR CONSENT**

The above-named investigator has answered my questions and I agree to be a research participant in this study. By signing this consent form, I am acknowledging that I am at least 18 years of age.

Participant's Name: \_\_\_\_\_ Date: \_\_\_\_\_

Participant's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Investigator's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

## **Appendix B**

### **Survey Summary**

#### **Research involving Cyber-enabled Financial Abuse:**

Every year cyber criminals defraud Americans, in fact the Internet Crime Complaint Center received more than 300,000 complaints for a loss of more than \$1.4 billion dollars in 2017. While all citizens are potential victims, Internet criminals target people over 60 years of age. The types of crime reported by victims are wide ranging and include product non-payment and non-delivery, personal data breaches, computer technical support fraud, mortgage fraud, and phishing/vishing/smishing/pharming scams and investment scams. The purpose of this research is to better understand the criminals' behavior.

Information regarding demographic will be collected, but kept separate from the questions regarding cyber-enabled financial abuse. For secondary victims or persons responding to the questions who worked with or were related to the victim, the questions will be focused on the victim's demographics and experiences.

#### **1) Demographics**

- a. What is your age?
  - i. Under 50
  - ii. 50-60
  - iii. 60-64
  - iv. 65-69
  - v. 70-84
  - vi. Over
- b. Ethnicity, check all that apply
  - i. White
  - ii. Hispanic or Latino
  - iii. Black or African American
  - iv. Native American or American Indian
  - v. Asian/Pacific Islander
  - vi. Other
- c. Education
  - i. No schooling completed
  - ii. 8<sup>th</sup> grade
  - iii. Some high school, no diploma
  - iv. High school graduate or equivalent diploma
  - v. Some college credit
  - vi. Associate degree
  - vii. Bachelor's degree
  - viii. Master's degree
  - ix. Professional degree

- x. Doctorate degree
  - d. Household Composition
    - i. Single, never married
    - ii. Married or domestic partnership
    - iii. Widowed
    - iv. Divorced
    - v. Separated
  - e. Living Relationship
    - i. Live alone
    - ii. Live in group home, non-domestic partner/spouse
    - iii. Live with family, non-domestic partner/spouse
    - iv. Live with spouse or domestic partner
  - f. Professional or Employment Status
    - i. Currently employed
    - ii. Out of work and looking for work
    - iii. Out of work and not looking for work
    - iv. Retired
- 

**2) Questions related to Internet and Computer use**

- a. Do you own a computer?
- b. Are you online?
- c. How often do you go online?
- d. What electronic devices do you use?
- e. How often do you go on the Internet?
- f. How do you communicate?
  - i. Chat rooms
  - ii. Email
  - iii. Instant messaging
  - iv. Other
- g. What types of social groups do you participate in?
  - i. Facebook
  - ii. Twitter
  - iii. Other
- h. Where do you get your news?
- i. Do you ever request assistance for household/financial/errands/pet care on-line?
- j. Do you use your computer or email for Social Security/medical/banking?
- k. Do you get health advice or medical services on-line?

**3) Questions related to cyber-enabled financial abuse. The intent is to find out the criminal's actions.**

- a. Looking back how did the person online?
- b. Were you asked to provide money or help them in some way?

- i. How long did the relationship continue before they asked for money?
- c. Have you ever purchased a product on-line you never received?
  - i. Can you tell me about the attempt to get the product?
- d. Have you had a friendship with someone where they eventually asked for money?
  - i. If so, did you ever meet the person?
  - ii. Did they ask for money to come see you?
  - iii. Can you tell me about the relationship?
- e. Did you make a charitable donation that you feel may not have been used for the intended use?
  - i. Can you tell me about how you were contacted for the donation and when you discovered the money would not be applied to the cause you intended?
- f. Have you made a financial investment to discover the money was not invested?
  - i. Can you tell me about how you were contacted and when you discovered the money was not invested?

**4) Questions related to financial loss**

- a. What was said or sent by the other individual (criminal) that made you feel comfortable enough to send money ((or provide assistance)?
  - i. What were the issues, affinity, or products interested you?
  - ii. How did they contact you? How did they know to contact you?
  - iii. Did the individual continue to contact you? If so, what were the means by which they contacted you?
  - iv. How often did they contact you?
  - v. When was the last time you were in communication?
- b. What did you think when you realized what happened?
  - i. What was your reaction when you realized what happened?
- c. What has been the hardest part of the incident for you?
- d. What do you think needs to happen to make things right?
- e. Is there anything else about the criminal you can share that may shed light on their behavior or means of doing business?

**5) How familiar are you with cybercrime and communications law?**

- a. Did you report it to APS, IC3, FBI, FTC or another agency?
  - i. If not, why not?
  - ii. If so, did they help?

**6) What types of personal information on you do you think is available legally on the Internet?**

Name  
Address

Age  
Phone  
Social Security Number  
Income  
Marital Status  
Family members/relatives  
Favorite television programs  
Favorite internet sites  
Credit rating  
Home value  
Education level  
Employment status  
Political affiliation  
Criminal History  
Tax history  
Books read  
Photograph

- 1) On a scale of 1 to 5 how vulnerable to cyber-enabled financial abuse are people over 60 and why?**
- 2) Do you still work or volunteer your time? On a scale of 1-5 how does no longer participating in the workforce contribute to the likelihood of victimization?**
- 3) Based on your experience, what is the likelihood of an older victim losing their entire financial savings and requiring public assistance?**

## **Appendix C**

### **Survey Results**

This appendix contains the survey results used to assess the opinions, attitudes, and knowledge of cyber-enabled elder abuse across a wide age spectrum of adult residents of Florida, Maryland, and Virginia over 18 years of age.

1. Many older Americans are less tech savvy and many not be aware of these scams, or don't have the resources to research claims on the internet to determine if callers or emailer could be legitimate or not. They may get conned by fake charity calls and such because they might have had experience with a particular charity, or the disease that the caller claims to be researching. If the scammer poses as an authority figure, they might be afraid of getting into trouble if they don't comply with the fake request in the email.
2. They are highly vulnerable because they are the least knowledgeable about cyber. They are also probably targeted more often.
3. Lack of awareness of how info might be used and non-sophistication about hi-tech capabilities to misuse their info.
4. Many over 60 are not as familiar with new technologies and are easily fooled by what appears to be legitimate requests for personal data.
- 5 Everyone is vulnerable. The opportunities for fraud are abundant.
6. Less experienced with cyber activities, thus more likely to believe fraudulent requests for information.
7. At times there is a lack of awareness of the types of cyber-enabled financial abuse schemes being conducted.
8. Most people age 60 have an OK appreciation of the internet; but some are still "living the 20<sup>th</sup> Century" and are not savvy that their pockets can get picked via the internet faster than in real life. A vast majority of people are too trusting and figure if it's on the internet – it is OK. Has to be – the internet police are watching it – right??? Most people do not look at the URL to see if it is 1secure and 2 a link to the real Wells Fargo or Bank of America or something that sort of looks like it but is really shady.
9. Eagerness to receive resolution of problems may lead 60+ yr. olds to trust without verification first.
10. Because they are less computer/internet savvy, they would be more susceptible to opening emails and clicking URLs that would enable malicious content to be downloaded to their computers. They probably tend to be more trusting, too.

11. My parents are targeted almost daily, and it is hard to fight off every attempt. Occasionally they are tricked into it. It is the scale of the attack that is so disturbing. They are pretty smart, well educated people with PhDs. And they do occasionally fall for a scam.

12. Older people may not really understand the current technology and would likely believe a story told by the scammers. I stopped my mom who was about to buy “special” gold and silver coins off of an ad in the back of NY Times.

13. Too much information on the internet. They follow elderly and what they do, what they like and prey upon them.

14. This is a generalization, but the elderly just aren't as savvy with and read into cyber issues. I think many just don't understand the availability of their data on the Internet, the ways that criminals can defraud them, and what to do if it happens. In what may be contributing factors, I think elderly with declining mental facilities are more likely to get defrauded, and I \ve heard anecdotes of people who have been defrauded not telling anyone about it because they are too embarrassed.

15. They do not know how to protect themselves over the internet. They did not grow up from childhood with particular mindsets – digital.

16. They do not understand how easy it is to give out information to someone, who is trying to gain info illegally, by answering a few innocuous questions. They also don't fully understand phishing attempts by people who claim to be from your bank, utility, or government agency.

17. They are probably aware of the risks, but not actively taking measures to mitigate them.

18. This statement may apply to people regardless of age; if we don't understand how much people can find out, then we don't understand how easy it is to trick us.

19. No comment

20. Both questions 1 and 2 are very vague. If you pay for an online search service or have a private investigator do contract work you can find out a lot of information on someone legally (through public records, public notices, home sales, etc.). To me, everything in question 1 is legal except for financial records and criminal history which are protected by various laws and regulations. Again, if you're the right person with the right connections and a need to know you can get just about anything legally online. For question 2, I think it just comes down to how involved someone 60 or older is involved with their financials. Anyone at any age can be scammed. Or taken advantage of if they don't have power of attorney to conduct their own financial affairs. The age doesn't really matter in my opinion. One thig to note too is that someone at age 60 or older was born in 1959 so they are used to the methods and means of conducting financial transactions from about 1975 onward (this includes physical deposits of cash, checks, bonds, and hard investment information form newspapers and shareholder meeting

information). Questions 4 and 5 are also really vague. What does participating in the workforce have to do with being a victim of cyber-enabled financial crimes? The two seem unrelated if only for the fact that being in the workplace keeps your brain active and probably forces you to manage your income and expenditures more closely. For question 5, if you're talking about as a result of cyber-enabled financial abuse, I'm not sure there's really a way to guess this. Making broad statements about an entire generation of people, or of a certain age group, doesn't really seem to get at the heart of the problem. Some older Americans are very financially savvy while others are not...and this is for many reasons such as what their previous profession was, level of education, experiences growing up with family, potential loss or gain of substantial wealth before they hit 60, loss of retirement or pension plan, etc.

Example: My grandfather passed away at 94 in Dec. 2016, but still had a really good sense of his financials up until the last day. He never used a computer which meant he wasn't connected to the internet and almost never used a cellphone. A close family member who was highly educated and had a long, established career as a corporate attorney made sure that he couldn't be taken advantage of in his old age. (But it took constant work)> When family members help other older family members the results are much better in my opinion. Hope this helps! Interesting topic you're trying to solve.

21. No comment

22 Like any age bracket, it's going to depend how cyber savvy they are. If you have someone who has kept up and knows risks, they won't be as vulnerable.

23. People who are 60 should be well aware of the threats and risks. People who are 80 or above I would count as highly at vulnerable.

24. I think they are no more or less vulnerable than the rest of the population. They may be targeted more and have more money, but people over 60 are just as capable now as people under 30 (or more so), they just have more to lose.

25. They are more trusting and not necessarily on technology issues.

26. Nearing retirement and perhaps concerned if they are prepared. Perhaps make uneducated decisions based on worry. Also, not as tuned in to all the ways they are making themselves vulnerable online.

27. Lack of awareness that their information is readily accessible.

28. People aged 60 and over are far less familiar with the internet and less likely to detect nefarious activity on the internet.

29. They didn't grow up with the technology and most likely to not have all the information or knowledge to defend against cyber hacks or scams.

30. I believe they are easier to victimize due to their age, possible lack of knowledge of technology, and easier to [persuade that someone they know needs the money when in reality it isn't someone they know.

31. Many Americans 60+ did not grow up using computer technology and may be unfamiliar with vulnerabilities associated with the internet and technology.

32. Older Americans are targeted

33. This type of abuse may be relatively new to people 60 or older, they didn't grow up with this technology, the exposure and access of their personal data, social media, may feel more vulnerable because of their age, and given their age may have family members such as children and grandchildren living further away from them.

34. Some people 60 and older are not familiar with the cyber world and tend to be more trusting than other individuals.

35. Too trusting

36. People of age 60 and over are less savvy regarding threats from the internet. The internet as an avenue to conduct crimes is not well known, understood, or intuitive. Individuals of age 0 and over are more attuned to physical security measures such as locking a car, closing windows, stopping mail when gone for extended periods of time. Taking steps to protect one's personal information from internet theft is not likely common practice among this age group.

37. The demographic is less inclined to understand and/or have an awareness of the vulnerabilities associated with the technologies used today (cell phones, tablets, other smart devices) unless they have a technical background.

38. Older people are less familiar with the technology.

39. Lack of internet savvy and awareness of bad actors and spear phishing.

40. I'm assuming most people over 60 are not as aware of their vulnerability to cyber-enabled financial abuses.

41. Generalizing, but the older population is typically more susceptible to scams and social engineering of all types (or at least more targeted) whether it be in-person, telephonic, or cyber-enabled. Additionally, folks with less familiarity / experience with technology, may be more prone to falling for certain scams that utilize that –e.g. more likely to call a number or turn over information to strangers to 'fix IT problems,' so a lack of cyber-savvy creates additional vulnerabilities that could be exploited.

42. Those over 60 and older have a tendency not to be aware of the dangers of cyber criminals and malicious software. Not all but as a trend. Also, those 60 and older, especially older, do not always question information delivered to them by what they perceive as a trusted source.

43. I am marking this relative to a 20-year old. Not as a sort of absolute measure of risk. In general, I believe most people are very susceptible to fraud. Risk factors only increase when conducted online and targeting the elderly. I worked at a bank and on about one customer per month wiring money to fraudsters. I've helped perform auditing of an estate sale in order to prevent fraud. The risks are real. Evidence is difficult to generate for police involvement and the personal humiliation victims experience prevents them from seeking help anyway.

44. Seniors are typically less in tuned to the tricks of cyber criminals and thus more prone to being targets by cyber criminals.

45. Vulnerable because (as a stereotype) older people are often in a position of dependency on younger people for help with changes in technology and personal/home economic matters that have changed over time. While older people are capable of learning the new ways of doing things, they often don't for a variety of reasons and remain in a position where they are forced to simply trust those that help. This relationship can be abused.

46. There is a lack of education about cyber threats and best practice on the Web for this age group.

47. I think this is truer for folks over 70- those who have not spent their adult lives in the digital sphere and do not fully understand how it operates or how a criminal can use it for nefarious intent. There are also generational differences in how you respond to unsolicited questions. In my experience, over 70s still feel compelled to answer the phone or the door.

48. Since I am in that age group, I do not feel I am any more vulnerable than younger people.

49. Technology has led beyond the tail-end 'baby-boomers' in many cases. People in their 60s are not exposed to, or educated about, the intricacies of the deception associated with new cyber technologies.

50. They are generally less computer savvy, and some have memory or other cognitive problems.

51. People over 60 may not be as familiar with the internet as the younger generations, (such as those in their teens – say 40s), so they may put info out there not realizing who can see it.

52. Unfamiliar with some of the technology and often unsuspecting of criminal intent.

53. Not educated enough. Can't keep up with the tech.

54. Classic confidence scam, just a different method of communication.

55. Older people have not grown up in an age where they had to question the legitimacy of everything in front of them.

56. This is all about experience and training. For those that use the internet for basics but choose, or do not know how, to stay apprised of the risks, there is a higher possibility their naiveté puts them at a higher risk of abuse.

57. Lack of cyber awareness.

58. Personal opinion – most simply don't understand how there is little to no regulation about what is out on the internet/control of information.

59. Many people in their 60s are not comfortable with technology, specifically on the computers. Simultaneously, many are trusting of people and susceptible to scamming via the phones and can be coerced into providing valuable information for access to home computers with financial information.

60. I think those in their 60s are more familiar with on-line cybercrimes whereas older (70+) have less familiarity with computers/on-line matters and therefore, more likely to fall for scams.

61. Those 60 with a mindset of continuous improvement or lifestyle has lesser chances of becoming a victim.

62. Because people will access their financial information on Wi-Fi networks. In addition, I know a few individuals who do not believe in software security on their computers or smart phones.

63. They may not know the sign of scams.

64. I frequently read articles about financial abuse and scams conducted. Some elderly people are very savvy, but it's the ones who don't understand all the technical vulnerabilities and jargon (e.g. phishing, fileless, and malware) are most susceptible.

65. No comment.

66. Some elderly may feel obligated to provide additional personal information in order to protect their finances when being told additional information is required.

67. Generally are not aware of the level of sophistication of scammers and their methodologies.

68. They may not be tech savvy. Elder abuse!

69. Unfamiliarity with the operating system, coupled with loneliness.

70. People at the age of 60 have lived much of their lives in a time when modern technology was being developed, but not when they needed it for their careers. In my

opinion, they can probably use the internet wisely without providing critical information to strangers, but are more susceptible than younger generations who grew up surrounded by this technology to cyber-enabled financial abuse.

71. Most likely due to a lack of familiarity with modern technologies that enable cybercrimes and the vulnerabilities of those technologies to hacking.

72. Too many people don't understand the power of the Internet.

73. Callers use threats such as "if you don't respond today to this pain medication ad, then Medicare will consider you ineligible for any further assistance." This is a quote from a phone call yesterday. The use of tactics is quite common "the sheriff is on the way to your house now to arrest you for Tax Fraud. If you don't answer now, you will be arrested and there is nothing I can do." Another quote.

74. Lack of experience with computer and phone security.

75. Because of the number of robo calls and phishing attempts I receive. I am one of those individuals who are over 60. I hope my social security number is not available on the internet, but I am not sure.

76. Increased technology complexity while decreasing keeping up at that age.

77. Not savvy enough to be aware of phishing.

78. My parents are both above 60 years old and are still relatively new to technology. I remain extremely concerned with their Internet use and not being able to discern legitimate websites vs spoofed ones and the same about emails/phishing attempts.

79. Many are not a computer savvy as they need to be.

80. My sixteen-year-old was dubbed into buying malware and she is pretty tech savvy—easy for someone who does not understand technology.

81. Older Americans are more likely to answer the phone or an email query and believe solicitors who are offering them some kind of "deal" or are claiming to be in need of immediate assistance.

82. It would depend on how connected to the internet they are. I would say a fair amount of people over 60 do not use the internet and those that do are probably at risk because they do not necessarily understand how it works.

83. As they grew up, they were constantly taught that more automation is better. They trusted automation. They grew up believing computers make everything faster, more efficient, makes life better, and thus more trustworthy.

84. Longer digital and archived hardcopy histories, and have to deal with Social Security Administration and other poorly disciplined agencies such as OPM who get your data fumble it.

85. Because senior citizens might not be well-versed in technology and they might have retired from work (with money to spend), they become an easier and much attractive target.

86. Their lack of knowledge and experience using technology, and how exploitable it is.

87. The older the user, the more likely they trust published sources. They are used to print and broadcast media as their content providers and assume the same sort of editorial control is present in on-line publication.

88. Might be easy to lure an older individual into a “sweepstake” type win, especially if the older person doesn’t know how to research a fraud situation.

89. The current over 60 cohort lack some awareness of shared nature of data provided both on-line and off. While some of this will get better as younger people age, the over 60 crowd is often starting on a path of cognitive decline as well as seeming to lack patience for things that don’t work and can give information to get things sorted out without thinking about the consequences.

90. I would not limit the vulnerability to people over 60. The vulnerability is universal. The susceptibility to exploitation is higher for people over 60 because a significant percentage of older individuals are less aware of how much personally identifiable information is digital, legally collected, and therefore, more available for malicious intent.

91. No comment

92. People over age of 60 are usually less tech savvy and unaware of the many ways they could be scammed via the internet or social media; therefore, in general, they are more of a vulnerable age group than many others.

93. A lot of people underestimate how much info is available on the internet for free or a low fee. For example, several services will provide reports listing phone numbers, past addresses, relatives and criminal history of people on demand. If we read electronic books or visit websites, all that info can be tracked by cookies stored in our web browsers. For federal workers, WTOP once had a link to a database that listed names of federal employees and their salary level. The less familiar people are with the internet, the more vulnerable they may be if they use it. Additionally, the number of internet scams and emails with bogus links has increased.

94. No comment.

95. My mother has twice been scammed out of thousands of dollars, when she was 75 and 79 years old, respectively. The second scam was initiated by an email from the

“Microsoft Rebate Center.” Both times, the scammers asked her to do things (wire money internationally, pay them with gift cards) that she would have known were strange when she was younger and didn’t have memory problems.

96. A lot of older people are not familiar with today’s technology and would not realize something is a scam or not.

97. People over 60 don’t understand how much of the internet technology works, what are the best security practices, etc.

98. No comment.

99. Many people over 60 have spent the past decade becoming more savvy with the internet via their phones, ipads or tablets, and computers. This familiarity and additional free time mean that they spend a good deal of time online but they may not be attuned to the risks that come with the online exposure. Presumably, those who are retired are not receiving the same briefings and awareness notifications as those in the workforce.

100. Many are too trusting of everyone who contacts them.

101. Because they are not familiar with the internet and are very trustworthy.

102. Everyone is vulnerable and the less familiar an individual is with online platforms, tools or processes, the more likely they are to be caught in a scam.

103. I think they share the same risk as others, but as they get older and have less on an active on-line footprint/activity.

104. Because they believe what they read.

105. Data is not secure.

106. They are trusting and do not understand that scammers are out to trick them.

107. Unfamiliar with phishing strategies. Lonely and willing to chat. Don’t know how to set security controls. Unfamiliar in how information is collected on the internet. Do not understand the implications of Big Data. It is difficult to keep pace with the amount of change in IT and the associated risks. I can even find the make of your car and what year it is. I can find a list of everyone on your street, political affiliation on dating sites. Not understanding the dangers of chat rooms or interactions with networked games or making friends on-line. Do not understand how to identify a fake email or insecure link. Do not use strong passwords. Use public WiFi.

108. They don’t understand internet/social media.

109. Ignorance. Trust those emailing.

110. Lack of knowledge

111. Everyone is vulnerable. Those with less familiarity with technology are more vulnerable. Decrease cognitive and hearing – just callers are an issue/risk.

112. Not sure, but becoming more prevalent especially with robo calls going out of control and unsuspecting people, young and old, are being scammed with increasing frequency.

113. Generation of trust

114. No comment

115. No comment

116. Are less alert, maybe senile. Easily convinced. Easily frightened.

117. As people age, their senses diminish. They lose family and friends thereby become more isolated. These and other reasons make them more vulnerable.

118. Seniors are called and asked personal questions over the phone, being trustworthy and never throughout their life did they have these scams.

119. More trusting, uninformed. If you provide it on Facebook, etc... it is public “knowledge.”

120. No comment

121. No comment

122. Less computer literate

123. No comment

124. I think people over 60 today are increasingly more knowledgeable than previous years/decades- so hopefully this is improving. Since people over 60 may also be 70 – 80 – 90. I have still I still retain this as a high vulnerability due to unsophisticated with computers and lack of keeping up with computer security; unsuspecting of hoaxes – gotta be alert always; lack of confidence to say NO; lack of current information as the rate of cyber change(s) happens faster and faster – hard to keep up with even as a young person; and lonely. In 2019, a 60-year-old today who drops out of the workforce is likely still a big cyber user for various activities including banking and finance and social activities. However, not working may reduce interaction with others who may share computer security knowledge what they then take home, but now that resource is not available. The victims of these cyber abuses usually fall hard! Never hear a story of less.

125. Not knowledgeable and become less and less informed as they age. Lose cognitive abilities as they age.

126. Because the “retirement class” have their money in the bank, because of not being too savvy, and because of loneliness and therefore gullibility.

127. Because they are conditioned to respect authority more than younger folks.

128. They trust strangers. Think all think others are nice as themselves.

129. The older one gets, more vulnerable, 60-70 not so much.

130. No comment

131. No comment

132. Dementia, Alzheimer’s, widowed – leaves us vulnerable

133. Lack of familiarity with internet and how to operate, what to avoid, may lack education on how to avoid hacks.

134. Too trusting. Criminals have better knowledge and tools. Loneliness.

135. Because their ignorance and naiveté regarding the internet.

136. Everyone are all vulnerable

137. No comment.

138. Seniors are lonely and uninformed.

139. Not sure – but highly likely

140. Many have lost a spouse – unfamiliar with financing the household. Many have no one to turn to.

141. They know enough to get into trouble. They need to keep up-to-date and actively read financial sources. Too many just turn over everything to relatives and “advisors.”

142. Are willing to trust people more and think people are honest.

143. In today’s society people who are over 60 might be less technically advanced.

144. No comment.

145. Older people typically have less experience on the internet and are more likely to trust people on the internet. Younger people have been consistently exposed to scams and are more comfortable with their technical and internet skills so usually fall for less.

146. I think individuals over the age of 60 are more vulnerable to cyber-enabled abuse because I think they have not grown up in the same technological environment with ease of internet access and are probably more hesitant to understand or just have a lack of

knowledge on the capability overall. I think they also trust more in people's word. I think communication with relatives or younger individuals on internet practices would help.

147. Less familiar with technical exploitation (phishing, etc.). More likely to have failing mental capacities (dementia, etc.).

148. Less familiar with the amount of data out there that can be used against them.

149. People over 60 are more likely to not be "in the know" on the internet and the risks posed as well as the risks from phone scammers (i.e. telemarketers, people posing as the IRS, etc...).

150. Technology is always changing, and older people are less likely to keep up with those changes.

151. A lot of people over 60 (really any age) may not take the proper precautions to protect their personally identifiable information which is usually what gets stolen or exploited. Simple boredom with nothing to do, some may go to the internet to pass the time.

152. General understanding of the internet and prevalence of malicious actors plays a large role. I think this age group tends to take people at face value more than younger generations.

153. May not be as informed about on-line fraud, security settings, scams, on-line surveys to collect data, etc...

154. They don't have a full understanding of the capabilities of those who are seeking this info.

155. I feel they're the most vulnerable due to being easier to trust.

156. We're all vulnerable, but in general the less experienced we are with the internet, the more ways we can be taken advantage of.

157. Trusting and unfamiliar with the depth of cyber fraud and their vulnerabilities of who and what they are dealing with on the web.

158. Generally, though not exclusively, lack of familiarity with new data dynamics and availability.

159. Some calls are almost too convincing and sound like authorities. Others work hard to ignore requests to stop calling and badgering.

160. Extremely vulnerable, as we are becoming more dependent on cyber world for day-to-day living.

161. They have more information in general out on the web and they also may not be up to date on the best and newest practices on how to protect themselves.

162. They don't understand the technology enough to know the vulnerabilities. Nor are they likely privy to latest crime trends to watch out for.

163. Their brains aren't functioning or processing information like they used to due to the aging of their brains regions like the frontal lobe being "worn down" and or weakening.

164. No comment.

165. Especially with the prevalence of large-scale hacks of major corporations, which hold personal information, I think everyone is vulnerable to cyber criminals now more than ever. With regard to older people, they would be more vulnerable to phishing scams involving technology than a younger person if they didn't know how things on the internet should work.

166. Probably a combination of factors to include unfamiliarity with the internet in general, lack of awareness of scams. Perhaps more trusting generation. Loneliness in some cases.

167. Very vulnerable. They are not aware of phishing and effects of malware. More internet time. Decreasing awareness.

168. A large number of people over 60 are unfamiliar with technology jargon, technical exploitation techniques, and too easily trust. They could easily be scammed.

## **Appendix D**

### **Definitions of Terms**

There is a lack of standardized definitions of elder abuse, internet crime, and financial terms across the federal government and the 50 independent states. Contributing to the problem is the variability among state laws and failure to adopt federal definitions found in documents or in laws such as the Older Americans Act. For the purposes of this study, the definitions of terms used in this report are listed to ensure clarity and consistency. Where necessary, the citation is included.

*big data*—Large, diverse, complex, datasets

*bit*—Binary information digit.

*burner*—A mobile phone application that enables smartphone users to have a temporary or disposable telephone number.

*communications protocol*—Rules permitting entities to send and receive information across a system. The protocol is software and hardware defined and implemented through a set of syntax, communication synchronization, and other rules.

*computer*—An electronic, magnetic, optical, electrochemical, or other high-speed data-processing device performing logical, arithmetic, or storage functions; this includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such does not include an

automated typewriter or typesetter, a portable hand held calculator, or other similar device.

*confidence fraud*—A knowing misrepresentation or concealment of truth or facts to induce another person to act to his or her detriment. A financial loss due to a breach in a relationship of trust. This includes incidents involving a fraudulent attempt to get the complainant to send money and where nothing is bought or sold. (IC3 2012). In auction fraud, a transaction occurs in an online auction site with nondelivery of merchandise or payment. Overpayment fraud occurs when the victim receives an invalid monetary instrument with instructions to deposit it in a bank account and to send the excess funds back to the sender. In advance fee fraud, criminals convince victims that to receive something, they must first pay money to cover some sort of incidental cost or expense (IC3 2008).

*covered entity*—Covered entity has the same meaning as telecommunications carrier.

*cybercrime*—A crime committed via telecommunications networks in which computers or computer networks are used for criminal activity. Activities may include financial exploitation, denial of service, credit card fraud, identity theft, blackmail, harassment, stalking, software piracy and child pornography (IC3 2012). Advanced cybercrime—often termed high-tech crime—is a crime committed where the computer is the target (Interpol 2016). In cyber-enabled crime, a computer is the tool of the crime (Interpol 2016).

*cryptobin*—A website for storing and sharing texts, which may have been obtained illegally.

*cryptocat*—An application that enables encrypted online chat sessions.

*cryptojacking*—A form of cyberattack whereby the target’s computer processing power is used to mine cryptocurrency.

*counterfeited*—A document that is claimed to be genuine but is not, because it has been falsely made or manufactured in its entirety.

*cyberspace*—Network of networks including the internet (Anderson and Rainie 2017).

*data*—Anything that describes the physical location and state of an entity—its position, temperature, vector of motion, existence in a time continuum, or any other attribute of its existence. Answers four basic questions—who, what, where, and when.

*data aggregation*—“Data aggregation systems are little discussed by the platform businesses that provide them access. Knowing the degree to which their personal behavior is being monitored may make consumers queasy. Because data aggregation is a large and growing source of revenue for platform companies, managing it appropriately poses an enormous ethical, legal and business challenge” (Parker, Van Alstyne, and Choudary 2016, 146).

*data breach*—“An unauthorized or unintentional exposure, disclosure, or loss of an organization’s sensitive information” (GAO 2018, 3). The information may include social security numbers, personally identifiable information, or financial information (GAO 2018).

*digital certificate*—Encrypted electronic token used to authenticate servers and systems (GAO 2018)

*email*—Electronic mail developed by Ray Tomlinson in 1971.

*email spoofing*—Sending email with false information, including the name of the originator.

*fictitious identity*—A false identity.

*file*—A collection or unit of records.

*financial or material exploitation*—The illegal or improper use of funds, property, or assets. Examples in the context of this study include but are not limited to cashing checks without authorization or permission; forging an older person's signature; misusing or stealing an older person's money or possessions; coercing or deceiving an older person into signing a document (e.g., contracts or a will); and the improper use of conservatorship, guardianship, or power of attorney (AoA 2011). Specifically, perpetrators of financial exploitation take advantage of victims' psychological vulnerability or lack of capacity to make an appropriate decision (Hill 1994; Roubick 2009).

*forged*—A document that claims to be genuine, but is not because it has been falsely produced, altered, signed, or endorsed, to contain a false addition or deletion therein or is a combination of two or more genuine documents.

*fraud*—Deceiving or tricking a victim who has the capacity to make an informed decision based on the available information (Hill 1994; Roubick 2009). Fraud is a malignant version of a healthy and fair free-flowing financial market space; it is not an externality like air pollution, for which a tax on gas can be levied to help mitigate the problem (Akerlof and Shiller 2015).

*FTP*—File transfer protocol is a program that enables the transfer of files among computers on the network.

*fundamental attribution error*—The tendency to form a judgment about others and underestimate the importance of the situation (O’Sullivan 2003).

*gaming fraud*—A misrepresentation of the odds of winning a prize or tampering with a bet.

*information*—Data that are put into some sort of context to answer questions of how and why, which attributes explanatory relationships among the data.

*hacker*—An individual who possesses a level of skill in computers and technology and has used this ability to access computer systems with or without the owner’s permission (Holt 2005).

*hacking*—A type of crime where a computer is broken into for the purposes of accessing personal or sensitive information.

*host*—A computer that communicates over the internet.

*ICT*—Information and communication technologies.

*identity theft*—Unauthorized use of a victim’s personal identifying information to commit fraud or other crimes (IC3 2008).

*information asymmetry*—Whenever one party to an interaction knows facts that the other parties do not and uses that knowledge for personal advantage (Parker, Van Alstyne, and Choudary 2016).

*Internet*—A “term in section 1101 of the Internet Tax Freedom Act noted in 47 USC.”<sup>60</sup> A collection of networks.

*Internet of things* (IOT) – provides the ability of devices to communicate with each other using embedded sensors that are linked through wired and wireless networks. The

---

<sup>60</sup> 18 U.S.C. § 225 (2007).

myriad of connected devices ranges from a home thermostat, to a car, or a pacemaker monitored by a doctor. The internet is used to transmit, compile, and analyze the data (Podesta et al. 2014).

*investment fraud*—Deceptive practices involving the use of capital to create more money through means designed to result in capital gains. Market manipulation, Ponzi schemes, and pyramid schemes are examples of investment fraud.

*IP (internet protocol) address*—An address hosted on the internet represented by a 32-bit number.

*IP-enabled voice service*—Real-time voice communications transmitted over a customer owned equipment using TCP/IP protocol with interconnection capability in order to originate traffic to, or terminate traffic from, the public switched telephone network.

*IP spoofing*—A method of attack where the hacker forges the addresses to fool trusted computers.

*lurking*—Reading posted messages without responding.

*malvertising*—Malicious software advertisements added to valid online advertising webpages and networks.

*masquerading*—When an individual uses another person’s identity in order to gain access to a computer.

*network*—The physical domain of cyberspace (Anderson and Rainie 2017).

*offense*—“Any criminal offense . . . which is in violation of an Act of Congress and is triable in any court established by Act of Congress.”<sup>61</sup>

---

<sup>61</sup> 18 U.S.C. § 3156

*older American*—A citizen aged 60 years or older (also *elder* or *senior citizen*). There is no universally accepted definition of a senior citizen or elderly person. Each state independently defines the terms in accordance with affected laws and policies. For the purposes of this study, a senior citizen or elder is defined as someone who is eligible for social security by virtue of their age, whether or not they receive benefits or have chosen to continue to work. Many citizens in this age category prefer to be labeled *older Americans* because the terms *elderly* and *senior* may be considered by some as pejorative (Applewhite 2016). In this study, all three terms are used interchangeably.

*organized crime*—Any group having some manner of a formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of actual or threatened violence, corrupt public officials, graft, or extortion, and generally have a significant impact on the people in their locales, region, or the country as a whole (FBI 2016).

*Pastebin*—An online website for sharing and storing texts.

*personally identifiable information*—Any information that can be used to recognize an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information (GAO 2018).

*phishing*—A portmanteau of *fish* and *phreaking* often referred to as electronic bait. A criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity information and financial account data by deceptive means (Anti-Phishing Working Group 2012).

*phreaking*—A portmanteau of phone system breaking.

*psychographics*—Market research or statistics classifying populations according to psychological variables such as attitudes, values, desires as well as demographical variables such as age, gender, sex, race.<sup>62</sup>

*romance fraud*—Criminals use online dating sites or social network sites to meet victims. False promises and emotional connections entice victims to send something of value (IC3 2008).

*scams*—In FBI scams, a criminal acts as though they are an employee of the FBI to defraud victims. In social security scams, a criminal claims the victim owes money that must be paid immediately.

*secure socket layer (SSL)*—A technology that encrypts communications between a website and the consumer—the internet user (Cyveillance 2010).

*short message service (SMS)*—A text messaging service that provides text communications to cell many telephones, internet, and mobile devices.

*social engineering*—The practice of deceiving a target, who may never realize they have been victimized, using nontechnical means through personal interaction with the express intent of tricking the victim into revealing personal information, giving up something of value, or breaching normal security practices (Long 2008).

*social media*—A means to transmit information. It is also the sharing of real names and profiles, behavioral tracking, data mining, postings and media through channels. (Silverman 2015).

*social networks*—Groups of people who converse with one another. A web-based service that enables an individual to create, within a bounded structure, a public profile

---

<sup>62</sup> Merriam-Webster Online Dictionary, online s.v. “psychographics,” accessed June 5, 2019, <http://www.merriam-webster.com/dictionary/psychographic>

and display their social connections for others to view and search (Boyd and Ellison 2007).

*social organization*—The patterns of relationships among people as part of a network of social relations (Best and Luckenbill 1982).

*spam*—The distribution of unsolicited email with false information intended to sell products, conduct phishing schemes, distribute spyware or malware, or attack the host computer. Unsolicited and unwelcome email, usually mass distributed.

*technical subterfuge*—Schemes implant crimeware in computers to steal credentials, often using systems to intercept consumers online account usernames and passwords to corrupt navigational infrastructures to misdirect consumers to counterfeit websites (Anti-Phishing Working Group 2012).

*telecommunications carrier*—Includes any provider of IP-enabled voice service.

*Tor*—An encrypted network through which clandestine messages can be sent and received.

*transmission control protocol/Internet protocol* (TCP/IP)—Program developed by Vinton Cerf, Yogen Dolal, and Carl Sunshine.

*Trojan*—Appears to be like any other program but is malicious in nature and is capable of performing unauthorized tasks.

*victim*—A person who through the use of the internet responded to a request or notification or offer and provided personal information or an asset, which led to either a financial or non-financial loss (Cross, Smith, and Richards 2014).

*virus*—An executable file that remains dormant until opened and then deletes information as it collects it.

*vishing*—A portmanteau of *voice* and *phishing*. Voice over IP allows for caller ID spoofing, and automated systems make it difficult for legal authorities to monitor trace or black. Usually used to steal credit card numbers.

*VOIP* (voice over Internet protocol)—Allows the user to make voice calls over the internet.

*vulnerability*—“A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by an attacker” (GAO 2018, 4).

*vulnerable elder*—One whose physical and mental health puts him or her at increased risk of abuse.

*web site*—A set of files hosted on a server that are accessed via the internet using a web browser.

*worm*—a program that travels across the network from one server to another capable of spreading without the assistance from other files. Coined by John Brunner in his 1975 novel *The Shockwave Rider*.

## References

- AARP (American Association of Retired Persons). 1996. *Telemarketing Fraud Victimization of Older Americans: An AARP Survey*. Washington, DC: Princeton Survey Research Associates.
- . 1999. *Consumer Behavior, Experiences and Attitudes: A Comparison by Age Groups*. Princeton, NJ: Princeton Survey Research.
- . 2003. *Off the Hook: Reducing Participation in Telemarketing Fraud*. Washington, DC: US Department of Justice and AARP Foundation.
- Agarwal, Sumit, John C. Driscoll, Xavier Gabaix, and David Laibson. 2009. "The Age of Reason: Financial Decisions over the Life-Cycle with Implications for Regulation." Brookings Papers on Economic Activity. October 19, 2009. [https://www.brookings.edu/wp-content/uploads/2016/07/2009b\\_bpea\\_agarwal.pdf](https://www.brookings.edu/wp-content/uploads/2016/07/2009b_bpea_agarwal.pdf)
- Akerlof, George A., and Robert J. Shiller. 2015. *Phishing for Phools: The Economics of Manipulation and Deception*. Princeton, NJ: Princeton University Press.
- Albanese, Jay S. 2012. "Deciphering the Linkages Between Organized Crime and Transnational Crime." *Journal of International Affairs* 66 (1): 2–16.
- Alkaabi, Ali, George Mohay, Adrian McCullagh, and Nicholas Chantler. 2011. "Dealing with the Problem of Cybercrime." Digital Forensics and Cyber Crime. ICDF2C. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Edited by I. Baggili, 53: 1–18. Berlin.
- Alter, Adam. 2017. *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked*. New York: Penguin Press.
- Analysis Group. 2012. "Complex Financial Instruments." Accessed December 20, 2012. [http://www.analysisgroup.com/complex\\_financial\\_instruments.aspx](http://www.analysisgroup.com/complex_financial_instruments.aspx).
- Anderson, Janna, and Lee Rainie. 2017. "The Future of Truth and Misinformation Online." Pew Research Center: Internet and Technology. October 18, 2017. <http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/>.
- Anderson, Keith B. 2013. *Consumer Fraud in the United States, 2011: The Third FTC Survey*. Washington, DC: Federal Trade Commission.
- Anderson, Monica, and Andrew Perrin. 2017. "Tech Adoption Climbs among Older Adults." Pew Research Center. May 17, 2017. <http://pewinternet.org/2017/05/17/tech-adoption-climbs-among-older-adults>.

- Angwin, Julia. 2015. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: St. Martin's Press.
- Anti-Phishing Working Group. 2012. *Phishing Activity Trends: Report for the Second Quarter 2012*. September 12, 2012.  
[http://docs.apwg.org/reports/apwg\\_trends\\_report\\_q2\\_2012.pdf](http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf).
- AoA (Administration on Aging). 2011. *FY2011 Report to Congress*.  
[http://www.aoa.gov/AoARoot/About/Annual\\_Report/doc/FY%202011%20Report%201020Congress%20AoA%20Final%2012%2012.pdf](http://www.aoa.gov/AoARoot/About/Annual_Report/doc/FY%202011%20Report%201020Congress%20AoA%20Final%2012%2012.pdf).
- . 2013. *Future Growth*. December 31, 2013.  
[http://www.aoa.gov/AoARoot/Aging\\_Statistics/Profile/2013/4.aspx](http://www.aoa.gov/AoARoot/Aging_Statistics/Profile/2013/4.aspx).
- . 2014. “Administration on Aging Programs.” Accessed March 22, 2014.  
[http://www.aoa.gov/AoARoot/AoA\\_Programs/OAA/index.aspx](http://www.aoa.gov/AoARoot/AoA_Programs/OAA/index.aspx).
- . 2016. “Administration on Community Living.” July 22, 2016.  
[http://www.aoa.gov-aos\\_programs/elder\\_rights/ea\\_prevention/whatisea.aspx](http://www.aoa.gov-aos_programs/elder_rights/ea_prevention/whatisea.aspx).
- AP News*. 2017. “State: TV Maker Improperly Tracked Consumers’ Viewing Habits.” February 6, 2017. <https://apnews.com/d9365f9e45034f438944edeba982b5b6>.
- Applewhite, Ashton. 2016. *This Chair Rocks: A Manifesto Against Ageism*. New York: Networked Books.
- Aransiola, Joshua Oyeniyi, and Suraj Olalekan Asindemade. 2011. “Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria.” *Cyberpsychology, Behavior, and Social Networking* 14, no. 2 (November): 759–63.
- Archick, Kristin. 2006. *Cybercrime: The Council of Europe Convention*. Congressional Research Service, Washington, DC: The Library of Congress.
- Ariely, Dan. 2009. *Predictably Irrational: The Hidden Forces That Shape Our Decisions*. New York: HarperCollins.
- Asch, Solomon. 1956. “Studies of Independence and Conformity: A Minority of One Against a Unanimous Majority.” *Psychological Monographs: General and Applied* 70, no. 9: 1–70.
- Asp, Erik, Kenneth Manzel, Bryan Koestner, Catherine A. Cole, Natalie L. Denburg, and Daniel Tranel. 2012. “A Neuropsychological Test of Belief and Doubt: Damage to Ventromedial Prefrontal Cortex Increases Credulity for Misleading Advertising.” *Frontiers in Neuroscience* (July) 6, no.100:  
[http://www.frontiersin.org/Decision\\_Neuroscience/10.3389/fnins.2012.00100/ful](http://www.frontiersin.org/Decision_Neuroscience/10.3389/fnins.2012.00100/ful).
- Aston, Kevin. 2016. “The Inevitable Internet of Things.” *IQT Quarterly* 8, no.1: 9–12.

- Babazadeh, Natasha. 2018. "Legal Ethics and Cybersecurity: Managing Client Confidentiality in the Digital Age." *Journal of Law and Cyber Warfare* 7, no. 1: 85– 116.
- Bainbridge, John. 1955. "The Braveness to Be Herself: In Private Affairs or in Public Garbo Ignores Others' Opinions." *Life*, January 24, 1955, 113.
- Banerjee, Sudipto. 2011. "State-by-State Financial Capability Survey: How Do Financial Literacy and Financial Behavior Vary by State?" FINRA: Investor Education Foundation. November, 2011.  
[http://www.usfinancialcapability.org/pr\\_12082010.html](http://www.usfinancialcapability.org/pr_12082010.html).
- Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. February 8, 1996.  
<https://www.eff.org/cyberspace-independence>.
- Barnes, Lisa L., Carlos F. Mendes de Leon, Julia L. Bienias, and Denis A. Evans. 2004. "Social Resources and Cognitive Decline in a Population of Older African Americans and Whites." *Neurology* 63, no. 12: 2322–26.  
<http://doi.org/10.1212/01.WNL.0000147473.04043.B3>.
- Barrett, Michael, Andy Steingruebl, and Bill Smith. 2011. *Combating Cybercrime: Principles, Policies, and Programs*. April, 2011. [http://www.paypal-media.com/assets/pdf/fact\\_sheet/PayPal\\_CombatingCybercrime\\_WP\\_0411\\_v4.pdf](http://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf).
- Batson, C. Daniel, Bruce D. Duncan, Paula Ackerman, Teresa Buckley, and Kimberly Birch. 1981. "Is Empathic Emotion a Source of Altruistic Motivation?" *Journal of Personality and Social Psychology* 40, no. 2: 290–302.
- Beach, Derek, and Rasmus Brun Pedersen. 2013. *Process-Tracing Methods: Foundations and Guidelines*. Ann Arbor: The University of Michigan Press.
- Becker, Gary. 1968. "Crime and Punishment: An Economic Approach." *The Journal of Political Economy* 76, no. 2: 169–217.
- Becker, Gary S. 1993. "Nobel Lecture: The Economic Way of Looking at Behavior." *The Journal of Political Economy* 101, no. 3: 385–409.
- Bell, J. Bowyer, and Barton Whaley. 1991. *Cheating and Deception*. New Brunswick, NJ: Transaction.
- Bennett, Andrew, and Jeffrey T. Checkel. 2012. "Process Tracing: From Philosophical Roots to Best Practices." *Simons Papers in Security Development* 21 (June): 1–48.

- Bensinger, Greg. 2019. "Google Employs Humans to Listen to Some Voice-Assistant Recordings." *Washington Post*, July 11, 2019.  
<https://www.washingtonpost.com/technology/2019/07/11/google-employs-humans-listen-some-voice-assistant-recordings>.
- Bergman, Michael K. 2001. *The Deep Web: Surfacing Hidden Value*. White paper, University of Michigan, Ann Arbor. <https://doi.org/10.3998/3336451.0007.104>.
- Bertoni, Daniel. 2009. *Identity Theft*. Washington, DC: Government Accountability Office. <http://www.gao.gov>.
- Best, Joel, and David F. Luckenbill. 1982. *Organizing Deviance*. Englewood Cliffs, NJ: Prentice-Hall.
- Biegelman, Martin T. 2009. *Association of Certified Fraud Examiners*. September/October. Accessed October 23, 2011.  
<http://www.acfe.com/article.aspx>.
- Bok, Sissela. 1999. *Lying: Moral Choice in Public and Private Life*. New York: Vintage Books.
- Bonnie, Richard J., and Robert B. Wallace, editors. 2003. *Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America*. Report to National Research Council. Washington, DC: The National Academies Press.
- Borchers, Timothy A. 2013. *Persuasion in the Media Age*. 3rd. ed. Long Grove, IL: Waveland Press.
- Borgesius, Frederik Zuiderveen, and Joost Poort. 2017. "Online Price Discrimination and EU Data Privacy Law." *Journal of Consumer Policy* 40, no. 3: 347–66.
- Bossler, Adam, and Thomas J. Holt. 2009. "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3, no. 1: 400–20.
- Boutin, Paul. 2016. "The Secretive World of Selling Data About You." *Newsweek*. May 30. <http://www.newsweek.com/secretive-world-selling-data-about-you-464789>.
- Boyd, Danah, and Nicole Ellison. 2007. "Social Network Sites:Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, no.1 (October): 210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>.
- Brenner, Susan W. 2002. "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships." *North Carolina Journal of Law and Technology* 4, no. 1: 1–50.
- . 2013. "Cyber-threats and the Limits of Bureaucratic Control." *Minnesota Journal of Law, Science, and Technology* 14, no. 1: 137–258.

- Bressler, Amery & Ross. 2019. "Senior and Vulnerable Investor Laws." Accessed July 2019. <https://www.bressler.com/senior-map>.
- Briers, Barbara, Mario Pandelaere, and Luk Warlop. 2007. "Adding Exchange to Charity: A Reference Price Explanation." *Journal of Economic Psychology* 28, no. 1: 15–30.
- Broadhurst, Roderic, and Lennon Y. C. Chang. 2012. "Cybercrime in Asia: Trends and Challenges." In *Asian Handbook of Criminology*, edited by S. Jou, J. Liu, and B. Hebenton, 49–64. New York: Springer.
- Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime." *International Journal of Cyber Criminology* 8, no. 1: 1–20.
- Bromley, Dennis B. 1990. "Academic Contributions to Psychological Counselling: I. A Philosophy of Science for the Study of Individual Cases." *Counselling Psychology Quarterly* 3, no. 3: 299–307.
- Brooks, David. 2011. *The Social Animal: The Hidden Sources of Love, Character, and Achievement*. New York: Random House.
- Brown, Kay. 2012. *Elder Justice: National Strategy Needed to Effectively Combat Elder Financial Exploitation*. GAO-13-110. Washington, DC: United States Government Accountability Office. <http://www.gao.gov/products/GAO-13-110>.
- Brown, Stephanie L., Terrilee Asher, and Robert B. Cialdini. 2005. "Evidence of a Positive Relationship between Age and Preference in Consistency." *Journal of Research in Personality* 39, no. 5: 517–33.
- Brownstein, Joseph. 2010. "Health Care Overhaul's Uncertain-Super-Majority Free Future." *ABC News Medical Unit*. January 10. Accessed April 5, 2014. <http://abcnews.go.com/Health/HealthCare/scott-brown-win-massachusetts-begs-question-health-care/story?id=9615918>.
- Buchanan, Margot A. 2011. "Privacy and Power in Social Space: Facebook." PhD Diss., University of Stirling, Scotland. Accessed March 15, 2018. <https://dspace.stir.ac.uk/bitstream/1993/9150/1/PhD thesis .>
- Bullee, Jan-Willem, Lorena Montoya, Marianne Junger, and Pieter Hartel. 2017. "Spear Phishing in Organisations Explained." *Information and Computer Security* 25, no. 5: 593–613.
- Burgard, Anna, and Christopher Schlembach. 2013. "Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet." *International Journal of Cyber Criminology* 7, no. 2: 112–24.

- Butler, Robert N. 1975. *Why Survive? Being Old in America*. Baltimore: Harper and Row.
- Bytheway, Bill. 1995. *Ageism*. Philadelphia: Open University Press.
- Cardozo, Nate. 2017. "D.C. Circuit Court Issues Dangerous Decision for Cybersecurity: Ethiopia is Free to Spy on Americans in Their Own Homes." *Electronic Frontier Foundation*. Accessed December 3, 2018.  
<https://www.eff.org/deeplinks/2017/03/dc-circuit-court-issues-dangerous-decision-cybersecurity-ethiopia-free-spy>.
- Carlson, Eric. 2006. "Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow." *The Elder Law Journal* 14, no. 2: 424–52.
- Carstensen, Laura L. 2009. *A Long Bright Future*. New York: Broadway Books.
- Castle, Elizabeth, Naomi I. Eisenberger, Teresa E. Seeman, Wesley G. Moons, Ian A. Boggero, Mark S. Grinblatt, and Shelley E. Taylor. 2012. "Neural and Behavioral Bases of Age Differences in Perceptions of Trust." *The Proceedings of the National Academy of Sciences* 109, no. 51 (December): 20848–20852.  
<https://doi.org/10.1073/pnas.1218518109>.
- Cavan, Ruth Shoule. 1962. "Self and Role Adjustment During Old Age." In *Human Behavior and Social Process: An Interactionist Approach*, edited by Arnold Rose, 526–36. Boston: Houghton-Mifflin.
- Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II*. Washington, DC: Center for Strategic and International Studies. <http://csis.org/analysis/et-losses-estimating-global-cost-cybercrime>.
- Chabinsky, Steven R. 2009. *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy Rights in Cyberspace*. Washington, DC, Department of Justice.  
<https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2009/11/17/2009-11-17-fbi-chabinsky-cybersecurity.pdf>.
- Chang, Joshua J. S. 2008. "An Analysis of Advance Fee Fraud on the Internet." *Journal of Financial Crime* 15, no. 1: 71–81.
- Chertoff, Michael. 2018. *Exploding Data: Reclaiming Our Cyber Security in the Digital Age*. New York: Grove Atlantic.
- Chessen, Matt. 2017. *The Madcom Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy... And What Can Be Done About IT*. Washington, D.C.: Atlantic Council. <http://www.atlanticcouncil.org/publications/reports/the-madcom-future>.

- Chesterton, Gilbert Keith. 1905. *Daily News*, July 29, 1905.
- Chickowski, Ericka. 2014. "6 Recent Real-Life Cyber Extortion Scams." *Information Week: Darkreading*, June 23, 2014. <http://www.darkreading.com/attacks-breaches/6-recent-real-life-cyber-extortion-scams/d/d-id/1278774>.
- Childress, Autumn. 2019. "Local Woman Scammed Out of More Than \$600,000 in Online Scam." *WHSV3*, February 15, 2019. <https://www.whsv.com/content/news/local-woman-scammed-out-of-over-600000-dollars-police-say-505920171>.
- Choi, Namkee G., Jinseok Kim, and Joan Asseff. 2009. "Self-Neglect and Neglect of Vulnerable Older Adults: Reexamination of Etiology." *Journal of Gerontological Social Work* 52, no. 2: 171–87. <https://doi.org/10.1080/01634370802609239>.
- Christl, Wolfie. 2017. "How Companies Use Personal Data against People." *Cracked Lab—Institute for Critical Digital Culture*, October, 2017. [http://crakedlabs.org/dl/CrackedLabs\\_Christl\\_CorporateSurveillance.pdf](http://crakedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)
- Cialdini, Robert B. 1993. *Influence: The Psychology of Persuasion*. New York: William Morrow.
- Cialdini, Robert B. 2001. *Influence: Science and Practice*. 4th ed. Boston: Allyn and Bacon.
- Cialdini, Robert B. 2016. *PRE-SUASION: A Revolutionary Way to Influence and Persuade*. New York: Simon and Schuster.
- Clandinin, David J., and Janice Huber. 2010. "Narrative Inquiry." In *International Encyclopedia of Education*, 3rd ed., edited by B. E. Baker and P. P. Peterson McGaw, 436–441. New York: Elsevier.
- Clarke, Roger. 1988. "Information Technology and Dataveillance." *Communications of the ACM*, edited by Josheph Savirimuthu, III, (31): 498-512. <https://www.taylorfrancis.com/books/9781315243566/Chapters/10.4324/9781315243566-27>.
- Clough, Jonathan. 2014. "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation." *Monash University Law Review* 40, no. 3: 698–736.
- Cohen, Aaron M. 2010. "Wiring the Elderly." *Internet* 44, no. 2: 7–8.
- Cohen, Lawrence, and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4: 588–608.
- Colello, Kirsten J. 2012. *Older Americans Act: Long-Term Care Ombudsman Program*. Report for Congress. Washington, DC: Congressional Research Service.

- . 2017. *The Elder Justice Act: Background and Issues for Congress*. R43707. Washington, DC: Government Accountability Office. <http://www.crs.gov>.
- Consumer Financial Protection Bureau. 2015. *Financial well-being: The goal of financial education*. [http://files.consumerfinance.gov/f/201501\\_cfpb\\_report\\_financial-well-being.pdf](http://files.consumerfinance.gov/f/201501_cfpb_report_financial-well-being.pdf).
- Consumer Financial Protection Bureau. 2017. DFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products. (January 3, 2017) <https://www.consumerfinance.gov/cfp-orders-transunion-and-equifax-pay-dec>.
- Cookson, Amelia. 2009. "Net Gains." *Nursing Older People* 21, no. 1: 6–7.
- Corrigan, Jack. 2019. "Lawmaker: Congress Needs Fewer Committees with Cyber Oversight." *Nextgov*. January 29, 2019. <https://www.nextgov.com/cybersecurity/2019/01/lawmaker-congress-needs-fewer-committees-cyber-oversight/154506/>.
- Covey, Stephen M. R. 2006. *The Speed of Trust: The One Thing That Changes Everything*. With Rebecca R. Merrill. New York: Free Press.
- Coyne, Christopher J., and Peter T. Leeson. 2004. "Who's to Protect Cyberspace?" [http://www.peterleeson.com/Who\\_s\\_to\\_Protec\\_Cyberspace.pdf](http://www.peterleeson.com/Who_s_to_Protec_Cyberspace.pdf).
- Craven, Samantha, Sarah Brown, and Elizabeth Gilchrist. 2006. "Sexual Grooming of Children: Review of Literature and Theoretical Considerations." *Journal of Sexual Aggression* 12, no. 3: 287–99.
- Creswell, John W. 2009. *Research Design: Qualitative, Quantitative, and Mixed-Methods Approaches*. Thousand Oaks, CA: SAGE Publications.
- Crisan, I. 2010. "The principles of legality 'nullum crimen sine lege, nulla poena sine lege; and their role.'" *Effectius Newsletter*, 5.
- Cross, Frank B. 2005. "Law and Trust." *Georgetown Law Journal* 93, no. 5: 1461–543. <http://ssrn.com/abstract=813028>.
- Cross, Cassandra. 2019. "Oh we can't actually do anything about that: The problematic nature of jurisdiction for online fraud victims." *Criminology and Criminal Justice*: 1–18 (March 13, 2019): online. <https://doi.org/10.1177/48895819835910>.
- Cross, Cassandra, Russell G. Smith, and Kelly Richards. 2014. "Challenges of Responding to Online Fraud Victimization in Australia. *Trends and Issues in Crime and Criminal Justice*. 474, (May): 1–6. <https://aic.gov.au/publications/tandi/tandi474>.

- Cyveillance. 2010. "Clamping Down on American Companies That Assist Cybercrime." August 13, 2010. <https://www.lookingglasscyber.com/blog/threat-intelligence-insights/clamping-down-on-american-compaines-that-assist-cybercrime>.
- Dai, Yue, Soo Yun Shin, Nicole Kashian, Jeong-woo Jang, and Joseph B. Walther. 2016. "The Influence of Responses to Self-Disclosure on Liking in Computer-Mediated Communication." *Journal of Language and Social Psychology* 35 no. 4: 394–411.
- Daniel, Michael. 2017. White House Cybersecurity Coordinator for President Obama. Interview by Christine W. Lyons, January 13, 2017.
- DARKOWL. 2016. "Darknet Series: What is the Darknet?" Accessed October 22, 2016. <https://www.darkowl.com/what-is-the-darknet/>.
- Davies, Caroline. 2014. "Welcome to DarkMarket—Global One-Stop Shop for Cybercrime and Banking Fraud." *The Guardian*, January 14, 2014. <http://www.theguardian.com/technology/2012/jan/14/darkmarket-online-fraud-trial-wembley>.
- Decary-Hetu, David, and Benoit Dupont. 2012. "The Social Network of Hackers." *Global Crime* 13, no. 3: 160–75.
- Decary-Hetu, David, Carlo Morselli, and Stephane Leman-Langlois. 2011. "Welcome to the Scene: A Study of Social Organization and Recognition among Warez Hackers." *Journal of Research in Crime and Delinquency* 49, no. 3: 359–82.
- Deem, D. L. 2000. "Notes from the Field: Observations in Working with the Forgotten Victims of Personal Financial Crimes." *Journal of Elder Abuse & Neglect* 12, no. 2: 33–48.
- DeLiema, Marguerite, Martha Deevy, Annamaria Lusardi, and Oliva S. Mitchell. 2018. "Financial Fraud Among Older Americans: Evidence and Implications." *The Journals of Gerontology Series B, Psychological Sciences and Social Sciences*: December: doi:10.1093/geronb/gby151.
- Demirdjian, Z. S., and Zara Mokatsian. 2015. "The Cost of Cyber Crimes to Business and Society." *Proceedings of the American Society of Business and Behavioral Sciences*, 22, no. 1: 104–9.
- Dempsey, David. 2008. "The Path to Social Justice Goes Through Politics and Economics." *Journal of Policy Process* 7, no. 2–3: 94–105. <https://doi.org/10.1080/15588740801937888>.
- Denzin, Norman K. 2001. *Interpretive Interactionism*. 2nd ed. Thousand Oaks, CA: Sage.
- Department of Homeland Security. 2017. "U.S. Immigration and Customs Enforcement Child Exploitation Investigation Unit." Accessed February 5, 2017. <https://www.ice.gov/predator>.

- DHHS (Department of Health and Human Services). 1978. *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. <https://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>.
- \_\_\_\_\_. 1992. *Report from the Secretary's Task Force on Elder Abuse*. <http://aspe.hhs.gov/daltcp/reports/elderab/htm>.
- \_\_\_\_\_. 1997. *Privacy and Health Research. Privacy, Confidentiality, Security* <http://aspe.hhs.gov/report/privacy-and-health-reseasrch/privacy-confidentiality-security>
- \_\_\_\_\_. 2009. *Federal Policy for the Protection of Human Subjects ("Common Rule")*. June 3, 2009. <http://hhs.gov/ohro/regulations-and-policy/regualtions/common-rule/index.html>.
- \_\_\_\_\_. 2010. *Congressional Report on the Feasibility of Establishing a Uniform National Database on Elder Abuse*. Washington, DC: DHSS.
- \_\_\_\_\_. 2014. *Elder Justice Coordinating Council 2012–2014 Report to Congress*. DHHS Administration for Community Living. [http://www.oao.acl.gov/AoA\\_Programs/Elder\\_Rights/EJCC/Meetings/2016-04-27](http://www.oao.acl.gov/AoA_Programs/Elder_Rights/EJCC/Meetings/2016-04-27).
- \_\_\_\_\_. 2017. Food and Drug Administration (FDA), Center for Drug Evaluation and Research (CDER) 2017. *Repackaging of Certain Human Drug Products by Pharmacies and Outsourcing Facilities Guidance for Industry*. Washington, DC: Food and Drug Administrations. <http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidance/default.htm>.
- Dinstein, Yoram. 1985. "International Criminal Law." *Israel Law Review* 20, no. 2–3: 206–42.
- Divita, David. 2012. "Online in Later Life: Age as a Chronological Fact and a Dynamic Social Category in an Internet Class of Retirees." *Journal of Sociolinguistics* 16, no.5: 585–612.
- DOJ (Department of Justice) v. Reporters Comm. For Free Press 489 US 749 (1989).
- \_\_\_\_\_. 2015. *Financial Crime Fraud Victims*. <http://www.justice.gov/usao-wdwa/victim-witness/victim-info/fiancial-fraud>.
- \_\_\_\_\_. 2016. "The United States Attorney's Office Western District of Washington." Accessed October 1, 2016. <https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud>.

- \_\_\_\_\_. 2018a. "Justice Department Coordinates Nationwide Elder Fraud Sweep of More Than 250 Defendants." February 22, 2018.  
<https://www.justice.gov/opa/pr/justice-department-coordinates-nationwide-elder-fraud-sweep-more-than-250-defendants>.
- \_\_\_\_\_. 2018b. "Seven Individuals Sentenced to Prison in Multi-Million Dollar International Money Laundering Conspiracy." June 1, 2018  
<https://www.justice.gov/usao-sdfl/pr/seven-individuals-sentenced-prision-multi-million-dollar-international-money-laundering>
- Drozdenko, Ronald G., and Perry D. Drake. 2002. *Optimal Database Marketing: Strategy, Development, and Data Mining*. Thousand Oaks, CA: Sage.
- Duhigg, Charles. 2007. "Bilking the Elderly, with a Corporate Assist." *The New York Times*, May 20, 2007.  
[http://www.nytimes.com/2007/05/20/business/20tele.html?\\_r=0](http://www.nytimes.com/2007/05/20/business/20tele.html?_r=0).
- Eagleman, David. 2015. *The Brain: The Story of You*. New York: Vantage Books.
- Easton, Stephen T., and Alexander K. Karaivanov. 2009. "Understanding Optimal Criminal Networks." *Global Crime* 10, no. 1–2: 41–65.
- Edwards, Matthew, Guillermo Suarez-Tangil, Claudia Peersman, Gianluca Stringhini, Awais Rashid, and Monica Whitty. 2018. "The Geography of Online Dating Fraud." Presented at Workshop on Technology and Consumer Protection, San Francisco. <https://researsrch-information.bristol.ac.uk/files/152062431/geoscammy.pdf>.
- Ekman, Paul. 1988. "Telling Lies: Clues to Deceit in the Marketplace." In *Self-Deception: An Adaptive Mechanism*, edited by Joan S. Lockard and Delroy L. Paulhus, 229–50. Englewood Cliffs, NJ: Prentice Hall.
- Ekman, Paul. 1991. *Telling Lies*. New York: W.W. Norton.
- Ekman, Paul, and Mark G. Frank. 1993. "Lies That Fail." In *Lying and Deception in Everyday Life*, edited by Lewis M. and C. Saarni, 184–200. New York: Guilford Press.
- Emile, Melanie, Fabienne d'Arripe-Longueville, Boris Cheval, Massimiliano Amato, and Aina Chalabaev. 2015. "An Ego Depletion Account of Aging Stereotypes' Effect on Health-Related Variables." *The Journal of Gerontology*. 70, no. 6: 876–85.
- Equifax. 2017. "Cybersecurity Incident & Important Consumer Information." October 2, 2017. <https://www.equifaxsecurity2017.com>.
- Degli-Esposti, Sara. 2014. "When big data meets dataveillance: The hidden side of analytics." *Surveillance and Society*. 12, no. 2: 209–225.  
<https://doi.org/10.24908/SS.V12I2.5113>.

European Cybercrime Center. 2018. *Internet Organised Crime Threat Assessment 2018*.  
Europol, European Union Agency for Law Enforcement Cooperation.

Facebook, Inc. v. Power Venues, Inc. 16-1105 (9<sup>th</sup> Cir. 2017).

Facebook. 2019. *Consumer Privacy User Profile Litigation 2019*. <https://cand.uscourts.gov/judges/chhabria-vince-vc/in-re-facebook-inc-consumer-privacy-user-profile-litigation>

Facebook. 2019. “Terms of Service.” <https://www.facebook.com/terms.php>  
(Accessed November 19, 2019).

FBI (Federal Bureau of Investigation). 2016. “Organized Crime.” November 30, 2016.  
<http://www.fbi.gov/hq/cid/orgcrime/glossary.htm>.

Fogg, Brian J. 1997. “Charismatic Computers: Creating More Likable and Persuasive Interactive Technologies by Leveraging Principles from Social Psychology.” PhD diss., Stanford University.

\_\_\_\_\_. 1998. “Persuasive Computers: Perspectives and Research Directions.” In *Proceedings of the CHI '98 Conference on Human Factors in Computing Systems*, (January) 225–32. <https://doi.org/10.1145/274644.274677>.

\_\_\_\_\_. 2003. *Persuasive Technology: Using Computers to Change What We Think and Do*. New York: Morgan Kaufmann.

\_\_\_\_\_. n.d. “Home page.” Accessed May 2019. <http://captoloty.stanford.edu/>.

Forward, Joe. 2016. “No Love for Skillful Fraudster Who Preyed on Elderly through Romance Scams.” *State Bar of Wisconsin*, June 10, 2016.  
<https://www.wisbar.org/NewsPublications/Pages/General-Article.aspx?ArticleID=24885>.

Fowler, Geoffrey. 2019. “Alexa Has Been Eavesdropping on You This Whole Time.” *Washington Post*, May 6, 2019.  
<https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time>.

\_\_\_\_\_. 2019. “It’s the Middle of the Night. Do You Know Who Your iPhone is Talking to?” *Washington Post*.  
[https://www.washingtonpost.com/technology/20190528/its-middle-night-do-you-know-who-your-iphone-is-talking?utm\\_term=.b6fc2f1a88c9](https://www.washingtonpost.com/technology/20190528/its-middle-night-do-you-know-who-your-iphone-is-talking?utm_term=.b6fc2f1a88c9).

Frankfort-Nachmias, Chava, and David Nachmias. 2000. *Research Methods in the Social Sciences*. 6th ed. New York: Worth.

- Franklin, Jason, and Vern Paxson. 2007. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 375–388. Alexandria, VA: ACM. <https://doi.org/10.1145/1315245.1315292>.
- Frederickson, H. George. 2008. "Toward a New Public Administration." In *Classics of Public Administration*, edited by Jay M. and Albert C. Hyde Shafritz, 296–307. Boston: Wadsworth.
- Freedman, Jonathan L., and Scott C. Fraser. 1966. "Compliance without Pressure: The Foot-in-the-Door Technique." *Journal of Personality and Social Psychology* 4, 2: 195–202.
- Friedman, Thomas L. 2016. *Thank You for Being Late*. New York: Picador.
- Friend, Karen, and David Levy. 2001. "Reductions in Smoking Prevalence and Cigarette Consumption Associated with Mass-Media Campaigns." *Health Education Research* 17, no. 1: 85–98.
- FTC (Federal Trade Commission). 2011. "Consumer Confidence in Internet Marketplace Depends on Privacy Protections FTC Tells Senate Commerce Committee." June 29, 2011. <http://www.ftc.gov/opa/2011/06/privacytestimony.shtm>.
- . 2011. "FTC Testifies on Data Security." May 4, 2011. <http://www.ftc.gov/opa/2011/05/security.shtm>.
- . 1996. "Consumer Privacy in the Information Age: A view from the United States." <http://www.inquiresjournal.com/articles/1450/the-right-to-privacy-in-a-digital-age-reinterpreting-the-concept-of-personal-privacy>.
- . 2019. "FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. July 24. <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.
- Fuchs, Christian. 2017. *Social Media: A Critical Introduction*. 2nd ed. London: Sage.
- Funk, McKenzie. 2016. "The Secret Agenda of a Facebook Quiz." *The New York Times*, November 19, 2016. <https://www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html>.
- GAO (Government Accountability Office). 1991. *Elder Abuse: Effectiveness of Reporting Laws and Other Factors*. HRD-74 <http://www.gao.gov/products/HRD-91-71>.
- . 2011. *Elder Justice: Stronger Federal Leadership Could Enhance National Response to Elder Abuse*. GAO-11-208. <http://www.gao.gov./products/GAO-11-208>.

- . 2013. *Elder Justice: More Federal Coordination and Public Awareness Needed*. <http://www.gao.gov/assets/660/655820.pdf>.
- GAO. 2017. *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. GAO-18-559. Washington, DC: GAO.
- GAO. 2018. *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. Washington, DC: GAO. <https://www.gao.gov/products/GAO-18-559>.
- Gaus, John M. 1947. *Reflections on Public Administration*. Birmingham: The University of Alabama Press.
- Gennep, Arnold Van. 1960. *The Rites of Passage*. Chicago, IL: University of Chicago.
- George Mason University. “IRC (Internet Relay Chat)” University of George Mason 2019. <http://mason.gmu.edu/%7Emontecin/IRC.html>.
- Gillen, Martina. 2012. “Lawyers and Cyberspace: Seeing the Elephant?” *A Journal of Law, Technology and Society* 9, no. 2: 130–47. <https://doi.org/10.2966/script.0890212.130>.
- Glennan, Stuart S. 1996. “Mechanisms and the Nature of Causation.” *Erkenntnis* 44, no. 1: 49–71.
- Glenny, Misha. 2009. “McMafia: A Journey Through the Global Criminal Underworld.” Wilson Center. April 17, 2008. <http://www.wilsoncenter.org/event/imcmcia-journey-through-the-global-underworld>.
- Goggin, Malcolm L., Ann O. Bowman, James P. Lester, and Laurence J. O’Toole Jr. 1990. *Implementation Theory and Practice: Toward a Third Generation*. Glenview, IL: Scott Foresman/Little, Brown Higher Education.
- Golle, Philippe. 2006. “Revisiting the Uniqueness of Simple Demographics in the US Population.” Paper presented at the ACM Workshop on Privacy in the Electronic Society, New York, October 2006. <https://www.parc.com/publication/1713/revisiting-the-uniqueness-of-simple-demographics-in-the-us-population.html>.
- Gonzalez, Roberto. 2017. “Hacking the Citizenry? Personality Profiling, ‘Big Data’ and the Election of Donald Trump.” *Anthropology Today* 33, no. 3: 9–12. <http://doi.org/10.1111.1467-8322.12348>.
- Goodman, Marc. 2015. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York: Anchor Books.

- Goodwin, Gretta L., and Jenny Grover. 2019. *Elder Justice: Goals and Outcome Measures Would Provide DOJ with Clear Direction and a Means to Assess its Efforts*. Report to Congress, Washington, DC: Government Accountability Office.
- Grabosky, Peter. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies* 10, no. 2: 243–49.
- Grauer, Yael. 2018. "What Are 'Data Brokers,' and Why Are They Scooping Up Information about You?" *Motherboard*, March 27, 2018. [https://motherboard.vice.com/en\\_us/article/bjp3w/what-are-data-brokers/](https://motherboard.vice.com/en_us/article/bjp3w/what-are-data-brokers/).
- Greenwald, Ted. 2014. "How Facebook and Candy Crush Got You Hooked." *Wired*, December 23, 2014. <https://www.wired.com/2014/12/how-to-build-habit-forming-products>.
- Greenwood, Shannon, Andrew Perrin, and Maeve Duggan. 2016. "Social Media Update 2016." Pew Research Center Internet, Science and Tech. November 11, 2016. <http://www.pewinternet.org/2016/11/11/social-media-update-2016>.
- Griffin, E. M., and Andrew Ledbetter. 2012. *A First Look at Communication Theory*. 9th ed. New York: McGraw Hill.
- Gross, Doug. 2011. "'Mafiaboy' Breaks Silence Paints 'Portrait of a Hacker.'" *CNN Tech*, August 15, 2011. <http://www.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/>.
- Hadnagy, Christopher. 2011. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley.
- Hakmeh, Joyce. 2017. "Cybercrime and the Digital Economy in the GCC Countries." Research paper, The Royal Institute of International Affairs, Chatham House, London. <https://www.chathamhouse.org/event/cybercrime-and-digital-economy-gcc-countries>.
- Hale, Nathan. 2008. "7 Fla. Residents Sentenced For Money-Laundering Plot." Law360, June 1, 2018. <https://www.law360.com/articles/1049326>.
- Hallinan, Joseph T. 2009. *Why We Make Mistakes*. New York: Broadway Books.
- Hannigan, Robert. 2017. "Criminal Cyber Gangs are Disrupters in the Digital Economy." *Financial Times*, August 3.
- Hanser, Robert D. 2011. "Gang-Related Cyber and Computer Crimes: Legal Aspects and Practical Points of Consideration in Investigations." *International Review of Law, Computers and Technology* 25, no. 1–2: 47–55.

Haque, Akhlaque. 2015. *Surveillance, Transparency, and Democracy: Public Administration in the Information Age*. Tuscaloosa: The University of Alabama Press.

Harmon, Elliot. 2018. "FOSTA Would Be a Disaster for Online Communities." *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2018/02/fosta-would-be-disaster-online-communities>.

Harris, Tristan. 2016. "How Technology Hijacks People's Minds—from a Magician and Google's Design Ethicist." <http://www.tristanharris.com/essays>.

Haselton, Martie G., Daniel Nettle, and Paul W. Andrews. 2005. "The Evolution of Cognitive Bias." In *The Handbook of Evolutionary Psychology*, edited by David M. Buss, 724–46. Hoboken, NJ: Wiley.

Haury, Amanda C. 2012. "10 Most Costly Computer Viruses of All Time." Investopedia. May 24, 2012. <http://www.investopedia.com/financial-edge/0512/10-of-the-most-costly-computer-viruses-of-all-time.aspx>.

Herley, Cormac. 2012. "Why Do Nigerian Scammers Say They Are from Nigeria?" Microsoft Research. June 20, 2012. <http://research.microsoft.com/pubs/167719/Whyfromnigeria.pdf>.

Hern, Alex, and Carole Cadwalladr. 2018. "Revealed: Aleksandr Kogan Collected Facebook Users' Direct Messages." *The Guardian*, April 13, 2018. <https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages>.

HEW (Department of Health, Education and Welfare). 1961. *The Nation and Its Older People, Report of the White House Conference on Aging January 9–12, 1961*. Washington, DC: HEW, Special Staff on Aging.

Hill, Claire A., and Erin Ann O'Hara. 2006. "A Cognitive Theory of Trust." *Washington Law Review* 87 (7): 1717–96. [http://openscholarship.wustl.edu/law\\_lawreview/vol84/iss7/4](http://openscholarship.wustl.edu/law_lawreview/vol84/iss7/4).

Hill, John L. 1994. "Exploitation." *Cornell Law Review* 79, no. 3: 631–99.

HIPAA Journal. 2018. "Security Breaches in Healthcare in the Last Three Years." March 18, 2018. <http://hippajournal.com>.

*HiQ Labs v. LinkedIn Corp.* F. 11 (9<sup>th</sup> Cir. 2019)

Hollis, Duncan B. 2011. "An e-SOS for Cyberspace." *Harvard International Law Journal*, 52, no. 2: 392–93.

- Hollis-Peel, Meghan, Danielle Reynald, Maud van Bavel, Henk Elffers, and Brandon Welsh. 201. "Guardianship for crime prevention: a critical review of the literature." *Crime Law Social Change* 56, (May): 53-70. <https://doi.org/10.1007/s10611-011-9309-2>.
- Holt, Thomas 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, Thomas J. 2005. "Hack, Cracks, and Crime: An Examination of the Subculture and Social." PhD diss., University of Missouri, St. Louis.
- Holt, Thomas J. 2013. "Exploring the Social Organisation and Structure of Stolen Data Markets." *Global Crime* 14, no. 2–3: 155–174.
- Holt, Thomas J., and Max Kilger. 2012. "Know Your Enemy: The Social Dynamics of Hacking." The HoneyNet Project. May 28, 2012. <http://www.honeynet.org>.
- Holt, Thomas, Deborah Strumsky, Olga Smirnova, and Max Kilger. 2012. "Examining the Social Networks of Malware Writers and Hackers." *International Journal of Cyber Criminology* 6, no. 1: 891–903.
- House, James S. 2001. "Social Isolation Kills, But How and Why." *Psychosomatic Medicine* 63, no. 2: 273–274. <https://doi.org/10.1097/00006842-2000103000-00011>.
- Howard, John D. 1997. *An Analysis of Security Incidents on the Internet 1989–1995*. PhD diss., Carnegie Mellon University, Pittsburg, PA.
- Hudak, Steve. 2017. "FinCEN Fines Western Union Financial Services, Inc. for Past Violations of Anti-Money Laundering Rules in Coordinated Action with DOJ and FTC." January 19, 2017. Washington, DC: FinCEN..
- Hueler, Kelli Hustad. 2010. "The Retirement Income Challenge: Making Savings Last a Lifetime." Hueler Companies Written Statement for the Record Senate Special Committee on Aging United States Congress. June 16, 2010. <http://aging.senate.gov/events/hr222kh.pdf>.
- Hutchings, Alice, and Hennessey Hayes. 2009. "Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?" *Current Issues in Criminal Justice* 20, no. 3: 433–451.
- IC3 (Internet Crime Complaint Center). 2008. *Internet Crime Report*. [https://pdf.ic3.gov/2008\\_IC3Report.pdf](https://pdf.ic3.gov/2008_IC3Report.pdf).
- . 2009. *2008 Internet Crime Report*. [https://pdf.ic3.gov/2009\\_IC3Report.pdf](https://pdf.ic3.gov/2009_IC3Report.pdf).

- \_\_\_\_\_. 2010. *2009 Internet Crime Report*. February 24, 2010.  
<http://www.ic3.gov/media/annualreport>.
- \_\_\_\_\_. 2011. *2010 Internet Crime Report*. February 24, 2011. <http://www.ic3.gov>.
- \_\_\_\_\_. 2012. *2011 Internet Crime Report*.  
[http://www.ic3.gov/media/annualreport/2011\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf).
- \_\_\_\_\_. 2013. *2012 Internet Crime Report*.  
[http://www.ic3.gov/media/annualreport/2012\\_ic3Report.pdf](http://www.ic3.gov/media/annualreport/2012_ic3Report.pdf).
- \_\_\_\_\_. 2014. *2013 Internet Crime Report*. <https://pdf.ic3.gov>.
- \_\_\_\_\_. 2015. *2014 Internet Crime Report*. September 24, 2015. <http://ic3.gov>.
- \_\_\_\_\_. 2016. *2015 Internet Crime Report*. Washington, DC: Department of Justice.  
<https://www.ic3.gov/about/default.aspx>.
- \_\_\_\_\_. 2017. *2016 Internet Crime Report*. <https://pdf.ic3.gov>.
- \_\_\_\_\_. 2018. *2017 Internet Crime Report*. Washington, DC: Federal Bureau of Investigation.
- \_\_\_\_\_. 2019. *Internet Crime Report 2018*. <https://www.ic3.gov/meida/annualreports>.
- Iffat, Rabia, and Lalitha K. Sami. 2010. “Understanding the Deep Web.” Library Philosophy and Practice. May 2010.  
<http://www.webpages.uidaho.edu/~mbolin/iffat-sami.htm>.
- Interpol. 2016. “Social Engineering Fraud.” August 1, 2016.  
<http://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud>.
- Iowa. 2005. “State of Iowa v Walter Karl, Inc.: Application for Order Enforcing Attorney General’s Civil Investigative Demand.” March 2, 2005. Polk County, IA: Iowa District Court.
- Ito, Tiffany A., Jeff T. Larsen, N. Kyle Smith, and John T. Cacioppo. 1998. “Negative information weighs more heavily on the brain: The negativity bias in evaluative categorizations.” *Journal of Personality and Social Psychology* 75, no. 4: 887–900.
- Jackman, Tom 2018. “House passes anti-online sex trafficking bill, allows targeting of websites like Backpage.com.” *The Washington Post*. (Februaray 27, 2018):  
<https://www.washingtonpost.com/news/true-crime/wp/hous-passes-anti-online-sex-trafficking-bill/>
- James, Bryan D., Patricia A. Boyle, and David A. Bennett. 2014. “Correlates of Susceptibility.” *Journal of Elder Abuse and Neglect* 26, no. 2: 107–22.

- Jehiel, Philippe, and David Ettinger. 2005. "Towards a Theory of Deception." *PSE Working Papers n2005-28*. halshs-00590767. <https://halshs.archives-ouvertes.fr/halshs-00590767>.
- JND. 2019. "Equifax Data Breach Settlement." November 14, 2019. <http://equifaxbreachsettlement.com>.
- Juniper Research. 2015. "Cybercrime Cost Businesses over 2 Trillion." *Juniper Research*. May 5, 2015. <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>.
- Kahneman, Daniel. 1982. *Judgment Under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.
- Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. New York: Farrar, Straus, and Giroux.
- Kahneman, Daniel, and Amos Tversky. 1979. "Prospect Theory: An Analysis of Decision Under Risk." *Econometrica* 47, no. 2: 263–292.
- Kahneman, Daniel, and Amos Tversky. 1982. "The Psychology of Preferences." *Scientific American*, 246, no. 1: 160–173.
- Kanell, Michael E. 2018. "A year after data breach: Atlanta-based Equifax unbowed." *PHYS.ORG*, August 1. 2018. <https://phys.org/news/2018-08-year-breach-atlanta-based-equifax-unbowed.html201>.
- Kaplan, Andreas M., and Michael Haenlein. 2009. "Users of the World, Unite! The Challenges and Opportunities of Social Media." *Business Horizons*, September 3, 2009, 61.
- Kaplan, Peter 2018. "Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Practices." Federal Trade Commission (March 26, 2018): <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>.
- Kaufman, Roger, Hugh Oakley-Brown, Ryan Watkins, and Doug Leigh. 2003. *Strategic Planning for Success: Aligning People Performance, and Payoffs*. San Francisco: Wiley.
- Kerley, Kent and Heith Copes. 2002. "Personal Fraud Victims and Their Official Responses to Victimization." *Journal of Police and Criminal Psychology*, 17, no. 1: 19-35.
- Kerr, Orin S. 2009. "The Case for the Third-Party Doctrine." *Michigan Law Review*, 107, no. 4: 561-602.

- Kiel, Joan. 2005. "The Digital Divide: Internet and E-mail Use by the Elderly." *Medical Informatics & the Internet in Medicine* 30, no. 1: 19-23.
- Kigerl, Alex C. 2018. "Email Spam Origins: Does the CAN SPAM Act Shift Spam Beyond the United States Jurisdiction?" *Trends in Organized Crime* 21, no. 1: 62-78.
- King, Kevin. 2017. "The 115th Congress is Among the Oldest in History." Accessed June 28, 2017. <https://blog.quorum.us/the-115th-congress-is-among-the-oldest-in-history-1>.
- Kirkpatrick, Robert. 2013. "A New Type of Philanthropy: Donating Data." Harvard Business Review. Accessed June 30, 2016. <https://hbr.org/2013/036/a-new-type-of-philanthropy-don>.
- Konnikova, Maria. 2016. *The Confidence Game: Why We Fall for It...Every Time*. New York: Penguin Books.
- Kochman, Ben. 2019. "Equifax To Pay Up to \$700M To Settle Data Breach Probes." *LAW360* July 22, 2019. Accessed September 3, 2019. <https://www.law360.com/articles/1180467/equifax-to-pay-up-to-700m-to-settle-data>.
- Koop, C. Everett. 1985. "Call for a Smoke-free Society." *Pediatric Pulmonology* 1, no. 1: 4-5.
- Koop, C. Everett. 1989. *Reducing the Health Consequences of Smoking: 25 Years of Progress: A Report of the Surgeon General*. Washington, D.C.: National Institutes of Health.
- Kramer, Andrew E. 2013. "Technology: Online Attack Leads to Peek into Spam Den." *New York Times*, September 9, 2013. <http://www.nytimes.com/2013/09/03/business/global/online-attack-leads-to-peek-into-spam-den.html>.
- Krebs, Brian. 2014. *Spam Nation*. Naperville: Sourcebooks, Inc.
- Krebs, Brian. 2015. "Inside Target Corp. Days After 2013 Breach." Krebs on Security. Accessed December 20, 2015. <https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/>.
- Krebs, Dennis L. 1975. "Empathy and Altruism." *Journal of Personality and Social Psychology* 32, no. 6: 1134-1146.
- Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Stuart H. Starr, Larry K. Wentz, and Frank D. Kramer, 24-42. Washington, DC: National Defense University Press.

- Kumar, Mohit. 2018. "15-Year-Old Schoolboy Posed as CIA Chief to Hack Highly Sensitive Information." *The Hacker News: Security in a Serious Way*. Accessed January 31, 2018. <https://thehackernews.com/2018/01/crackas-with-attitude-hacker.html>.
- Lachs, Mark, Christianna Williams, Shelley O'Brien, Karl Pillemer, and Mary Charlson. 1998. "The Mortality of Elder Mistreatment." *Journal of the American Medical Association* 280, no. 5: 428-432.
- Lachs, Mark and Jacqueline Berman. 2011. *Under the Radar: New York State Elder Abuse Study*. Weill Cornell Medical Center of Cornell University and New York City Department for the Aging, Rochester: Lifespan of Greater Rochester, Inc. Accessed May 20, 2015. [www.ocfs.state.ny.us/main/reports/UndertheRadar051211finalreport.pdf](http://www.ocfs.state.ny.us/main/reports/UndertheRadar051211finalreport.pdf).
- Lahtiranta, Janne, and Kai Kimppa. 2006. "Elderly People and Emerging Threats of the Internet and New Media." *International Federation of Information Processing* 226:13-21. Edited by R. Suomi, R. Cabral, J.F. Hampe, A. Heikkila, J. Jarvelaninen, and E. Koskivaara. Accessed November 29, 2011. [https://link.springer.com/chapter/10.1007/978-0-387-39229-5\\_2](https://link.springer.com/chapter/10.1007/978-0-387-39229-5_2).
- Lea, Stephen, Peter Fischer, and Kath M. Evans. 2009. *The Psychology of Scams: Provoking and Committing Errors of Judgement*. London: Office of Fair Trading.
- Lebo, Harlan. 2016. "The Digital Future Report." USC Annenberg School Center for the Digital Future. Accessed February 10, 2017. <https://www.digitalcenter.org>.
- Leonard, Mike. 2019. "Zuckerberg Sued Over Privacy Scandals, Alleged Insider Trades." Bloomberg Law Securities Law News. Accessed May 2, 2019. <https://news.bloomberg.com/securities-law/facebook-zuckerberg-sued-over-scandals-alleged-insider-trades>.
- Leslie, Ian. 2016. "The Scientists Who Make Apps Addictive." The Economist. Accessed January 2019. <https://www.1843magazine.com/features/the-scientists-who-make-apps-addictive>.
- Lessig, Lawrence. 2006. *Code 2.0*. 2<sup>nd</sup> ed. New York: Basic Books.
- Levy, David T., Karen Friend, Harold Holder, and Maria Carmona. 2001. "Effect of Policies Directed at Youth Access to Smoking: Results from the SimSmoke Computer Simulation Model." *Tobacco Control* 10, no. 2: 108 - 116.
- Lewis, Scott. 2018. "Who Actually Owns Your Data: Cloud Computing Data Security." Winning Technologies. Accessed May 20, 2019. <https://winningtech.com/who-actually-owns-your-data>.

- Li, Xiaoyan. 2010. "Extending the Working Lives of Older Workers: The Impact of Social Security Policies and Labor Market." PhD diss., Pardee RAND Graduate School.
- Li, Ye, Jie Gao, A. Zeynep Enkavi, Lisa Zaval, Elke U. Weber, and Eric J. Johnson. 2015. "Sound Credit Scores and Financial Decisions Despite Cognitive Aging." *Proceedings of the National Academy of Sciences* 112, no. 1: 65-69.
- Licklider, J. and Robert Taylor. 1968. "The Computer as a Communication Device." *Science and Technology* (April) 21-41.
- Linberg, Brian W., Charles P. Sabatino, and Robert B. Blancato. 2011. "Bringing National Action to a National Disgrace: The History of the Elder Justice Act." *NAELA Journal* 7, no. 1 (March): 105-124. Accessed March 31, 2014. <https://www...>
- Lodder, Arno R. 2013. "Ten Commandments of Internet Law Revisited: Basic Principles for Internet Lawyers." *Information and Communications Technology Law* 22, no. 3: 264-276. Accessed December 4, 2017. <http://dx.doi.org/10.1080/13600834.2013.852769>.
- Long, Johnny. 2008. *Hacking Guide to Social Engineering*. Burlington, MA: Syngress Publisher, Inc.
- Lormel, Dennis M. 2001. *Hearing on Swindlers, Hucksters and Snake Oil Salesmen: The Hype and Hope of Marketing Anti-Aging Products to Seniors*. Testimony before United States Senate Special Committee on Aging, Chief, Financial Crimes Section, Washington, DC: Federal Bureau of Investigation. Accessed July 3, 2016. <http://www.quackwatch.org/01QuackeryRelatedTopics/Hearing/fbi.html>.
- Lovett, Guillaume. 2007. How Cybercrime Operations Work and Why They Make Money. Accessed December 3, 2014. <http://www.out-law.com/page-7791>.
- Lovett, Kimberly M. and Timothy K. Mackey. 2013. "Online Threats to Senior Safety: The Direct-To-Consumer Medical Marketplace and Elder Abuse." *NAELA Journal* 9, no. 1: 91-113.
- Lu, Yong, Xin Luo, Michael Polgar, and Yuanyuan Cao. 2010. "Social Network Analysis of a Criminal Hacker Community." *Journal of Computer Information Systems* 51, no. 2: 31-41.
- Lukasik, Stephen J. 2011. "Protecting Users of the Cyber Commons." *Communications of the Association for Computing Machinery* 54, no. 9: P54-61. doi: 10.1145/1995376.1995393.

- Lusardi, Annamaria. 2012. "Financial Literacy and Financial Decision-Making in Older Adults: An Economist's Look at the Level of Financial Knowledge Among Elders and the Quality of Their Financial Decisionmaking." *Journal of the American Society on Aging* 26, no. 2 (June): 25-32.
- Lusthaus, Jonathan. 2013. "How Organised is Organised Cybercrime?" *Global Crime* 14, no. 1: 52-60.
- Lusthaus, Jonathan. 2012. "Trust in the World of Cybercrime." *Global Crime* 13, no. 2: 71-94.
- Luton, Larry S. 2010. *Qualitative Research Approaches for Public Administration*. New York: M.E. Sharpe, Inc.
- MacInnis, Deborah J. and Hae Eun Chun. 2007. *Understanding Hope and its Implications for Consumer Behavior: I hope, Therefore I Consume*. Hanover, MA: Now Publishers, Inc.
- Macknik, Stephen L., Susana Martinez-Conde, and Sandra Blakeslee. 2011. *Sleights of Mind: What the Neuroscience of Magic Reveals About Our Everyday Deceptions*. New York: Picador.
- Mallinson, Daniel J. and Peter K. Hatemi. 2018. "The Effects of Information and Social Conformity on Opinion Change." Public Library of Science ONE. Accessed May 3, 2019. <https://doi.org/10.1371/journal.pone.0196600>.
- Mann, David and Mike Sutton. 1998. "Netcrime." *Oxford Journal* 38, no. 2: 201-229.
- Marriott. 2018. "Marriott Announces Starwood Guest Reservation Database Security Incident." *U.S. Securities and Exchange Commission*. Accessed June 30, 2018. <https://www.sec.gov/Archives/edgar/data/104828/000162828018014745/a2018ex99.htm>.
- Martin, Kirsten. 2016. "Data Aggregators, Consumer Data, and Responsibility Online: Who is Tracking Consumers Online and Should They Stop?" *The Information Society* 32, no. 1: 51-63.
- Martin, Shannon E. 2003. "States Begin to Permit Web Posting for Legal Ads, Public Notices." *Newspaper Research Journal*. 24, no. 4: 112-117.
- Martin, Stevie. 2011. "Sovereignty and the Responsibility to Protect." *Griffith Law Review* 20, no. 1: 153-187.
- Martinez, Jennifer. 2013. "Pentagon: Chinese Government Hacking into US Computers." The Hill. Accessed November 16, 2014. <http://thehill.com/policy/technology/298153-pentagon-claims-chinese-government-behind-intrusions-on-us-computers>.

- Mason, Karen A. and Michael L. Benson. 1996. "The Effect of Social Support on Fraud Victim's Reporting Behavior: A Research Note." *Justice Quarterly* 13, no. 3: 511-524.
- Matsakis, Louise. 2019. "The WIRED Guide to Your Personal Data (and Who Is Using It)." WIRED. Accessed February 27, 2019. <https://www.wired.com/story/wired-guide-personal-data-and-who-is-using-it/>.
- Maurushat, Alana. 2010. "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?" *University of New South Wales Law Journal* 33, no. 2: 431-473.
- Maynard, Trevor and Nick Beecroft. 2015. "Business Blackout: The Insurance Implications of a Cyber-Attack on the U.S. Power Grid." Lloyd's of London. Accessed March 15, 2019. <https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blockout20150708.pdf>.
- Mazlish, Bruce. 1993. *The Fourth Discontinuity: The Coevolution of Humans and Machines*. New Haven: Yale University Press.
- Mazmanian, Daniel A. and Paul A. Sabatier. 1983. *Implementation and Public Policy*. Lanham: Scott, Foresman and Company.
- McDaniel, Darwin. 2019. "Rep. Jim Langevin Calls on Congress to Limit Committees with Cyber Oversight." Executive Gov. Accessed February 20, 2019. <https://www.executivegov.com/2019/01/rep-jim-langevin-calls-on-congress-to-limit-committees-with-cyber-oversight>.
- McDonough, John E. 2011. *Inside National Health Reform*. Los Angeles: University of California Press.
- McGuire, Mike and Samantha Dowling. 2013. *Cyber crime: A Review of the Evidence Research Report 75 Chapter 2*. London: Home Office Research Report. Accessed June 2016. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/450375/Cyber\\_crime\\_A\\_review\\_of\\_the\\_evidence\\_Chapter\\_2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450375/Cyber_crime_A_review_of_the_evidence_Chapter_2.pdf)
- McNamee, Roger. 2019. *Zucked: Waking Up to the Facebook Catastrophe*. New York: Penguin Press.
- Mead, Margaret. 1975. "A Reflection". Guest Speaker at Jacksonville University, Jacksonville, Florida. Author's notes.
- Melville, Herman. 2010. *The Confidence-Man: His Masquerade*. New Brunswick: Transaction Publishers.

- Merriam-Webster. 2016. "Social Media." Accessed July 30, 2016. [www.merriam-webster.com/dictionary/social media](http://www.merriam-webster.com/dictionary/social media).
- Meyer, Gordon K. 1989. "The Social Organization of the Computer Underground." Master Thesis, Northern Illinois University.
- Michalek, Gabriela, Georg Meran, Reimund Schwarze, and Özgür Yildiz. 2016. "Nudging as a New 'Soft' Policy Tool: An Assessment of the Definitional Scope of Nudges, Practical Implementation Possibilities and Their Effectiveness." *Economics* 18 (2016): 1-34. Accessed June 15, 2018. <http://www.economics-ejournal.org/economics/discussionpapers/2016-18>.
- Miles, Leonora. 2008. "The Hidden Toll." *Adults Learning* 19, no. 9 (May): 28-29.
- Milgram, Stanley. 1963. "Behavioral Study of Obedience." *Journal of Abnormal and Social Psychology* 67, no. 4: 371-328.
- Mishra, Sandeep and Laurence Fiddick. 2012. "Beyond Gains and Losses: The Effect of Need on Risky Choice in Framed Decisions." *Journal of Personality and Social Psychology* 102, no. 6: 1136-1147.
- Mishra, Sandeep, Margaux Gregson, and Martin L. Lalumiere. 2012. "Framing Effects and Risk-Sensitive Decision Making." *British Journal of Psychology* 103, no. 1: 83-97. doi: 10.1111/j.2044-8295.2011.02047.x.
- Mitnick, Kevin and William L. Simon. 2002. *The Art of Deception*. Indianapolis: Wiley Publishing, Inc.
- Modic, David and Stephen E.G. Lea. 2013. "Scam Compliance and the Psychology of Persuasion." SSRN. Accessed June 20, 2018. <https://ssrn.com/abstract=2364464>.
- Money. 2014. "Data Breach Tracker: All the Major Companies That Have Been Hacked." Money. Accessed December 20, 2015. <http://time.com/money/3528487/data=breach-identity-theft-jp-morgan-kmart-staples>.
- Mordock, Jeff. 2018. "Phony Homeland Security agents sentenced to prison for online dating scam." *The Washington Times*. April 5, 2018. Accessed November 3, 2019. <https://www.washingtontimes.com/news/2018/apr/5/phony-dhs-agents-sentenced-online-dating-scam/>.
- Morgan, Robert M. and Shelby D. Hunt. 1994. "The Commitment-Trust Theory of Relationship Marketing." *Journal of Marketing* 58 (July): 20-38.
- Morselli, Carlo. 2009. *Inside Criminal Networks*. Edited by Frank Bovenkerk. New York: Springer.

- Muscanell, Nicole L., Rosanna E. Guadagno, and Shannon Murphy. 2014. "Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams." *Social and Personality Psychology Compass* 8, no. 7 (July): 388-396.
- Nader, Ralph. 1966. *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*. New York: Grossman Publishers.
- Nagin, Daniel S. and Greg Pogorsky. 2001. "Integrating Celerity, Impulsivity and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence." *Criminology* 39 (4) (November): 865 - 892. doi:10.1111/j.1745-9125.2001.tb00943.x.
- NAPSA (National Adult Protective Services Association). 2014. *History: About Adult Protective Services from 1960 to 2000*. Accessed April 5, 2014.  
<http://www.napsa-now.org/about-napsa/history>.
- Narayanan, Arvind and Vitaly Shmatikov. 2010. "Viewpoints: Privacy and Security myths and Fallacies of 'Personally Identifiable Information.'" *Communications of the ACM* 53, no 6: 24-26.
- National Science Foundation. 2012. *Solicitation 12-499: Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA)*. Washington, DC: National Science Foundation. Accessed September 20, 2018.  
<http://www.nsf.gov/pubs/2012/nsf12499.pdf>.
- National Security Council. 2014. "Strategy to Combat Transnational Organized Crime: Definition." *National Security Council*. Accessed December 2, 2014.  
<http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/definition>.
- "National Security Presidential Directive 54/Homeland Security Presidential Directive 23." (CNCI/NSPD-54/HSPD-23) 2008. Federation of American Scientists. Accessed July 3, 2017. <https://fas.org/offdocs/nspd/nspd-54.pdf>.
- National White-Collar Crime Center. 2010. *National Public Survey on White Collar Crime*. Report. Fairmont: National White Collar Crime Center.
- National White-Collar Crime Center. 2012. National White Collar Crime Center. Accessed December 3, 2012. <http://www.nw3c.org>.
- NCEA (National Center on Elder Abuse). 1998. "The National Elder Abuse Incidence Study." The Administration for Children and Families and The Administration on Aging in The U.S. Department of Health and Human Services. Accessed November 10, 2013.  
[http://www.aoa.gov/AoARoot/AoA\\_Programs/Elder\\_Rights/docs/ABuseReport\\_Full.pdf](http://www.aoa.gov/AoARoot/AoA_Programs/Elder_Rights/docs/ABuseReport_Full.pdf).

- NCEA (National Center on Elder Abuse). 2013. "National Center on Elder Abuse Administration on Aging." Accessed May 3, 2013. <http://www.nces.aoa.gov>.
- . 2014. "National Center on Elder Abuse & Neglect at Irvine." Accessed March 15, 2014. [http://www.centeronelderabuse.org/NCEA\\_at\\_UCI.asp](http://www.centeronelderabuse.org/NCEA_at_UCI.asp).
- NCOA (National Council on Aging). 2016. "National Council on Aging Statistics and Facts." Accessed September 25, 2016. <https://www.ncoa.org/public-policy-action/elder-justice/elder-abuse-facts/#intraPagNav1>.
- NCPEA (National Committee for the Prevention of Elder Abuse). 2012. "Financial Abuse." Accessed October 12, 2012. <http://www.preventelderabuse.org>.
- NCSC (National Center for State Courts). 2019. "Justice Responses to Elder Abuse Online Course." Accessed February 5, 2019. <http://www.courses.ncsc.org>.
- NCVC (National Center for Victims of Crimes). n.d. *The National Center for Victims of Crime*. Accessed December 6, 2011. <http://www.ncvc.org>.
- Negroponte, Nicholas. 1995. *Being Digital*. New York: Vintage Books.
- Nelson, Todd D. 2002. *Ageism: Stereotyping and Prejudice Against Older Adults*. Cambridge: MIT Press.
- Nelson, Todd D. 2005. "Ageism: Prejudice Against Our Feared Future Self." *Journal of Social Issues* 61, no. 2 (May): 207-221.
- Ng, Brian D. and Peter M. Wiemer-Hastings. "Addiction to the internet and Online Gaming." *CyberPsychology and Behavior*. 8, no. 2 (September): 110-113. <http://dx.doi.org/10.1089/cpb.2005.8.10>.
- Nunes, Teresa, Isabel Fragaga, Filipa Ribeiro, Teresa Palma, Joao Maroco, Jorge Cannas, Mario Secca, et al. 2010. "The Outcome of Elderly Patients with Cognitive Complaints but Normal Neuropsychological Tests." *Journal of Alzheimer's Disease* 19, no. 1: 137-145.
- Obama, Barack. 2012. "Taking the Cyberattack Threat Seriously." *The Wall Street Journal*. July 19, 2012 Accessed April 5, 2013. <https://www.wsj.com/articles/SB1000087239639044433090457753592693044650>.
- Ohm, Paul. 2009. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review Research Information Network* 57, no. 6 (August): 1071-1777.
- Oinas-Kukkonen, Harri and Marja Harjumaa. 2008. "Towards Deeper Understanding of Persuasion in Software and Information Systems." In *Proceedings of The First International Conference on Advances in Human-Computer Interaction, 2008*, 200-205. Saint Luce, Martinique.

- Oinas-Kukkonen, Harri and Marja Harjumaa. 2009. "Persuasive Systems Design: Key Issues, Process Model, and System Features." *Communications for the Association for Information Systems* 24, no. 1 (March): 485-500.
- Oke, Tayo. 2014. "Financial Crime Prosecution, Legal Certainty, and Exigency of Policy: Case of Nigeria's EFCC." *Journal of Financial Crime* 21, no. 1 (January): 56-65. doi:10.1108/F=JFC-06-2013-0044.
- Oliveira, Daniela S., Tian Lin, Harold Rocha, Donovan Ellis, Sandeep Dommaraju, Huizi Yang, Devon Weir, Sebastian Marin, and Natalie Ebner. 2019. "Empirical Analysis of Weapons of Influence, Life Domains, and Demographic Targeting in Modern Spam: An Age-Comparative Perspective." *Crime Science* 8, no. 3 (April): 1-14.
- Olshansky, S. Jay, Daniel Perry, Richard A. Miller, and Robert N. Butler. 2006. "In Pursuit of the Longevity Dividend: What Should We Be Doing to Prepare for the Unprecedented Aging of Humanity." *The Scientist* (March): 29-36.
- O'Shaughnessy, Carol and Angela Napili. 2006. *The Older Americans Act: Programs, Funding, and 2006 Reauthorization (P.L. 109-365)*. CRS Report for Congress. Washington, DC: Congressional Research Service.
- O'Sullivan, Maureen. 2003. "The Fundamental Attribution Error in Detecting Deception: The-Boy-Who-Cried-Wolf Effect." *Personality and Social Psychology Bulletin* 29, no. 10 (October): 1316-1327.
- O'Toole, Laurence J. Jr. 2000. "Research on Policy Implementation: Assessment and Prospects." *Journal of Public Administration on Research and Theory* 10, no. 2 (April) 263-288.
- Paganini, Pierluigi. 2017. "A Member of the Hacker Group 'Crackas With Attitude' Who Hacked US Intel Officials Has Been Sentenced to 5 Years in Jail." Security Affairs. Accessed January 31, 2018.  
<http://securityaffairs.co/wordpress/62880/cyber-crime/crackas-with-attitude-sentenced.html>.
- Paglin, Max D., editor. 1990. *A Legislative History of the Communications Act of 1936*. Oxford: Oxford University Press.
- Pak, Karla Blair Schweitzer and Philip Shadel. 2007. "The Psychology of Consumer Fraud." The TAO Institute. Accessed December 22, 2017.  
<https://www.taosinstitute.net/doug-shadel-and-karla-pak-dissertation>.
- Pankratz, Thomas and Hanns Matiasek. 2012. "Understanding Transnational Organised Crime: A Constructivist Approach Towards a Growing Phenomenon." *SIAK - Journal for Police Science and Practice*. 2: 38-46. doi: 10.7396/IE\_2012\_D.

- Paramaguru, Kharunva. 2013. "Private Data-Collection Firms Get Public Scrutiny." *Time*. Accessed October 25, 2016. <http://nation.time.com/2013/12/19/private-data-collection-firms-get-public-scrutiny>.
- Parker, Geoffrey G., Marshall W. Van Alstyne, and Sangeet Paul Choudary. 2016. *Platform Revolution: How Networked Markets are Transforming the Economy and How to Make Them Work for You*. New York: W.W. Norton and Company.
- Patel, Avanish B. and Virendra Kumar. 2015. "Challenges among the Elderly in Later Life." *Journal of Indian Academy of Geriatrics* 11, no. 4 (December): 171-173.
- Payne, Malcolm. 2012. *Citizenship Social Work with Older People*. Chicago: Lyceum Books, Inc.
- Public Broadcasting System. 2001. *Notable Hacks*. Accessed November 10, 2014. <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html>.
- Pelissic du Rausas, Mathieu, James Monyika, Eric Hagan, Jacques Bughin, Michael Chui, and Remi Said. 2012. "The Net's Sweeping Impact on Growth, Jobs and Prosperity." McKinsey Global Institute. Accessed April 20, 2013. [www.mckinsey.com/insights/high\\_tech\\_telecoms\\_internet-mattersnet](http://www.mckinsey.com/insights/high_tech_telecoms_internet-mattersnet).
- Pelletier, John. 2016. *2016 National Report on Adult Financial Literacy: Is Your State Making the Grade?* Burlington: Champlain College.
- Perez, Evan, Tal Kopan and Shimon Prokupecz. 2015. "U.S. Investigating Report Email Account Linked to CIA Director Hacked." CNN. Accessed September 20, 2016. <http://www.cnn.com/2015/10/19/politics/cia-fbi-alleged-hacking-report/>.
- Perez, Sarah. 2018. "39 Million Americans Now Own a Smart Speaker, Report Claims." Tech Crunch. Accessed January 20, 2019. <https://techcrunch.com/2018/01/12/39-million-american-now-own-a-smart-speaker-report-claims>.
- Peris, Rosana, Miguel A. Gimeno, Daniel Pinazo, Generos Ortet-fabregat, Virginia Carrero, M. Sanchez and Manuel I. Ibanez. 2002. "Online Chat Rooms: Virtual Spaces of Interaction for Socially Oriented People." *CyberPsychology and Behavior* 5, no. 1 (July): 43-51.
- Perrelli, Jaclyn. 2007. "Hackings Boy Wonder." *PC Magazine* 26, no. 16 (December): Accessed December 15, 2012. EBSCOhost.
- Perri, Frank S. and Richard G. Brody. 2011. "Birds of the Same Feather: The Dangers of Affinity Fraud." *Journal of Forensic Studies in Accounting and Business* 3, no. 1 (Fall): 33-46.
- Perri, Frank S. and Richard G. Brody. 2012. "The Optics of Fraud: Affiliations that Enhance Offender Credibility." *Journal of Financial Crime* 19, no. 3 (October): 305-320.

- Perrin, Andrew. 2015a. "American's Internet Access: 2000-2015." Pew Research Center. Accessed June 26, 2017. <http://www.pewinternet.org/2015/06/26/2015/internet-usage-across-2000-2015>.
- . 2015b. "Social Media Usage: 2005-2015." Pew Research Center. Accessed July 12, 2016. <http://www.pewinternet.org/2015/Social-Networking-Usage-2005-2015/>.
- Perry, Mark J. 2013. "Markets in Everything: Outsourcing Government Mandated Care for Elderly Parents in China." American Enterprise Institute. Accessed August 7, 2015. <http://www.aei.org/publication/markets-in-everything-outsourcing-government-mandated-care-for-elderly-parents-in-china/>.
- Peters, Ruth. 2006. "Ageing and the brain." *Postgraduate Medical Journal* 82, no. 964 (February): 84-88. Accessed September 10, 2018. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2596698>.
- Philpott, Daniel. 2016. "Sovereignty." The Stanford Encyclopedia of Philosophy. Accessed June 30, 2017. <https://plato.stanford.edu/archives/sum2016/entries/sovereignty>.
- Pinsker, Donna and Ken McFarland. 2010. *Exploitation in Older Adults: Personal Competence Correlates of Social Vulnerability, Aging, Neuropsychology, and Cognition*. Accessed December 6, 2011. <http://dx.doi.org/10.1080/1382585.2010.501403>.
- Podesta, John, Penny Pritzker, Sernest J. Moniz, John Holden, and Jeffrey Zients. 2014. *Big Data: Seizing Opportunities, Preserving Values*. Washington, DC: U.S. Government Print Office.
- Poole, Hilary W., Laura Lambert, Chris Woodford, and Christos J.P. Moschoritis. 2005. *Internet: A Historical Encyclopedia*. Santa Barbara, CA.: ABC-CLIO.
- Pratkanis, Anthony and Doug Shadel. 2005. *Weapons of Fraud: A Source Book for Fraud Fighters*. Seattle: AARP Washington.
- Pratt, Travis C., Kristy Holtfreter, and Michael D. Reisig. 2010. "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory." *Journal of Research in Crime and Delinquency* 47, no. 3 (August): 267-296.
- Public Law 113-274. 2014. "Cybersecurity Enhancement Act of 2014."
- Purkey, William W. and Betty L. Siegel. 2003. *Becoming an Invitational Leader: A New Approach to Professional and Personal Success*. Atlanta: Brumby Holdings, Inc.
- Purkey, William Watson and John Michael Novak. 2015. "An Introduction to Invitational Theory." *Journal of Invitational Theory and Practice* 1, no. 1 (Winter): 5-15.

- Rajesh, Iyer and Jacqueline K. Eastman. 2006. "The Elderly and their Attitudes toward the Internet: The Impact on Internet Use, Purchase and Comparison Shopping." *Journal of Marketing Theory & Practice* 14, no. 1 (December): 57-67. Accessed September 22, 2001. <https://www.tandfonline.com/doi/abs/10.2753/MTP1069-6679140104>.
- Ramirez, Edith, Julie Brill, Maureen K. Ohlausen, and Joshua D. Wright. 2014. *Data Brokers: A Call for Transparency and Accountability*. Washington, DC: Federal Trade Commission.
- Rankin, Katherine P., Andrea Salazar, Marc Solberger, Stephen Wilson, Danijela Pavlic, Christine M. Stanley, Shenly Glenn, et al. 2009. "Detecting Sarcasm from Paralinguistic Cues: Anatomic and Cognitive Correlates in Neurodegenerative Disease." *NeuroImage* 47, no. 4 (October): 2005-2015.
- Rasmussen, Heather N., Michael F. Scheier, and Joel B. Greenhouse. 2009. "Optimism and Physical Health: A Meta-analytic Review." *Annals of Behavioral Medicine* 37, no. 3 (June): 239-256. doi:10.1007/s12160-0029-9111-x.
- Raymond, Eric Steven 2000. *A Brief History of Hackerdom*. Website May 5, 2000, update August 2, 2002. <http://www.catb.org/~esr/writings/cathedral-bazaar/hacker-history/>. Accessed July 10, 2012.
- . 2012. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol: O'Reilly Media, Inc.
- Reed, David A. and Bruce O. Jolly. 2012. "Know the Signs of Elder Financial Abuse." *Credit Union Magazine* 78, no. 8 (August): 42-43.
- Reis, Myrna and Daphne Nahmaish. 1998. "Validation of the Indicators of Abuse (IOA) Screen." *Gerontologist* 38, no. 4 (August): 471-481.
- Report of 2005 White House Conference on Aging. 2005. "The Booming Dynamics of Aging: From Awareness to Action." Accessed June 30, 2013. [http://www.genpolicy.com/wordpress/wp-content/themes/spacio/pdfs/whoca\\_report\\_2005.pdf](http://www.genpolicy.com/wordpress/wp-content/themes/spacio/pdfs/whoca_report_2005.pdf).
- Riccucci, Norma M. 2010. *Public Administration: Traditions of Inquiry and Philosophies of Knowledge*. Washington, DC: Georgetown University Press.
- Richard J. Bonnie and Robert B. Wallace, editors. 2003. "Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America (2003)." National Academies Press. Accessed December 01, 2011. <https://www.ncbi.nlm.nih.gov/pubmed/22812026>.
- Riley, Patrick. 2006. "The Social Contract and Its Critics." In *The Cambridge History of Eighteenth Century Political Thought* by Mark and Robert Wokler, editors, 347-75. London: Cambridge University Press.

- Ritchie, Guy, dir. 2011. *Sherlock Holmes: A Game of Shadows*. Hollywood: Studio.
- Rochefort, David A. and Roger W. Cobb. 1994. *The Politics of Problem Definition: Shaping the Policy Agenda*. Rochefort: The University of Kansas.
- Rogin, Josh. 2012. "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History.'" The Cable. Accessed April 23, 2013.  
<http://www.thecable.foreignpolicy.com/posts/2012/07/09>.
- Rosenoer, Jonathan. 1997. *CyberLaw: The Law of the Internet*. New York: Springer-Verlag.
- Rosenzweig, Paul and David Inserra. 2013. "Obama's Cybersecurity Executive Order Falls Short." The Heritage Foundation. Accessed March 15, 2013.  
<http://report.heritage.org/ib3852>.
- Roth, Marcus and Philipp Hammelstein. 2007. "Hope as an Emotion of Expectancy: First Assessment Results." *German Medical Science: Psycho-Social Medicine* 4, no. 5 (April): 1-9. Accessed March 5, 2017.  
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2736531/>.
- Roubick, Joe. 2009. "Financial Abuse: Fraud vs Exploitation of the Elderly Why Fraud and Exploitation Are Different Crimes." Accessed September 16, 2012.  
<http://voices.yahoo.com/why-exploitation-crimes-misunderstood-4185977.html?cat=25>.
- Ryan, Tracii, John Reece, Andrea Chester, and Sophia Xenos. 2016. "Who gets hooked on Facebook? An exploratory typology of problematic Facebook users." *Cyberpsychology*. 10, no. 3 (September):1-25. <https://doi.org/10.5817/CP2016-3-4>.
- Salvatore, Tony. 2010. *The Suicide Paradigm*. Accessed December 5, 2011.  
[http://lifegard.tripod.com/PA Elder Suicide](http://lifegard.tripod.com/PA%20Elder%20Suicide).
- Salzborn, Samuel. 2015. "No Sovereignty without Freedom: Machiavelli, Hobbes and the Global Order in the Twenty-first Century." *Theoria: A Journal of Social and Political Theory* 62, no. 144 (September): 19-59.
- Samuelson, Paul. 1947. *Foundations of Economic Analysis*. Cambridge: Harvard University Press.
- Schein, Edgar H., Inge Schneier, and Curtis H. Harker. 1961. *Coercive Persuasion: A Socio-psychological Analysis of the "Brainwashing" of American Civilian Prisoners by the Chinese Communists*. New York: W.W. Norton and Company, Inc.

- Schicor, David, Jeff Doocy, and Gilbert Geis. 1996. "Anger Disappointment and Disgust: Reactions of Victims of a Telephone Investment Scam." In *International Victimology: Selected Papers from the 8th International Symposium*. no. 27 (January) 105-111. ISSN: 1034-5086
- Schrager, Allison. 2014. "Underpaid Employees are a Cybersecurity Risk." Bloomberg Business Week. Accessed November 30, 2014.  
<http://www.businessweek.com/articles/2014-10-06/underpaid-employees-are-a-cybersecurity-risk>.
- Schull, Natasha Dow. 2012. *Addiction by Design*. Princeton: Princeton University Review.
- Schwartz, Daniel M. and Tony Rouselle. 2009. "Using Social Network Analysis to Target Criminal Networks." *Trends in Organized Crime* 12, no. 2 (October): 188-207.
- Schwartz, Paul M. 2005. "Property, Privacy, and Personal Data." *Harvard Law Review* 117, no. 7 (May): 2056-2128.
- Scott, James. 2017. *Equifax: The Hazards of Dragnet Surveillance Capitalism*. Washington, D.C.: Institute for Critical Infrastructure Technology. Accessed June, 3, 2018. <http://icitech.org/wp-content/uploads/2017/10/ICIT-Analysis-Equifax-The-Hazards-of-Dragnet-Surveillance-Capitalism.pdf>.
- \_\_\_\_\_. 2018. "Equifax: The Hazards of Dragnet Surveillance Capitalism Part 2: Just Another Data Breach or C-Suite Criminal Negligence?" Institute for Critical Infrastructure Technology: The Cybersecurity Think Tank. Accessed January 5, 2019. <https://icitech.org/wp-content/uploads/2017/10/ICIT-Analysis-Equifax-The-Hazards-of-Dragnet-Surveillance-Capitalism.pdf>.
- Secretary of State. 2010. "Cybercrime Strategy." Secretary of State for the Home Department by Command of Her Majesty. Accessed November 30, 2014.  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228826/7842.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf).
- Security Scorecard. 2018. "2018 Government Cybersecurity Report." Security Scorecard. Accessed September 27, 2018. <https://securityscorecard.com/resources/2018-us-government-cybersecurity-research-report>.
- Seger, Alexander. 2016. "The Budapest Convention on Cybercrime: A Framework for Capacity Building." *Global Cyber Expertise Magazine* 2 (November): 29-31.
- Seife, Charles. 2015. *Virtual Unreality: The New Era of Digital Deception*. New York: Penguin Books.

- Sela-Shayovitz, Revital. 2012. "Gangs and the Web: Gang Members' Online Behavior." *Journal of Contemporary Criminal Justice* 28, no. 4 (October): 389-405.
- Shadel, Doug and Karla Pak. 2017. *AARP Investment Fraud Vulnerability Study*. Washington, DC: AARP Research.
- Shakespeare, William. *The Merchant of Venice*. 1596.
- Shalini, S. 2016. "Budapest Convention on Cybercrime: An Overview." Accessed June 3, 2017. <http://www.ccgnludelhi.wordpress.com>.
- Shulman, David. 2007. "Scams and Sweetners." *Pacific Affairs*. 80, no. 4 (Winter) 678-679.
- Sil, Rudra and Peter J. Katzenstein. 2010. "Analytic Eclecticism in the Study of World Politics: Reconfiguring Problems and Mechanisms across Research Traditions." *Perspectives on Politics* 8, no. 2 (June): 411-431.
- Silverman, Jacob. 2015. *Terms of Service*. New York: HarperCollins Publishers.
- \_\_\_\_\_. 2017. "Privacy under Surveillance Capitalism." *Social Research* 84, no. 1 (Spring): 147-164.
- Silverman, Stephen M. 2019. "It's a Wonderful Life Was a Winter Wonderland – in July" People.com Accessed December 14, 2019. <https://people.com/celebrity/its-a-wonder-life-included-life-like-snow/>
- Simon, Tobby. 2017. "Critical Infrastructure and the Internet of Things." *Centre for International Governance Innovation*. Accessed February 10, 2017. <https://www.cigionline.org/publications/critical-infrastructure-and-internet-0>.
- Simon, Herbert A. 1956. "Rational Choice and the Structure of the Environment." *Psychological Review* 63, no. 2: 129-138. doi:10.1037/h0042769. PMID 13310708.
- Simon, Herbert A. 1997. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations* 4<sup>th</sup> ed. New York: The Free Press.
- Simons, Herbert W. 1976. *Persuasion: Understanding, Practice and Analysis*. Boston: Addison-Wesley Publishing.
- Singer, Peter W. and Emerson T. Brooking. 2018. *Like War: The Weaponization on Social Media*. New York: Houghton Mifflin Harcourt.

- Sklamberg, Howard. 2014. "Counterfeit Drugs: Fighting Illegal Supply Chains." Testimony before U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, Deputy Commissioner for Global Regulatory Operations and Policy, Food and Drug Administration Department of Health and Human Services, Washington, D.C. Accessed January 20, 2017. <https://www.fda.gov/NewsEvents/Testimony/ucm387449.htm>.
- Smith, Adam. 1991. *The Wealth of Nations*. Amerst: Prometheus Books. (Orig. pub. 1776.)
- Smith, G. Stevenson. 2015. "Management Models from International Cybercrime." *Journal of Financial Crime* 2, no. 1 (January): 104-125. Accessed February 25, 2019. doi:10:1108/JFC-09-2013-0051.
- Sobczak, Blake. 2019. "'Denial of Service' Attack Caused Grid Cyber Disruption: DOE." Accessed May 2, 2019. <http://www.eenews.net/stories/1060254751>.
- Solove, Daniel J. 2011. *Nothing to Hide: The False Trade-Off Between Privacy and Security*. New Haven: Yale University Press.
- Somashekhar, Sandhya. 2014. "Slew of Changes to Health-Care Law Creates More Confusion for Consumers." *Washington Post Online*. Accessed March 15, 2014. [http://www.washingtonpost.com/national/health-science/slew-of-changes-to-health-care-law-creates-more-confusion-for-consumers/2014/03/08/b5c7e176-a621-11e3-a5fa-55f0c77bf39c\\_story.html](http://www.washingtonpost.com/national/health-science/slew-of-changes-to-health-care-law-creates-more-confusion-for-consumers/2014/03/08/b5c7e176-a621-11e3-a5fa-55f0c77bf39c_story.html).
- Spamhaus. 2018. *The Spamhaus Project*. Accessed February 5, 2018. <https://www.spamhaus.org/statistics/spammers/>.
- Spekman, Robert C. 1988. "Strategic Supplier Selection: Understanding Long-Term Buyer Relationships." *Journal of Business Research*, 31, no. 4 (July-August): 75-81.
- Spiekermann, Sarah, Alessandro Acquisti, Rainer Bohme, and Kai-Lung Hui. 2015. "The Challenges of Personal Data Markets and Privacy." *Electron Markets* 25, (April): 161-167.
- Spokeo, Inc. v. Robins 136 S. 1540 (9<sup>th</sup> Cir 2017).
- Social Security Administration. 2014. "Social Security Act." Accessed March 30, 2014. <http://www.ssa.gov/history/35act.html>.
- \_\_\_\_\_. 2016. "What You Can Do Online." November. Accessed November 5, 2016. <https://www.ssa.gov>.
- Stanger, Tobie. 2015. "Lies, Secrets, and Scams: How to Prevent Elder Abuse." *Consumer Reports* (November 3, 2018): 28-37.

- Sterling, Bruce. 2018. "Crackas With Attitude." *Wired*. Accessed January 31, 2018.  
<https://www.wired.com/2015/11/cia-email-hackers-return-with-major-law-enforcement-breach/>.
- Stiegel, Lori and Ellen Klem. 2007. "Types of Abuse: Comparison Chart of Provisions in Adult Protective Services Laws, By State." American Bar Association Commission on Law and Aging for the National Center on Elder Abuse. Accessed February 27, 2014.  
[http://www.americanbar.org/content/dam/aba/migrated/aging/about/pdfs/Abuse\\_Types\\_State\\_and\\_Category\\_Chart.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/migrated/aging/about/pdfs/Abuse_Types_State_and_Category_Chart.authcheckdam.pdf).
- Stratton Oakmont, Inc. v. Prodigy Services Co. WL 323719 NY. S. Ct. (1995).
- Storch, Tyson. 2012. "Cybersecurity: Cornerstone of a Safe, Connected Society." Trustworthy Computing Microsoft Corporation. Accessed April 19, 2013.  
<https://www.download.microsoft.com/download/B/8/7/B879F372-F724-4B42-AADC-1385D2AD9085/Trustworthy%20Computing%20Cybersecurity%20white%20paper.docx>.
- Strickland, Jonathan. 2014. *Who Owns the Internet?* Accessed November 10, 2014.  
<http://computer.howstuffworks.com/internet/basics/who-owns-internet.htm>.
- Stuart-Hamilton, Ian. 2006. *The Psychology of Ageing: An Introduction*. London: Jessica Kingsley.
- SuperiorTelegram Adminstrator. 2017. "Three sentenced in cyber fraud schemes involving more than \$17M." *SuperiorTelegram*. Accessed January 10, 2018. (November 22, 2017). <https://www.superiortelegram.com/news/4363704-three-sentenced-cyber-fraud-schemes-involving-more-17m>.
- Sweeney, Latanya. 2000. "Simple Demographics Often Identify People Uniquely." Data Privacy Working Paper 3. Pittsburgh: Carnegie Mellon University. Accessed December 20, 2016. <http://repository.cmu.edu/isr/230/>.
- Symantec. 2012. "Symantec MessageLabs Email AntiSpam.cloud." Accessed November 25, 2012. [https://www.insight.com/content/dam/insight/en\\_US/](https://www.insight.com/content/dam/insight/en_US/).
- Talbot, David. 2012. "A Phone that Knows Where You're Going." *MIT Technology Review*. Accessed December 15, 2015.  
<https://www.technologyreview.com/s/428441/a-phone-that-knows-where-youre-going>.

- Teaster, Pamela B., Tyler D. Dugar, Joanne M. Oto, Marta S. Mendiondo, Erin L. Abner, and Kara A. Cecil. 2006. "The 2004 Survey of State Adult Protective Services: Abuse of Adults 60 Years of Age and Older." Report to the National Center on Elder Abuse. Washington, DC: Administration on Aging. Accessed December 10, 2014. [www.napsa-now.org/wp-content/uploads/2012/09/2-14-06-FINAL-60+REPORT.pdf](http://www.napsa-now.org/wp-content/uploads/2012/09/2-14-06-FINAL-60+REPORT.pdf)
- Thaler, Richard H. and Cass R. Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New York: Penguin.
- The Official Social Engineering Portal. 2011. "What is Social Engineering?" Accessed December 02, 2011. <https://www.social-engineer.org>.
- Thomas, Dylan. 1953. *The Poems of Dylan Thomas*. New York: New Directions Publishing Corporation.
- Thomas, Jim. 2005. "The Moral Ambiguity of Social Control in Cyberspace: A Retrospective assessment of the 'Golden Age' of Hacking." *New Media & Society* 7, 5 (October): 599-624.
- Timmermann, Sandra. 2009. "Protecting the Most Vulnerable from Financial Abuse: What Should We Know?" *Journal of Financial Service Professionals* 63, no. 3: 23-25.
- Tocqueville, Alexis de. 1945. *Democracy in America*. Edited by Philip Bradley. New York: Alfred A. Knopf.
- Trend Micro. 2014. "Employees May be a Company's Biggest Cybersecurity Risk: The Threat of Social Engineering." Accessed November 30, 2014. <http://www.blog.trendmicro.com/employees-may-companys-biggest-cybersecurity-risk-threat-social-engineering>.
- Truman, Jennifer L. 2011. "Criminal Victimization, 2010 NCJ 235508." National Crime Victimization Survey. U.S. Department of Justice, Office of Justice Program, Bureau of Justice Statistics. Accessed December 3, 2012. <https://www.bjs.gov/content/pub/pdf/cv10.pdf>.
- Tsikerdakis, Michael and Sheralli Zeadally. 2014. "Online Deception in Social Media." *Communications of the ACM* 57, no. 9 (September): 72-80. Accessed December 10, 2015. <https://doi.acm.org/10.1145/2629612>.
- Tufte, Edward R. 1997. *Visual Explanations*. Cheshire: Graphics Press LLC.
- Turton, William. 2016. "The Daily Dot." Accessed November 1, 2016. <http://www.dailycdot.com/layer8/cracka-hacker-cia-john-brennan-email-arrested/>.

- Tversky, Amos and Daniel Kahneman. 1974. "Judgment Under Uncertainty: Heuristics and Biases." *Science* 185, no. 4157 (September 27, 1974): 1124-1131. Accessed November 25, 2015. <http://links.jstor.org/sici?doi=0036-8075%2819740927%293%3A185%3A4157%3C1124%3AJUUHAB%3E2.0.CO%3B2-M>.
- Tversky, Amos and Daniel Kahneman. 1986. "Rational Choice and Framing of Decisions." *The Journal of Business* 59, no. 4, Part 2 (October): S251-S278. <http://www.jstor.org/stable/2352759>.
- U.S. Congress Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law. 2017. "Equifax: Continuing to Monitor Data-Broker Cybersecurity." Accessed September 17, 2018. <https://www.judiciary.senate.gov/imo/media/doc/10-04-17%20Winterton%20Testimony1.pdf>.
- U.S. Congress Senate Committee on Finance. *The Elder Justice Coalition*. 116<sup>th</sup> Cong., 1<sup>st</sup> sess., July 23, 2019.
- Uchino, Bert N., John T. Cacioppo, and Janice K. Kiecolt-Glaser. 1996. "The Relationship Between Social Support and Physiological Processes: A Review with Emphasis on Underlying Mechanisms and Implications for Health." *Psychological Bulletin* 119, no. 3 (May): 488-531. doi:10.1037/0033-2909.119.3.488.
- Ulrey, Page. 2012. "Confusion on the Front Lines: The Response of Law Enforcement and Prosecutors to Cases of Elder Abuse." *Administration on Aging*. Accessed March 14, 2017. [http://www.aoa.gov/AoA\\_programs/Elder\\_Rights/EJCC/docs/Ulrey\\_White\\_Paper.pdf](http://www.aoa.gov/AoA_programs/Elder_Rights/EJCC/docs/Ulrey_White_Paper.pdf).
- Ulrey, Page. 2015. "Broken Trust: Combating Financial Exploitation of Vulnerable Seniors." Testimony before the Senate Special Comm. on Aging, 114th Cong. 13 (February 4, 2015) (written testimony of Page Ulrey).
- United Nations. 2010. "The Universal Declaration of Human Rights." Accessed December 10, 2018. [http://www.claiminghumanrights.org/udhr\\_article\\_12.html](http://www.claiminghumanrights.org/udhr_article_12.html).
- \_\_\_\_\_. 2017. "The Responsibility to Protect." Accessed August 17, 2017. <http://www.un.org/en/genocideprevention/about-responsibility-to-protect.html>.

- . 2011. "Report of the Special Rapporteur on the Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development." United Nations General Assembly. Accessed September 27, 2018.  
[https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
- United Nations Interregional Crime and Justice Research Institute. 2012. "Emerging Crimes: Cyber Crimes." Accessed December 12, 2012.  
[http://www.unicri.it/emerging\\_crimes/cybercrime/](http://www.unicri.it/emerging_crimes/cybercrime/).
- United Nations Human Rights Council. 2016. "United Nations General Assembly." Accessed June 10, 2017.  
[https://www.article19.org/data/files/Internet\\_Statement\\_Adopted.pdf](https://www.article19.org/data/files/Internet_Statement_Adopted.pdf).
- United Nations Office on Drugs and Crime. 2016. Draft February 2013. "Comprehensive Study on Cybercrime." United Nations. Accessed December 3, 2017.  
[https://www.unodc.org/documents/organized-crime/Cybercrime\\_comments/Contributions](https://www.unodc.org/documents/organized-crime/Cybercrime_comments/Contributions).
- . 2015. "A Study on the Effects of New Technologies on the Abuse and Exploitation of Children." Report to UN. Vienna: United Nations Office on Drugs and Crime.
- United States v. Morris. 928 F. 2d 504 2nd Cir. No. 774, *Docket 90-1336*. (1991).
- United States v. Iriri 7<sup>th</sup> Cir, *Docket 15-3692*. (2016).
- United States v. Pujols, Camilo, Etienne, Ocasio, Santos, Vasquez. *Docket 1:17-cr-20702-JEM*. FL (2017).
- United States v. Stencil, Broyles, Sierp, Stencil, Lewis, Fleming, Duke, Saccomanno, Swerden. *Docket 3:16-CR-221-MOC*. NC. (2017).
- United States v. Ugbah, Adegoke, Whipple. *Docket 3:17-cr-00105*. WI. (2017).
- United States v. Sciarra. *Docket 2:09-cr-00863-SRC*. NJ. (2017).
- United States v. Strobl. *Docket 0:17-cr-60066-WPD*. FL. (2017).
- United States v. Gohil, Chetiwal, Patel, Jiwani. *Docket 17-CR-212*. WI. (2018).
- United States v. Taher, Jaafar, Gonzalez, Tovar, Castillo, Castillo, Velasco, Estrella, Reyes. *Docket 0:17-cr-60223-UU*. FL. (2018).
- Ulrey, Page. 2015. "Broken Trust: Combating Financial Exploitation of Vulnerable Seniors." February 4, 2015. <https://www.aging.senate.gov/>

- Urban, Jennifer M. and Chris Jay Hoofnagle. 2014. "The Privacy Pragmatic as Privacy Vulnerable." In *The Symposium on Usable Privacy Security (SOUPS)*, July 9-11, Menlo Park, CA. <https://ssrn.com/abstract=2514381>.
- Usunier, Jean-Claude and Julie Anne Lee. 2013. *Marketing Across Cultures*, 6th ed. Harlow: Pearson Education.
- Van Meter, Donald and Carl Van Horn. 1975. "The Policy Implementation Process: A Conceptual Framework." *Administration and Society* 6, no. 4 (February 1, 1975): 445-488.
- Vasylendo, Olena. 2012. "Problem of Cybercrime in Ukraine: Spread of, Specific Nature, and Methods of Fighting." *Internal Security* 4, no. 1 (January-June): 153-163. <http://yadda.icm.edu.pl/yadda/element/bwmeta1.element-380ce9b2-21f3-3003-b452-1a54a02da456>.
- Vennesson, Pascal and Ina Wiesner. 2014. "Process Tracing in Case Studies." In *Routledge Handbook of Research Methods in Military Studies*. Edited by Joseph Soeters, Patricia M. Shields, and Sebastian Rietjens Soeters. London: Routledge.
- Vrij, Aldert, Par Anders Granhag, and Samantha Mann. 2010. "Good Liars." *The Journal of Psychiatry and Law* 38 no. 1-2 (March): 77 - 98.
- Wachs, Sebastian, Karsten D. Wolf, and Chig-Ching Pan. 2012. "Cybergrooming: Risk Factors, Coping Strategies, and Associations with Cyberbullying." *Psicothema* 24(4): 628-633. [www.psicothema.com](http://www.psicothema.com).
- Wagner, Ann and Hakeem Jeffries. 2019. "Wagner and Jeffries Introduce Legislation to Reduce Worldwide Sex Trafficking Demand." Congresswoman Ann Wagner website. (September 13, 2019). Accessed November 28, 2019. <https://wagner.house.gov/media-center/press-releases/wagner-and-jeffries-introduce-legislation-to-reduce-worldwide-sex>.
- Walther, Joseph B. 1996. "Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction." *Communication Research* 23(1): 3-43.
- Warren, Samuel D. and Loiss D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4(5): 193-220.
- Weber, Max. 1947. *The Theory of Social and Economic Organization*. New York: The Free Press.
- Webster. 1964. *Webster's New World Dictionary*. New York: The World Publishing Company.

- Weinert, Matthew S. 2007. "Bridging the Human Rights- Sovereignty Divide: Theoretical Foundations of a Democratic Sovereignty." *Human Rights Review* 8 (2): 5-32.
- West, Richard and Lynn H. Turner. 2018. *Introducing Communication Theory: Analysis and Application*. 6<sup>th</sup> ed. New York: McGraw-Hill. ISBN-13 978-1259870323.
- Westin, Alan F. 1976. *Computers, Health Records and Citizens Rights*. Gaithersburg: U.S. Department of Commerce: National Bureau of Standards. Accessed December 10, 2018. <https://www.govinfo.gov/content/pkg/GOV PUB-C13-a16c3d655120a7411d9dfa0fcaaf7367/pdf/GOV PUB-C13-a16c3d655120a7411d9dfa0fcaaf7367.pdf>.
- White House. 2011. "Strategy To Combat Transnational Organized Crime: Addressing Converging Threats to National Security." *White House Strategy to Combat Transnational Organized Crime*. July. Accessed March 30, 2013. [www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf](http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf).
- . 2015. *White House Briefing Room*. July 13. Accessed December 2, 2018. <https://obamawhitehouse.archives.gov/the-press-office/2015/07/13/fact-white-house-conference-on-aging>.
- Whittaker, Zack. 2019. "Court Says Vizio's Secret Smart TV Tracking Class-Action Settlement Can Move Forward." *TechCrunch*. January 7. Accessed January 8, 2019. [https://techcrunch.com/2019/01/07/vizio-settlement-moves-forward/?wpisrc=nl\\_cybersecurity202&wpmm=1](https://techcrunch.com/2019/01/07/vizio-settlement-moves-forward/?wpisrc=nl_cybersecurity202&wpmm=1).
- Whitty, Monica T, Tom Buchanan. 2012. "The Online Romance Scam: A Serious Cybercrime." *Cyberpsychology, Behavior, and Social Networking* 15, no. 3: 181-183.
- Whitty, Monica T. 2013. "The Scammers Persuasive Techniques Model." *The British Journal of Criminology* 53, no.4: 665-684.
- World Health Organization. 2011. *European Report on Preventing Elder Maltreatment*. World Health Organization, Regional Office for Europe. Bonn, Germany. Accessed March 31, 2014. [http://www.eur.who.int/\\_data/assets/pdf/0010/144676/e95110.pdf](http://www.eur.who.int/_data/assets/pdf/0010/144676/e95110.pdf).
- Williams, Amrit. 2015. "Silicon Valley Doesn't Lead Breach Prevention. But It Should." *BuzzNews*. March 5. Accessed July 27, 2016. <https://www.informationsecuritybuzz.com/articles/silicon-valley-doesnt-lead-breach-prevention-but-it-should>.

Wilshusen, Gregory C. and Nabajyoti Barkakati. 2013. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented*. Washington, D.C. Government Accountability Office. February 14. Accessed March 30, 2013. [www.gao.gov](http://www.gao.gov).

Wilson, Woodrow. 1887. "The Study of Administration." *Political Science Quarterly* 2, no. 2: 197-222.

Woodiwiss, Michael and Dick Hobbs. 2009. "Organized Evil and the Atlantic Alliance: Moral Panics and The Rhetoric of Organized Crime Policing In America And Britain." *British Journal of Criminology* 49(1): 106-128.

Wright, David, and Twyla Hill. 2009. "Prescription for Trouble: Medicare Part D and Patterns of Computer and Internet Access Among the Elderly." *Journal of Aging & Social Policy* 21(2): 17-186.

Yadav, Sushama, Sudhir Yadav, and S.K. Tripathi. 2010. "Legislative Microscopy of Cyber Crimes." *Medico-Legal Update*, 10 (2): 107-111.

Yin, Robert K. 2003. *Case Study Research, Design, and Methods*. Thousand Oaks: SAGE Publications.

Yin, Robert K. 2014. *Case Study Research: Design and Methods 5th ed*. Thousand Oaks: SAGE Publications.

Young, Kimberly S. 2007. "Cognitive behavior therapy with Internet addicts: treatment outcomes and implications." *Cyberpsychology and Behavior*. 10, no.5 (October): 671-679. Accessed December 30, 2018. <https://doi.org/10.1089/cpb.2007.9971>.

Young, Sean. 2013. "The Science Behind Using Online Communities to Change Behavior." *TechCrunch*. September 28. Accessed January 28, 2018. <https://techcrunch.com/2013/09/28/the-science-behind-using-online-communities-to-change-behavior/>.

Young, Sean, Debo Dutta, and Gopal Dommetty. 2009. "Extrapolating Psychological Insights From Facebook Profiles: A Study of Religion and Relationship Status." *CyberPsychology and Behavior*, 12 (3): 347-350. doi:10.1089/cpb.2008.0165.

Youssef-Morgan, Carolyn and Fred Luthans. 2015. "Psychological Capital and Well-being." *Stress and Health*.31, no.3 (July): 180-188. doi:10.1002/smj.2623.

Zak, Paul. 2017. "The Neuroscience of Trust." *Harvard Business Review* 109: (January-February) 14-17. <https://hbr.org/2017/01/the-neuroscience-of-trust>-

Zetter, Kim. 2015. "Teen Who Hacked CIA Director's Email Tells How He Did It." *Wired*. October 15. Accessed July 15, 2016. <https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/>.

Zinn, Brad. 2019. "Man Said He Needed Cash to Release Inheritance, Scams Woman." *Staunton News Leader*, February 15. Accessed April 15, 2019.  
<https://www.newsleader.com/story/news/2019/02/15/augusta-county-woman-loses-600000-online-scam/28811537002>.