Digital Anonymity: Investigating the Open Threat by the Hidden User

Derrick B. Rumer

Follow this and additional works at: http://digitalcommons.apus.edu/theses

Part of the Computer Law Commons, and the Digital Communications and Networking Commons

Recommended Citation

APUS Library Capstone Submission Form

This capstone has been approved for submission to and review and publication by the APUS Library.

<table>
<thead>
<tr>
<th>Student Name [Last, First, MI] *</th>
<th>Rumer</th>
<th>Derrick</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Number [e.g. INTL699] *</td>
<td>ITCC698</td>
<td>Paper Date [See Title pg.] 06/2015</td>
</tr>
<tr>
<td>Professor Name [Last, First] *</td>
<td>Dr. Watson-Stone, Novadean</td>
<td></td>
</tr>
<tr>
<td>Program Name * [See list]</td>
<td>Master of Science in Information Technology</td>
<td></td>
</tr>
<tr>
<td>Keywords [250 character max.]</td>
<td>digital forensics, forensics, security, investigate, investigation, TOR</td>
<td></td>
</tr>
</tbody>
</table>

| Passed with Distinction * Y or N | Y                                      |
| Security Sensitive Information * Y or N | N                                      |
| IRB Review Required * Y or N | If YES, include IRB documents in submission attachments. |
| Turnitin Check * Y or N | All capstone papers must be checked via Turnitin. |

* Required

Capstone Approval Document

The thesis/capstone for the master’s degree submitted by the student listed (above) under this title *

DIGITAL ANONYMITY: INVESTIGATING THE OPEN THREAT BY THE HIDDEN USER

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

<table>
<thead>
<tr>
<th>Program Representatives</th>
<th>Signatures</th>
<th>Date (mm/dd/yyyy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed, 1st Reader * [capstone professor]</td>
<td>(Signature)</td>
<td></td>
</tr>
<tr>
<td>Signed, 2nd Reader (if required by program)</td>
<td>(Signature)</td>
<td></td>
</tr>
</tbody>
</table>
| Recommendation accepted on behalf of the program director * | Novadean Watson-Stone Digitally signed by Novadean Watson-Stone
  DN: 0xNovadean Watson-Stone,
  =American Public University System,
  =APUS, email=awatson@apus.edu,
  =US Date: 2015.07.07 11:55:35 -04'00' |                     |
| Approved by academic dean * | Dan Benjamin Digitally signed by Dan Benjamin
  Date: 2015.07.08 11:55:35 -04'00' |                     |

* Required
The author hereby grants the American Public University System the right to display these contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by United States copyright law for the inclusion of any materials that are not the author’s creation or in the public domain.

© Copyright 2015 by Derrick B Rumer

All rights reserved.
DEDICATION

I dedicate this thesis to my wife, children, parents, and friends. I could not have completed this without their patience, understanding, and support. Never end your pursuit of learning.
ACKNOWLEDGMENTS

I wish to thank all of the IT and forensics experts that has come before me as well as the men and women working for the Government and law enforcement agencies who have chosen digital forensics as their specialty. Finally, I would like to thank Dr. Novadean Watson-Stone for her support, encouragement, and leadership throughout this process.
DIGITAL ANONYMITY

ABSTRACT OF THE THESIS

DIGITAL ANONYMITY: INVESTIGATING THE OPEN THREAT BY THE HIDDEN USER

by

Derrick B. Rumer

American Public University, May 2015

Charles Town, West Virginia

Dr. Novadean Watson-Stone, Thesis Professor

Anonymous networks provide users the opportunity to navigate the internet anonymously by adding additional connections between client and server that mask the users IP address and provide other layers of security that protect user identities while navigating the web. With this technology also come ramifications when criminals use the technology to cover their tracks. This paper will provide insight to digital anonymity as well as review previous research conducted on the subject. The United Stated Government and law enforcement agencies have made great strides in combatting crimes conducted over anonymous networks. The purpose of this study is to determine if the United States Government and law enforcement agencies are adequately prepared to combat crimes conducted over anonymous networks. This research also contains a survey polling willing participants on topics of digital anonymity to include personal experiences and opinions on issues surrounding this topic. The survey will be used to determine if U.S. citizens believe that anonymizing technologies should be federally regulated. It will also determine if the participants feel that regulating such a technology infringes on their constitutional right to privacy.
Keywords: digital forensics, forensics, security, investigate, investigation, TOR, Darknet, anonymous, anonymous networks, digital anonymity
TABLE OF CONTENTS

COPYRIGHT PAGE ...................................................................................................... ii  
DEDICATION ............................................................................................................. iii  
ACKNOWLEDGMENTS .............................................................................................. iv  
ABSTRACT .................................................................................................................. v  
TABLE OF CONTENTS ............................................................................................ vii  
LIST OF TABLES ....................................................................................................... x  
LIST OF FIGURES ..................................................................................................... xi

CHAPTER                                                                 PAGE
I. INTRODUCTION ..................................................................................................... 1  
   Problem Statement ............................................................................................... 2  
   Purpose of Study ................................................................................................... 2  
   Significance of the Study ...................................................................................... 3  
   Assumptions, Limitations, and Delimitations ....................................................... 4  
   Definitions of Terms ............................................................................................. 4  

II. LITERATURE REVIEW .......................................................................................... 6  
   Introduction ........................................................................................................... 6  
   Anonymous Network Overview ............................................................................. 6  
   Methods to Provide Digital Anonymity ................................................................. 9  
   Previous Surveys on Digital Anonymity ............................................................... 14
Concerns Surrounding Digital Anonymity ......................................................... 21
Actions to Improve Investigations Involving Digital Anonymity ......................... 26
Summary and Remaining Questions ................................................................. 30

III. METHODOLOGY .......................................................................................... 32
Data Collection Technique ................................................................................. 32
Hypothesis and Research Questions ................................................................. 33
Subjects and Setting ......................................................................................... 36
Statistical Analysis ............................................................................................ 37
Limitations of the Study .................................................................................... 38

IV. RESULTS ........................................................................................................ 39
Survey Demographics ......................................................................................... 39
Impact of Gender and Age .................................................................................. 47
Impact of Education ............................................................................................ 49
Impact of Employment ......................................................................................... 50
Impact of Experience .......................................................................................... 51

V. DISCUSSION ................................................................................................... 54

VI. SUMMARY ..................................................................................................... 59

VII. RECOMMENDATIONS ................................................................................ 61
LIST OF REFERENCES ........................................................................................................... 62

APPENDICES ..................................................................................................................... 68

Appendix A: Digital Anonymity Survey .......................................................................... 68
LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Number of Survey Participants by Demographics</td>
<td>41</td>
</tr>
<tr>
<td>2. Qualitative Questions</td>
<td>45</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Gender Distribution of the Sample Population</td>
<td>42</td>
</tr>
<tr>
<td>2. Age Distribution of the Sample Population</td>
<td>43</td>
</tr>
<tr>
<td>3. Education Distribution of the Sample Population</td>
<td>43</td>
</tr>
<tr>
<td>4. Computer Networking Distribution of the Sample Population</td>
<td>44</td>
</tr>
<tr>
<td>5. Employment Distribution of the Sample Population</td>
<td>44</td>
</tr>
<tr>
<td>6. Anonymous Networking Distribution of the Sample Population</td>
<td>45</td>
</tr>
<tr>
<td>7. Qualitative Response Distribution Per Question</td>
<td>46</td>
</tr>
<tr>
<td>8. Gender Impact of Qualitative Survey Questions</td>
<td>48</td>
</tr>
<tr>
<td>9. Age Impact of Qualitative Survey Questions</td>
<td>49</td>
</tr>
<tr>
<td>10. Education Impact of Qualitative Survey Questions</td>
<td>50</td>
</tr>
<tr>
<td>11. Employment Impact of Qualitative Survey Questions</td>
<td>51</td>
</tr>
<tr>
<td>12. Networking Experience Impact of Qualitative Survey Questions</td>
<td>53</td>
</tr>
<tr>
<td>13. Anonymous Networking Impact of Qualitative Survey Questions</td>
<td>53</td>
</tr>
</tbody>
</table>
Digital Anonymity: Investigating the Open Threat by the Hidden User

**Introduction**

The act of attempting to be anonymous can take many forms to try to hide one’s true identity. Reasons for anonymity can include performing such acts for fun as one would wear a costume for Halloween as well as doing it out of necessity as law enforcement would do while undercover. Anonymity can also be done for malicious reasons such as wearing a ski mask while robbing a bank. Being anonymous can also be applied to non-bodily forms to include digital anonymity.

Digital anonymity is defined as a process one takes in an attempt to conceal one’s identity while performing online transactions using technologies such as the internet or other forms of digital networks. Several technologies exist for allowing computer users anonymity while online. The most popular is the Tor Browser which allows users to not only conceal their identity to websites they visit but also conceal their on-line destinations from their Internet Service Providers (ISPs). It can also be used to bypass particular filters that may be in place to prohibit a user from gaining access to a particular network.

The Tor browser relies on a distributed network of peers interconnected and dispersed over large geographical regions. When a user attempts to connect to a particular server, the communication path connects to many different peers throughout this network with encryption occurring each time. Because of the many different layers of networking involved in this process, this technology is referred to as onion routing (Peng, 2014).
Problem Statement

Anonymizing technology has many pros and cons. The good part is that it allows computer users the opportunity to remain anonymous online while conducting personal or business related activity. This allows the user a layer of protection against those attempting to cause harm to them by locating their machine in an attempt to inject malicious code onto their system or in an attempt to steal their identity. It also provides a benefit to law enforcement agencies and other government agencies to conduct anonymous transactions in the attempt to collect intelligence to investigate or communicate with those involved with criminal behavior. The bad part of using this technology is that criminals use it as well to conduct illegal activities online. They use it to connect to underground sites and make transactions to purchase weapons, drugs, and other items that have illegal implications to include illegal pornography or to illicit services. By using this type of technology, it is difficult for law enforcement agencies to identify or locate the criminal.

Purpose of Study

This study intends to prove that technologies offering digital anonymity aren’t totally foolproof and that computer user’s perception of this technology is unjustified. It will also help determine the level of knowledge the U.S. Government has as it relates to investigations of the technology. The research methods used will gauge computer user’s knowledge of the technology as well as their opinion on such technologies to include how it relates to the U.S. citizen’s right to privacy as outlined in the Fourth Amendment. It is believed that the topic of digital anonymity is an important one to understand as anonymizing software and processes are federally unregulated. Federally regulating such activity would allow for more simplicity and faster
turnaround times for investigations into crimes using the technology however it may also introduce a controversial standpoint of the government regulating too much of the citizen’s life and prohibiting freedom of communication.

**Significance of the Study**

This study will build on past studies involving American computer user’s views on anonymous networks. The intention is to provide statistics of the common computer user and their involvement with using anonymous networking technologies. It will also illustrate the common computer user’s views regarding regulation for this technology to include the extent of government involvement. This study will incorporate literature reviews of studies of a similar nature to include digital anonymity, computer crimes using this particular technology, and past government and law enforcement investigations on this topic. It will also examine the legal ramifications of anonymizing technologies as they pertain to the United States Constitution and current laws outlining cybercrimes.

The results of the survey to be administered for this study will be used to gauge the common American citizen’s view on regulation towards anonymizing technology. The results of this study, in conjunction with the research being performed, will also be used to draw a conclusion to inform the audience on the usefulness and potential limitations of anonymizing technologies and to aid in the formation of policy and laws governing cybercrimes using this technology.
Assumptions, Limitations, and Delimitations

This research study of digital anonymity will be conducted under the assumption that significant information regarding past studies of similar topics will be readily available and that the majority of individuals approached will participate in the survey questions. It is further assumed that the audience participating in the survey come from diverse backgrounds and will provide responses indicative of a productive sample for this study.

Limitations of this study include a non-diverse background of participants who can be physically approached to participate in this study due to geographical, time, and financial constraints allocated for this study. The risk for this limitation will be mitigated by using technology to include social media and e-mail to reach a diverse background of participants in an efficient manner. The scope of this study will be limited to the literature review and the survey questions outlined in the testing methodology of this research paper. The participants of this study will be limited to U.S. citizens as the focus of this paper revolves around legal ramifications of U.S. policy and law. No other particular demographic will be selected for participant segregation. The survey used for this research topic will only include close-ended and Likert scale questions requiring the user to select the choice corresponding to their background and opinions.

Definition of Terms

Digital anonymity

The act of using technologies or processes to conceal the true identity of a user involved in online activities.
Onion routing

A technology that involves many different computers in a diverse geographical setting to construct an ad hoc peer-to-peer network of users allowing for many layers, or hops, to be included as the communication method between client and server.

Online marketplaces

Marketplaces that involve the selling of goods or services using computer networks as its predominant means of soliciting buyers and sellers.
Literature Review

Introduction

Concealing one’s identity has been perpetrated for centuries for various reasons. Digital anonymity can be a useful tool for computer users who wish to remain anonymous while using computer networks to include the internet. It can also serve as a useful tool for cybercriminals. Early forms of anonymizing technologies simply used network and software technologies to obscure a computer user’s IP address and other identifying components. Over the years this technology has become sophisticated. Users are now able to download software that provides them the capability to create a virtual network of anonymizing tools.

Several studies exist identifying different types of anonymizing technologies to include how they are used for legal and illegal means. The studies also illustrate how the U.S. Government and law enforcement agencies have gotten better at investigating crimes using anonymizing technologies. Even though the technology is better understood by investigating officials there is still a knowledge gap.

Anonymous Network Overview

The term anonymity is derived from Greek vocabulary to mean “without a name”. The term as used in modern society means to describe an action an individual or group takes in an attempt to mask their identity (Vocabulary.com, 2014). Examples of anonymity dates back many years to include examples illustrated in The Bible. Many Christians feared persecution due to their idealistic view of Christianity during the Iron Age. Because of this, many of these Christians conformed to “anonymous Jahwism”, or anonymous Christianity (Grenholm, 1996,
p.69). During the Trojan War, circa 1240 BC, the Greeks constructed a large wooden horse sculpture and left it at the gates of their adversaries, the Trojans. The Trojans believed that this was a gift from the departing Greeks when in all reality the hollowed horse sculpture contained Greek soldiers inside of it. The Trojans wheeled the horse into their closed off compound where the Greeks attacked them once inside (Gill, 2015). The Greeks were able to mask themselves as a wooden sculpture to gain access to the Trojan compound where they otherwise were denied entry. This example illustrates not only an early form of anonymity but also how a group can obtain anonymity as opposed to an individual.

Anonymity can be obtained in physical form by the use of a mask or other forms of concealment however anonymity can also be obtained in a non-physical environment to include digital media. The term digital anonymity describes attempts to make a user of a digital network, such as the internet, anonymous while conducting transactions online. Over the past couple of decades, many technologies have been developed to provide anonymity for online users with the first occurring in 1983 in the form of a blind signature where the message content is disguised prior to being signed in the form of a certificate (Gritzalis, 2006, p. 120).

Since the advent of digital anonymity in 1983, many technologies and methods have been used in an attempt to gain anonymity. Without the use of sophisticated tools, anonymity only goes so far. A user’s internet service provider (ISP) maintains records of their subscriber’s activities. By issuing a subpoena, government entities could gain access to user’s activity logs maintained by their ISP. With the use of anonymizing tools users can gain some additional privacy with regards to their ISP. However there are additional advantages for using these tools such as the ability for an individual in a particular country gaining access to informative material that may be otherwise filtered and blocked by their country as well as comfort in knowing that
the user’s identity is concealed which proves valuable to victims of particular crimes or circumstances. Digital anonymity also proves valuable as a security measure as attackers may not gain user information that they would otherwise need to launch an attack on the user. Anonymizing technology has proven to be a powerful tool for government and law enforcement officials in conducting investigations and operational activities. Government and law enforcement officials can use these technologies to conceal their identity to garner a successful operation and gather information they may otherwise not be successful in doing as using their true identity may thwart such attempts (Rapoza, 2004).

When it comes to technology, there are two separate types of trust. The first is trust in the technology itself to include hardware and software. Trust in technology comes from standards put in place to ensure quality products are distributed to the public and that the technology will function as expected. The second type of trust is that of the human using the technology. Trust in humans comes from experience of past interactions with individuals. Many advances in technology allows for particular freedoms offered to computer users. Users are given the opportunity to work independently and remotely, to include telecommuting, in their job. The employee must be trusted that time outside of the traditional office is used effectively and that resources given to them are used wisely. Students now have the opportunity to complete their studies online. They are trusted by their educational institution and instructors that they complete their assignments as instructed and without the aid of outside sources that may be prohibited by that institution. Though the user may be known in these circumstances, there is a level of anonymity presented in that the work presented by individuals using these remote resources may not be original content authored by the users as expected. There is a direct correlation of anonymity and trust as it relates to privacy. Often online resources can operate in a non-governed
manner to include sites that track users which can collect a varying amount of data from users. Because of this, some feel that the user has a right to use technology to an extent to provide them with the maximum amount of anonymity as they can afford. On the flip side, others feel that using anonymizing technology users may feel more adventurous and take more risks than they normally would which may verge on the line of illegal activity or simply perform actions they normally wouldn’t which could have potential consequences (Baggio & Beldarrain, 2011, p. 1-10).

**Methods to Provide Digital Anonymity**

Because the use of computers have become so widespread and common in everyday life, users often become desensitized to the fact that they are identifiable when they log in to a network. Users connect to network by using internet protocol (IP) addresses. IP addresses are unique to the network and are used to identify digital media such as computers or other devices. Often a user will connect to the internet with their ISP providing an IP address which will often provide geographical identification of where the user is connecting from and can even provide information that may identify the user as well. Users can also leave traces of where they have been if their web browser is configured to use cookies. Cookies are used by web servers as a means of easier and faster identification of users when they connect to their services. There are several technologies available for users to attempt to navigate networks in an anonymous manner to include the Tor web browser, Tails operating system, Obfsproxy, bridge relays, and Darknets (Loshin, 2013).

The use of peer-to-peer (P2P) networks has provided a general framework of what constitutes an anonymous network. This technology uses a hybrid overlay design (Gritzalis,
A hybrid overlay network provides a cost effective resource sharing mechanism that depends on user cooperation. Users of this type of network store resources locally on their computers or servers will all computers or servers being interconnected in a heterogeneous environment. Many of these networks became popular with users sharing media to include copyrighted music and movies as well as other software content. It also became the network of choice for many online gamers as they could connect remotely with other users to play against one another (Mushtaq & Ahmed, 2007, p. 1-2). Because of the overlaying technology to include multiple network hops with many of those connections having subpar connections to the internet, there is a loss of performance however what is gained is anonymity. Another drawback to P2P networks is when a node is injected into the mesh with the intention to cause harm. This node may intentionally inject viruses into the system with the potential to populate onto many systems within the P2P network. It may also distribute ‘junk data’ which includes files that user’s had no intention to download. Because of these limitations, trust models have been developed to identify nodes that are more reliable on the P2P network to include increase speed and a history to include recommendations. Those nodes with higher trust ratings usually become the nodes user’s attempt to connect to and those with lower ratings tend to not be used as heavily (Li & Chunjian, 2013).

The Darknet consists of a network of computer nodes constructed in a hybrid overlay design similar to the P2P technology as previously discussed. Darknet networks use multiple nodes to connect client to server. In networking, the more computer nodes used to make a connection, also referred to as hops, the more difficult it is to trace a network connection. Darknets also use specialized software to provide encryption and obscurity between connections. This technology often used obscure protocols for communication and hidden domains that often
guarantee the average web user aren’t able to discover by accident or through regular searches. These domains often hide within the confines of an anonymized network with the only way to access it is with the use of anonymization software and the web address that has been provided by another party that serves as an invitation for the user to access. Because of the mysterious nature of these domains, the sites contained on them change frequently. Links to references are constantly changed or removed in an effort to maintain obscurity. Many Darknets contain search engines which often point to references in an effort to publicize additional anonymization techniques as well as literature of a political nature (Chacos, 2013).

The most popular anonymizing software tool to use is the Tor web browser. The use of this browser allows a user to web surf anonymously. This technology is referred to as onion routing as the hybrid overlay design and use of multiple nodes to create a connection provides many layers. As mentioned previously, multiple nodes are used to provide a connection between client and server. Each connection of these nodes is encrypted except for the final hop between the last Tor node and the server. Even though the connection between the final node and the server are in clear text, the risk is often minimized as the communications in clear text appear to come from the final node to the server as opposed to the original client and server. Domains within the Tor network are hidden with access only obtainable if the user knows the obscure address to the site. Sites within the Tor network are often designated with the .onion suffix. When sites are created within the Tor network, their uniform resource locator (URL) is auto generated using a public cryptography with the results being what appears to be a group of random characters. An example of a site within the Tor network is http://d93kfu5nsu4jwmr8.onion/. These sites will not resolve to a regular web browser or searchable by a standard search engine as they don’t reside on the common internet. Access to
these sites is only permitted through the use of the Tor browser which connects the user to the Tor network (Chacos, 2013).

Anonymizing software can also take the form of entire operating systems. There are Linux distributions available for download that provide the user anonymity for use on the internet. The most popular of these distributions is titled Tails. This operation system is stored and run from a DVD or USB drive. The user simply inserts the DVD or USB drive into their computer and boot into the media to provide a temporary user environment. The operating system provides software and services that allow users to perform web surfing as well as use communications tools. Because the operating system runs as a virtual environment, the user is unable to save data within the system however this limitation also provides anonymity as nothing from the user’s sessions is saved. Once the user is finished using the operating system they can boot into their actual computer’s operating system with no traces of their Tails session being saved anywhere. It is reported that many journalists use this technology to maintain confidentiality of their sources to include one of the most notorious whistleblowers in recent history, Edward Snowden (Finley, 2014).

Other technologies are available to be used in conjunction with other anonymizing technologies that further alter their network communication path. Many novice users may not be able to use these particular technologies as they required an understanding of networking to include implementation and the purpose of particular networking tools to include bridges and proxies. In general terms, bridges are used as a means to connect two local area networks (LANs) and enables packets to be transmitted between the two segments. Computers on the two segments appear to reside on one segment to the rest of the world as packet frames are delivered amongst all computers on both segments using media access control (MAC) addresses for
filtering (Comer, 2009, p. 295-296). Proxies are nodes put in place with the only intentional use being to verify the identities of other nodes and URLs and forward packets from one node to another. This networking method is often used to minimize security risks by using a proxy to check a URL for security risks prior to retrieving the page for the user (Comer, 2009, p. 525). The Tor suite offers a tool called obfsproxy. This tool converts traffic from the client to a bridge into traffic that appears to be something other than what it truly is. If someone were to inspect the traffic across the network, this traffic would appear to be innocuous as it is being masked from the traffic it truly is. This tool supports many protocols with each having a specified method in which it is transformed. Network traffic using Tor HTTP requests would be transformed for resembles regular HTTP traffic (Tor Project, 2015).

There are many anonymous proxy software solutions each offering something different. Java Anon Proxy (JAP) takes it a step further and provides a level of anonymity it a somewhat different manner. This technology injects ‘dummy’ traffic into real traffic streams. This technology connects users in a similar hybrid overlay technology already discussed. It also provides encryption between the client and server. The encryption in conjunction with the dummy traffic makes traffic analysis extremely difficult if not impossible. An HTTP proxy toolkit named Anonymizer removes header information from packets allowing for a level of anonymization as the sender information is removed (Kelly, Raines, Baldwin, Grimaila, & Mullins, 2012). These are just a few examples of anonymization techniques however a simple online search will reveal numerous different products available.

So far only anonymization techniques for wired networks have been discussed. There are also many ways to provide anonymization using wireless networks as well. The IEEE 802.11 standards allow for devices to have mobility as they were designed for. With this level of
mobility and convenience comes the potential for attackers to gain access to devices and track mobile users. There are many products available to wireless users to provide a level of anonymity such as MASK. MASK ensures that wireless communications isn’t exposed to anyone sniffing wireless communication traffic. It creates a dedicated circuit with a virtual data delivery mechanism (Kelly, Raines, Baldwin, Grimaila, & Mullins, 2012). Many of the wireless anonymization tools provide a similar technology. It is important to have familiarity of networking to know when certain anonymization techniques aren’t available. For example, the wireless tools described above will only protect the communications from the mobile device and the access point. Once traffic is received by the access point, it is more than likely being sent over the wire where the wireless anonymization tools will not work.

**Previous Surveys on Digital Anonymity**

The article titled *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* examines digital anonymity in a society enthralled with technology. The authors point out that the United States has no laws or policies outlining any right to anonymity and that any anonymizing technology should be viewed as a convenience and not a necessity. The authors do however illustrated that anonymity can be viewed as a component to the constitutional right to privacy and that and individual’s perspective on security and safety can dictate a need for anonymity. Arguments arise as the majority of jurisdictions in the United States require a form of identification with a requirement to produce identification when prompted by a law enforcement or government official. This example provides a clear distinction between anonymity in a digital world versus a physical setting. In order to operate an automobile on a public road or highway, the driver must possess a driver’s license and display it when required by law enforcement. Many jurisdictions have placed regulations that affect the public to
include commercial environments. Some have made it mandatory that consumers display an official form of identification when attempting to seek refunds or exchanges in stores. The United States provides very little opportunities for anonymization. Even in a court of law, the use of pseudonyms is prohibited in attempts to protect witnesses. In contrast, the U.S., has the stringiest policies with regard to anonymization compared to their counterparts. The United Kingdom supports the use pseudonyms to protect the identity of witnesses. Canada fully supports the use of pseudonyms for undercover operatives and for the protections of witnesses. They also allow them to be used in online use in an effort to remain anonymous in court (Kerr, Lucock, Steeves, 2009. p.438-440).

Previous studies show a correlation of not only anonymization tools but also tools used to penetrate or infect other computer systems. In the study titled Markets for Cybercrime Tools and Stolen Data, the authors indicate that in the past twenty years attackers have gotten less knowledgeable however tools and methods have gotten more sophisticated. Some may wonder how this is possible with the answer being quite simple. Currently the more knowledge attackers are developing sophisticated methods and toolsets for others to use. The tools and process developed are used by less experienced attackers who may only know to how to use the tools but not understand the theories that support them. This results in an increased number of attackers with better toolsets as opposed to fewer attackers using more rudimentary exploits as they did twenty years ago. The survey indicates that there is now a highly profitable market for computer exploits to include zero-day exploits. The authors further elaborate that much of this activity is not openly known as the marketplaces for these activities occur on Darknets (Ablon, Libicki, & Golay, 2014. p.25-26).
According to the article titled *Defining Anonymity and its Dimensions in the Electronic World* by Bart Goddyn, there are six different levels of anonymity. These levels are categorized from level 0 to level 5. Level 0 is no identification. This means that an individual uses a computer system in which the system relates to the user via a username or other form of credentials. The true identity of the user is unknown. Level 1 is anonymous identification. This level of anonymization is defined as the user being identifiable by the computer system but not as a particular user. Level 2 is pen-name identification. The computer user is known by the system by a username, pseudonym, or other form of credentials. The true identity of the individual is unknown by the system. Level 3 is latent identification. True identities of users of a computer system are known to the system. Pseudonyms are used for users so that other users are unable to identify them. Level 4 is usual identification. Users of a computer system are identified to the system by user credentials to include usernames and passwords. Level 5 is super-identification. This level is similar to level 4 where user credentials to include usernames and passwords are used by the system to identify users however this level is done in a secure manner. The author of this survey elaborates on threats to computer users such as having their personal information compromised while using digital resources or having their sessions hijacked. He also discusses opportunities for other sources to identify the user’s computer use and use it for marketing opportunities in the form of spam and other unsolicited forms of marketing being delivered to the user. The marketer’s usually employ technologies that will anonymize their identities so that the user cannot determine the true source of the information (Goddyn, 2001).

In a recent study regarding digital anonymity titled *Anonymity, Privacy, and Security Online*, it was determined that the majority of internet users would prefer to be anonymous during their online sessions. According to the survey used to conduct this study, 86% of online
users had previously used anonymizing technologies in an effort to mask their identity or internet usage. The types of anonymization outlined in the survey included clearing cookies, using encryption for email, name anonymization, and masking their IP address. More elaborate means of anonymization were used by 55% of the survey participants to elude particular individuals as well as government and organizational entities. Many different views on level of anonymization were discovered with 59% of the participants believing that total digital anonymity is not obtainable and 37% of participants believing that it is possible. The survey also provided metrics regarding personal online experiences. Twenty-one percent of the respondents have had a computer account compromised. Thirteen percent had experienced issues or conflicts in their personal lives because of content they had posted online. Twelve percent had experienced online harassment. Eleven percent has had their personal information compromised to include financial account numbers and Social Security Numbers. Six percent had experienced defamation of character due to online activity. Six percent of participants had been victims of online scams resulting in loss of money. Four percent of respondents encountered physical danger due to certain online activities. One percent had lost their job or employment and educational opportunities due to certain online activities. With regards to the respondents views on laws and regulations addressing online privacy, 68% felt that current laws were not sufficient in protecting users. Twenty-four percent of the participants believed that the current laws addressing online privacy were sufficient. The survey was administered by the Princeton Survey Research Associates International where they polled 1,002 adults aged 18 and older. They concluded that the majority of internet users felt that they had sufficient knowledge of their online activity and are aware of what key information about them is made publicly online. It further states that concern of privacy with regards to online activity is increasing among individuals over recent
years and they would like more control over personal content that is published online as well as confidence in the data they download. Data confidence can include files that are free of viruses and malware and only includes information that is expected to be contained in the files (Raine, Kiesler, Kang, & Madden, 2013).

The use of digital media is on the rise for those under the age of 18. Because of the frequent use of such media and the potential for the under aged users to utilize online resources there is a concern among parent and guardians. The concern is mostly two-fold to include online content that is available to minors and the potential for other users to monitor the activities of these minors in an attempt to communicate with them or provide other means of corruption. In a survey administered in a report titled *Parents, Teens, and Online Privacy: New Survey Findings from Pew Research Center and Berkman Center* parents of minors utilizing online content were polled to determine their views on particular subjects. 81% or the respondents were concerned about the magnitude and types of information that is available for online users with 46% of them being very concerned. Seventy-two percent were concerned with the interaction of individuals with their children in which they don’t know. Sixty-nine percent of the parents were concerned with their child’s online activity and the effects it may have on future professional or educational opportunities. Sixty-nine percent were concerned with how their child conducts themselves online and the effect it has on the child’s reputation. The results from the aforementioned survey questions were used in an effort to illustrate the potential for improved government regulations and intervention of where and how personal information is collected online. The results from additional questions from the survey were used to illustrate the rise in use of social media applications by minors. Minors of parents who use social media sites are likely to use the same sites with 39% of parents of children using social media helping them set their accounts up. It
further illustrates that 44% of the parents responding to the survey have taken measures to block personal content regarding their children online. This includes any information and isn’t limited to content in social media sites. Fifty percent of the parents responding to the survey have taken measures to apply filters and block content that their child is able to obtain or have used technologies to monitor their child’s online activity. The survey polled 802 parents of teens aged 12-17. The results from this survey show that there is concern regarding online use not only by individuals but by other members of their household (Madden, 2012). It also illustrates a consensual belief that more elaborate laws and policies should be put in place to regulate the amount of personal information that is available online.

With the increase of cybercrimes and threats to computer users it is critical that government and law enforcement agencies keep up with the latest trends in technology. This includes anonymous networks and how they are being used to conduct cybercrimes. Law enforcement agencies have always taken the approach of trying to be equal in capabilities if not one step ahead of the criminals. This is why they train to be proficient in using weapons and improve their driving skills in the event they are faced with having to use force to apprehend their suspect. It is often believed that physical skills such as these are fairly easy to improve on with hours of training. One thing that law enforcement has sometimes fallen behind the criminals in is the use of technology. Those who commit crimes with the use of technology are often advanced in the technology arena to include having a higher than average aptitude in software development, programming, and networking. Law enforcement is traditionally not trained in these avenues however with the increased use of technology they have identified the need to sharpen their skills or employ individuals who are trained and educated in these areas. The Government Accountability office (GAO) highlights four major areas that should be
accomplished in order to prepare for battling cybercrime. First they recommend that the crimes are reported. Second they indicate the need for sufficient capabilities for law enforcement in both the analytical and technical arena. The third area for recommendation is a multi-jurisdiction environment with cooperation from all law enforcement agencies to battle cybercrime. Finally they indicate the need to promote awareness on information security practices. It is estimated that it takes approximately 12 months for a law enforcement official to become proficient in a technology. In the digital arena, this is a relatively long timeframe as technologies become obsolete quickly or new methods are discovered to throw law enforcement off the trail while using the technology (Wolf, 2009).

The Journal on Telecommunications & High Technology Law addresses some key points with improving regulation on certain technologies. One of the authors, Molly Van Houweling, illustrates how she believes that technological protection measures (TPMs) can be put in place to help limit the number of cybercrimes that occur. Often some of these TPMs do not require government intervention with may being mandated without the involvement of the government. She uses an encryption method, CSS, as a technology that was devised without government intervention that has improved control access to DVD and other copyrighted material and has helped decrease the number of pirated digital copyrighted material. The author feels that certain regulations could be put forward with the help from Congress that does not require an agency to oversee it. She has the opinion that the Federal Communication Commission (FCC) is often the governing body of many polices with regards to digital provision however they should not be due to the limitation of the scope of work that the agency was put in place to perform (Van Houweling, 2005). Another recommendation for preventing cybercrimes is to regulate Bitcoins. Bitcoins are a digital currency that has security features such
as encryption built in. Transactions involving Bitcoins are considered anonymous which makes it the ideal currency for laundering and other criminal activity. This has been the currency of choice for marketplaces that operate in the confines of the Darknet. A survey titled *Regulating Bitcoin* examines the digital currency and conducts a feasibility study regarding the regulation of the currency. The author points out that the current lack of regulation on the currency is more than likely due to the lack of understanding of the technology that the currency comprises of. How can an agency regulate something it doesn’t understand? The author believes that over time the U.S. Government will provide updates to laws to provide oversight to the currency and more important placing a tax on such currency. He further feels that if regulations are placed on the currency, then the currency will be less desirable and eventually fade out of use as the idea behind Bitcoins was to provide an unregulated form of digital currency (Macurak, 2014).

**Concerns Surrounding Digital Anonymity**

Digital anonymity can be a very good thing as it provides a layer of security for many internet users. With all good things there are also the bad aspects. Anonymous networks have been used for many years to provide anonymity to individuals who have intentions to remain anonymous for the sake of eluding law enforcement due to illegal behavior being conduct online. The behavior includes stalking and harassing individuals online and conducting illegal transactions. Many marketplaces are hosted on the Darknet. These marketplaces provide goods and services of the legal nature but also provide a wide range of goods and services that are illegal in the U.S. Among these are drugs, weapons, prostitution, human trafficking, and media to include photographs and videos.
Using Darknets to conduct business of the illegal nature is not a recent problem, it traces back to 1969 with the introduction of the first connected computer network system. The Pentagon developed a network system called ARPANET which was designed to connect the Government in a manner to only include trusted sources. It was a sophisticated system for and solved a huge problem of transferring information in an efficient manner. Soon after the introduction of such a system, students and universities began using similar networks. Just as the Government was able to conduct business over closed networks so were many others (McCormick, 2014).

By the 1980s the Internet protocol (IP) had become an industry standard. Numerous closed networks were being used to host anything from gambling operations to illicit pornography. These network clusters were referred to as “data havens”. By the late 1990s digital networking had become a common tool to many as many homes now had access to the Internet due to the large number of Internet service providers (ISPs) allowing individuals with a modem attached to their computer to connect to their main server giving them unlimited opportunities to explore all the internet had to offer. Among these offerings were peer-to-peer networks. Access to these peer-to-peer networks were usually password protected and only allowed access to their members. The majority of these networks provided access to copyrighted material such as music and movies. Sites, such as Napster, soon appeared allowing peer-to-peer access to many to download an unlimited supply of copyrighted media for free. It didn’t take long for the Government and entertainment industry to begin cracking down on these sites. Many of the top Napster downloaders were soon identified with examples being made of them to discourage others to download media that was copyrighted using peer-to-peer networks. It didn’t take long
for technologies to advance to counter these attempts by the government and entertainment industry (McCormick, 2014).

At the beginning of the 2000s, software developers and hackers began creating networks that were deeply rooted into the darkest regions of the internet. Ian Clarke, a software developer, introduced Freenet based as a rebellious act against those who were attempting to put an end to peer-to-peer download sites. This move not only allowed for copyrighted material to still be exchanged it also allowed for other illegal content such as child pornography and instructions on how to build explosives. Soon after Clarke’s introduction of Freenet, many others followed suit in an attempt to gain financial riches. Many succeeded however many also failed miserably as they spent a lot of resources to purchase top of the line equipment and realized that many of sites similar to Freenet weren’t in it for the money with little potential for profit (McCormick, 2014).

In 2002, a concept of a hybrid overlay networking technology was introduced by the U.S Naval Research Laboratory. Because of the number of layers of networking this technology runs on, it was referred to as “The Onion Router” of Tor for short. While using this technology, the user’s location and IP address is concealed to the general public. It was introduced as a means for U.S. Government operatives to remain anonymous to conduct operations and as a means for repressed insurgents in other countries to communicate with U.S. Government entities. Once released for public consumption Tor became a heavily used product to enhance Darknet sites and how users connect to them. By 2005 it was estimated that more than half a million movies were downloaded per day using the Darknet. This resulted in approximately $34 billion in losses to the entertainment industry in that year (McCormick, 2014).
In 2009, the Bitcoin was developed as a form of untraceable digital currency with built-in security features such as encryption. This form of currency was a huge hit for those conducting business online as previous attempts failed due to users being able to copy money from other attempts. Because of the security and anonymizing features, it became the currency of choice for many marketplaces on the Darknet (McCormick, 2014).

By the early 2010s marketplaces had sprouted up in many areas of the Darknet. When Governments or law enforcement agencies feel that they had come close to catching criminals running and using these sites, processes and technologies would change to throw law enforcement off the trail. Some of these techniques included using file formats that were obscure and not searchable by common web browsers as well as dynamic database queries. All efforts were done to protect Darknet users by providing them anonymity and hiding them in a manner when their activity and many marketplaces are unable to be discovered by everyday internet users using regular search engines and web browsers. In order to find particular Darknet sites, a user needs to be invited so to speak. Once the user has been granted permission to access a site, they are given a roadmap instructing them on how to gain access to a particular Darknet site. Once a user gains access to the Darknet there is a wiki available to most users title Onionland. Onionland contains useful links and how-tos to help users navigate the Darknet. This wiki contains links and directories of certain categories such as where to find drugs and other goods and services. Many users find the majority of this wiki to be useless as sites is continuously shifting location in an effort to not be discovered by law enforcement. Because of the continuous shift, it is difficult to maintain the links in the wiki. Once users become familiar with navigating the Darknet the possibilities of purchasing just about anything and everything is endless. Not everything about Darknet is bad as it allows freedom of speech which is useful for citizens of
countries who observe more strict regulations of speech that what is offered in the U.S. (Chacos, 2013).

Among all of the marketplaces on the Darknet, one stood out as a leader. The Silk Road utilized the anonymity offered by the Darknet by operating solely in a Tor network environment. The Silk Road, which opened for business in 2011, also required the use of Bitcoins as currency for all transactions. This black market offered products that were otherwise difficult or impossible to find using other means. It specialized in drugs, drug paraphernalia, weapons, and pornography. The main page resembled any other online marketplace to include account information pertaining to orders. The banner at the top counted down the days and time to “Four Twenty” which is a reference to the consumption of cannabis and is often celebrated on April 20. On the left is a menu of products offered to include drugs, apparel, books, computer equipment, digital goods, drug paraphernalia, electronics, and fireworks. Under the drug category are subcategories to include cannabis, dissociatives, ecstasy, opioids, prescription, psychedelics, and stimulants (Christin, 2012, p. 1-3).

Even though the Silk Road specialized in products that were deemed socially unacceptable and illegal by U.S. standards, they did place restrictions on what could be sold through the site. It prohibited the selling of products that would hard or defraud others to include stolen products and information, credit card numbers, counterfeit currency, weapons, services that offer assassinations, and anything related to pedophilia. The buying and selling of weapons were once acceptable on the Silk Road but were transferred to their sister site dedicated to only buying and selling of weapons. Sellers could choose to not list their items in public and only sell them in a privatized manner on the site where the buyer and seller could communicate via messages using the site. The site developed a sophisticated method of transactions to include
only the use of Bitcoins which would be placed into an escrow account upon time of purchase and only be released to the seller once the item had been received by the buyer. If a seller were to not deliver as promised the funds would be returned to the buyer and the seller would be expelled from using the service (Christin, 2012, p. 3-4).

In a survey titled *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace* it was determined that in the site’s prime there were a few hundred sellers with approximately $1.2 in sales per month. It was also determined that the most common product being sold through the marketplace was marijuana and cannabis with 17.3 % of sales comprising of it. All other drugs comprised of 39.6 percent of all sales. It was further determined that U.S. citizens comprised of the largest number of sellers on the site at 43.83% as well as the largest percentage of buyers at 35.15% (Christin, 2012, p. 9-11).

**Actions to Improve Investigations Involving Digital Anonymity**

Law enforcement has traditionally struggled with keeping pace with technologies that are used to conduct cybercrimes. Local law enforcement agencies usually rely on the expertise of the larger governmental agencies to support their investigations. The large agencies have a larger budget and are able to employ more professionals that smaller law enforcement agencies are able to do. Also most federal agencies had had years of experience in investigating particular crimes and have even developed some of the tools that are used to commit some crimes. The downside of this is that federal agencies usually won’t aide in most cases handled by local law enforcement because the crime is usually minimal in nature compared to the larger issues the agency has to deal with. Most cases have to have a fairly large impact or be part of an ongoing investigation for larger agencies to become involved. Other issues come into play with local law enforcement
investigations to include jurisdiction. Many cybercrimes occur over a fairly large geographical footprint with participants of the crime residing in different towns, states, and even counties. Many of the smaller law enforcement agencies have been working with federal agencies to better understand what constitutes a cyber-threat and how to respond to cybercrimes. The Secret Service initiated a program that trains local law enforcement agencies to be better prepared in combating cybercrimes. Since the program’s inception in 2008 they have trained approximately 1,400 state and local law enforcement officers with the demand for the training being more than the agency can accommodate (USA Today, 2013).

With anonymizing technologies being so advanced it may concern some that law enforcement and Government agencies aren’t prepared to investigate most crimes. This may be true to an extent however there are some advantages Government agencies have. Andrew Lewman, Tor’s executive director, has admitted that authorities are alerted by the company when illegal activity is identified using the Tor technology however he also admitted that they do not actively search for it (Koul, 2012). According to a spokesman for the U.S. Naval Research Laboratory the group never considered the security and anonymity implications that are faced today. Part of their strategy was for the technology to take off in that many users would utilize the technology. The more users using the network the better the chances are for Government operatives to blend in and increase their chances of remaining anonymous while conducting operations. By making the software open source, it increased the odds that more computer users would use it. The Government apparently still believes in the technology. According to the Tor Project’s 2013 financial statement, the U.S. Government provided them $1.8 million that year with the majority of the funds coming from the State Department and the Department of Defense. This makes up approximately 60% of the project’s funding (Simons, 2014).
Notorious whistleblower, Edward Snowden, has reported that the National Security Agency (NSA) has made attempts at disabling Tor or to lessen the anonymity of its users.

Ironically, Snowden used the Tor network to send information to The Guardian Newspaper when he came public with the allegations (Simons, 2014). Many believe that the U.S. Government has a secret backdoor to the Tor network or other advantages since the technology was originally developed by the U.S. Navy (Loshin, 2013). Tor’s top executive, Andrew Lewman, has strongly denounced the allegations and pointed out that government agencies outside of the U.S., to include Sweden, also fund the project. He argues that the funding should be considered a grant as opposed to a procurement effort. The government stands by their claim that they do not desire a backdoor and acknowledge their contributions to the project is done in an effort for them to use the software during operations (Fung, 2013).

Government and law enforcement agencies usually don’t reveal their methods of operation in an effort to not have them compromised. However, there are many indications that the Government and law enforcement agencies understand the technology better. In 2014, authorities and Europe and the U.S. closed up multiple illegal websites operating in the confines of the Darknet. Many believe that the Government was able to crack the sophisticated encryption that enables Tor to be anonymous however many also believe that if this were the case then there would be implications that the software would no longer be used. The mere fact that authorities were able to track down the anonymous users who ran these sites indicates that the game of digital anonymity has taken a turn with the Government and law enforcement agencies evening the score a bit. A spokesman for the Tor Project stated that the group doesn’t know how the Government was able to identify those users and that they are investigating. During the seizure of Darknet sites, the authorities were able to shut down 414 web domains resulting in the arrest
of 17 individuals. They also seized $1 million worth of Bitcoins and approximately $224,000 worth of cash and precious metals. Among the shutdown was the illegal Darknet heavy hitter the Silk Road (Dalton & Grossman, 2014). Among the arrests were 26 year old Silk Road originator and owner, Blake Benthall. A description of the accounts leading up to the arrest indicate that old fashion police work may have been used instead of cutting edge technological advances in law enforcement. During the investigation an undercover agent obtained a job with the website which allowed him direct interaction with Benthall. While placing Benthall under surveillance, the agent was able to draw a correlation of his physical location and activity and compare it to his online presence. It was observed that when Benthall would leave his house, his anonymous online persona would go inactive. Once he returned home the account would go active (Leger, 2014).

Law enforcement and Government officials aren’t the only ones targeting illegal activity perpetrated online. In 2012 the notorious hacker group Anonymous demonstrated their continuous quest to perform activities of what they feel is right and what they feel law enforcement is incapable of doing. They began their quest, dubbed #OpPedoChat, to put an end to online pedophilia activities by identifying those sites on the Darknet that specialize in child pornography and shutting the sites down by force in the owners fail to comply with their demands to terminate service. This isn’t the first time the group Anonymous has target online pedophiles. In 2011 they gained access to a server and subsequently shut down 40 sites that participated in exchanging child pornography. The group also publicized personal details of members of the sites (Mlot, 2012). This indicates that not everyone using Darknet technologies are in it for malicious intent not are all hacking groups completely geared to causing harm to others.
Summary and Remaining Questions

Digital anonymity has proven to be a valuable tool for both legal and illegal purposes. In recent years, it has been proven that the U.S. Government and law enforcement agencies have increased their knowledge regarding the technology. Many marketplaces operating in the confines of the Darknet have been shut down with the site owners identified and arrested. Individuals participating in illegal anomalous activities such as child pornography and cyber stalking have been able to be identified by law enforcement and distanced from their victims.

Many questions exist surrounding digital anonymity. The largest question still looms of how will the Government and law enforcement agencies better prepare themselves to keep pace with the technologies that are used to conduct cybercrimes? Another big question is what is the future of anonymous networking?

A new social media application has recently made its way to the market. The application titled Secret was developed by two former Google employees. Similar to current social media applications like Facebook and Twitter, Secret is used to connect users. The major difference is that the users are anonymous. When the app is installed on a smartphone, it pulls in data from the user’s contact list to form a circle of friends. When the user posts and update or other content the members of their circle are able to see the updates and content however they won’t know which of their friends posted it. By providing anonymity, the developers of the application hope that the members using the anonymous social media app will better portray the user’s true persona as opposed to an online persona that used social media as a way of bolstering themselves to include obtaining a large number of friends. The developers hope that the users will be more concerned with seeking quality of friends over quantity (Stinson, 2014). Though the theory sounds
interesting and unique the question remains of how will the content from that and similar apps be exploited? Will this introduce a new challenge to hackers in exploiting the technology and exposing the user’s true identities? Also how will this technology play into technology misuse to include stalking and cyberbullying?

Another looming question is with the recent seizures of the sites containing marketplaces on Darknet, have users lost confidence in technologies such as Tor? What is the next form of anonymous networking? A new form of anonymous networks have recent been identified. This unique form of anonymous networks is referred to as “Dead Drops”. The concept behind “Dead Drops” is that devices, such as USB drives, are located throughout the world for public consumption. These USB drives are fixed in locations such as drilling a hole in a brick wall, inserting the USB drive, then patching the hole with concrete. This leaves only the end of the USB drive that inserts into a computer exposed so that the thumb drive is left intact but can still be plugged into a computer. This allows users to take their peer-to-peer network offline and reduce the chances of their identity or activities being compromised. Of course users of this technology are taking a huge risk of inserting a foreign USB drive into their computers with a high potential of obtaining a virus or other malicious file onto their computer. It also appears to be inconvenient for many users as they would physically have to travel to the destination that is housing the content they desire from a particular USB drive. The outstanding questions regarding this form of technology is how will the footprint of the investigation grow for law enforcement? Not only will they have to identify where the USB drives are located but also set up physical investigations to include observing which individuals are utilizing USB drives of interest (Sumitra, 2015).
Methodology

Data Collection Technique

This study on digital anonymity was completed in two parts. An exhaustive literature review was used to provide information regarding anonymizing technologies. It was also used to illustrate previous surveys on the topic of the technology itself to include instances of when the technology has been lawfully used to provide an increased security posture for computer users. Instances of when anonymizing technologies have been used to conduct cybercrimes are included in the literature review to illustrate how the technology has been a useful tool to conduct unlawful activity as well. Additionally, the literature review highlights previous surveys of how the United States Government and law enforcement agencies have performed investigations of cybercrimes that have used anonymizing technologies.

A survey was also used to collect data from participants to capture their opinions on anonymizing technologies and the extent of regulation they feel should be placed on the technology. The anonymous survey was constructed using the survey feature of Google Docs with a link to the survey provided to the participants to complete online. Microsoft Excel was also used to analyze the data and to construct charts containing statistical proof points of various metrics. The data collected from the survey was sent to and stored on a secure Google Drive account. The survey contained 6 demographic questions and 12 qualitative questions. A copy of the survey used is illustrated in Appendix A.

The demographic questions were used to determine the participant’s gender, age, work background, level of education, and skill level as it pertains to computer networking and digital anonymity. The quantitative questions were used to help determine the participant’s opinion on
the usefulness of anonymizing technologies and level of regulation they feel should be applied to the technology. The qualitative questions were divided into three sections. The first section was used for the participants to indicate their opinion towards the use of anonymous networks. These questions were directed towards individual users and governmental use of the technology. The second section asked the participants to indicate their opinion of the United States Government’s involvement of anonymous networks. The questions in this section were used to determine the participant’s opinion of the readiness of government and law enforcement to investigate cybercrimes using anonymizing technologies. It also gauged their opinion on the extent of regulation that should be imposed on the technology and if they felt that regulating the technology would violate their constitutional right to privacy. And finally the third section captured the participant’s opinion on the use of anonymizing technologies with online marketplaces. The quantitative portion of the survey used a Likert scale to determine how strong the participant’s felt towards the questions. The choices in the scale were strongly disagree, somewhat disagree, unsure, somewhat agree, and strongly agree. The participants were asked to select the answer that their opinion aligned with for each statement.

**Hypothesis and Research Questions**

This study is designed to prove or disprove five hypotheses. The following null hypothesis will be evaluated using results derived from the literature review and the survey.

**H1.** There are limitations to anonymizing technologies that users aren’t familiar with which may not make user’s online sessions as covert as expected.

**H2.** There is statistical evidence that the majority of common computer users are not familiar with digital anonymizing technologies.
H3. There is statistical evidence that the majority of common computer users believe that anonymizing technologies should be regulated.

H4. There is statistical evidence that the majority of users of digital anonymizing technologies believe that anonymizing technologies should not be regulated.

H5. There is statistical evidence that the majority of U.S. citizens believe that online marketplaces that operate solely via anonymous networks and are involved in illegal activities should not be in operation.

The questions in the survey were developed to help solve three main problems. Problem one this research investigates is the awareness of anonymous networks to common United States citizens. Anonymous networks are used by many different categories of computer users: normal users, journalists, law enforcement, activists, whistleblowers, business executives, bloggers, militaries, IT professionals, and high profile individuals (Tor Project, 2015). Two major groups of computer users; those using the technology to obfuscate their online footprint to commit cyber-crimes and those using the technology in official government or law enforcement capacity to conduct investigations or other tactical activities. To answer what the opinions are of common computer users in the United States with regards to anonymous networks the following questions were asked:

- Are anonymous networks a useful tool to conceal one’s identity when using the internet?
- Do anonymous networks provide total online anonymity?
- Should anonymous networks be standard practice for internet users?
- Are anonymous networks useful in conducting investigations for government and law enforcement agencies?
Problem two this research investigates is the preparedness of United States Government and law enforcement officials in investigating cyber-crimes using anonymous networks. The complexity of cyber-crimes continues to increase. Because of this, investigating officials have a difficult time keeping abreast of the latest technologies in computer crimes (USAID, 2015, p.2). To answer what the opinions are of common computer users in the United States with regards to the United States and law enforcements involvement of anonymous networks, the following questions were asked:

- Should the United States Government and law enforcement agencies be prepared to investigate crimes involving anonymous networks?
- Should anonymous networks be regulated by the government?
- Would regulating the use of anonymous networks infringe on the constitutional right to privacy for United States citizens?

Problem three this research investigates is the use of anonymous networks to facilitate transactions conducted between consumers and marketplaces. Many marketplaces exist on the Darknet and only allow connections to be made with the use of anonymous networks (Ablon, Libicki, & Golay, 2014. p.25-26). To answer what the opinions are of common computer users in the United States with regards to online marketplaces using anonymous networks the following questions were asked:

- Are private anonymous peer-to-peer networks acceptable even if they are used to engage in illegal activity to include sharing of copyrighted material and selling of items and services that are illegal in the United States?
• Are private anonymous peer-to-peer networks acceptable as long as they are not used to engage in illegal activity?

• Are online marketplaces that only allow digital anonymity acceptable even if they engage in the selling of items and services that are illegal in the United States?

• Are online marketplaces that only allow digital anonymity acceptable as long as they are not used in illegal activity?

• Is the United States Government justified in shutting down online marketplaces and incarcerating the marketplace owners for allowing illegal items to be purchased and sold through the website?

**Subjects and Setting**

The participants solicited to partake in the survey represent a small sample of the United States population. Solicitation for participation of the survey was conducted using social media applications and e-mail correspondence. The author has approximately 450 acquaintances with whom he is linked to using the social media applications Facebook and LinkedIn. These acquaintances are all United States citizens with an age range of 18 to 70 years old. They are distributed throughout the United States with the majority residing on the east coast. The sampling of educational and professional background is also diverse. Educational levels range from high school or equivalent to the doctorate level. Professions have a large distribution to include many different white and blue collar careers in the public and private sector as well as students and those who are unemployed. The author is also a member of various information technology groups on social media to include disciplines in security and digital forensics. Social media solicitation consisted of status updates to the author’s pages for his friends and followers
to read as well as postings to the walls of the IT groups. The solicitation provided a brief description of the survey, asked for participation, and provided the link to the web site hosting the survey.

The author is employed as an information technology professional in the Washington D.C. area and has a network of peers in that profession. Disciplines in this profession include network administration, systems administration, information technology security, software development, integration, support, and project management. Solicitation for survey participation was sent to these professionals via e-mail. The e-mail provided a brief description of the survey asking for participation and providing a link to the web site hosting the survey.

The minimum number of participants desired for this survey was 106. This would produce a 90% confidence level with an 8% margin of error as a representation of the internet users in the United States.

**Statistical Analysis**

The Likert scale for the quantitative portion had five possible answers ranging from strongly disagree to strongly agree. Each of the five answers were given a weight from 1 to 5 with 1 being strongly disagree and 5 being strongly agree. The data was compiled using the average weight from each question to determine the most popular answer. The data from the quantitative questions and from the qualitative data were entered into a Microsoft Excel spreadsheet to provide statistical analysis as well as graphically illustrate the results. This level of analysis helped determine what the most popular answer was for each qualitative question categorized by demographic variables of gender, age, educational background, profession, computer networking background, and background in using anonymous networks. This helped
determine the variance and deviation of not only the quantitative results as a whole but also for each demographic category.

**Limitations of the Study**

Limitations for this study included constraints for time, financial, and participation resources. Since this study was conducted for a Master’s thesis, it was conducted within the timeframe allotted for the students to complete the study which was approximately two weeks. Also because this was for a Master’s thesis with no financial backing provided to the researcher, there was no monetary budget allocated for this study.

Though the researcher utilized his professional and social media contacts, actual participation resulted in 83 participants. This equated to 19% of respondents from his social media and professional contacts. The limitation was a result of potential participants not actively reviewing their e-mail or social media status updates as well as refusal to participate.
Results

Survey Demographics

The survey used for this study had 83 participants. Of those participants, the primary demographics consisted mostly of females at 73%, were in the age range of 41-50 years old at 39%, and were educated at the Master’s degree level at 36%. The majority of the participants were employed by a company, government, agency, or private entity at 86% with the majority of them being at a novice level with regards to computer networking at 42%. The majority of participants had no prior experience or knowledge of anonymous networking technologies at 61%. Table 1 provides a breakdown of the survey respondents by gender, age, education, profession, computer networking experience, and anonymous networking experience. Figures 1-6 provides further analysis illustrating the distribution of each demographic category by percentage.

The qualitative questions asked in the survey are listed in Table 1. These questions were provided in a Likert Scale format in the survey. The answers available for each questions were strongly disagree, somewhat disagree, unsure, somewhat agree, and strongly agree. In order to provide statistical analysis to each of the responses they were given the following weights: Strongly disagree = 1, somewhat disagree = 2, unsure = 3, somewhat agree = 4, and strongly agree = 5. The distribution of responses to the qualitative questions is illustrated in Figure 7.

The distribution of responses shows that there is a general consensus for each question for most questions. There were two responses that clearly stand out from the others as having an overwhelmingly general agreement from the participants. Approximately 50% of the survey participants answered “strongly disagree” towards the question asking their beliefs towards
anonymous peer-to-peer networks being acceptable to engage in illegal activity (Q8). Also approximately 50% of the participants answered “somewhat agree” towards the question asking their beliefs towards anonymous peer-to-peer networks being acceptable as long as they are not used to engage in illegal activity (Q9). The remainder of the most popular responses per questions is:

- Q1. Anonymous networks are a useful tool to conceal one's identity while using the internet.
  - Unsure = 45% and somewhat agree = 31%

- Q2. Anonymous networks provide total online anonymity.
  - Unsure = 42% and somewhat disagree = 30%

- Q3. Anonymous networks should be standard practice for all online users.
  - Unsure = 35% and somewhat disagree = 33%

- Q4. Anonymous networks are useful for government agencies and law enforcement to conduct investigations.
  - Unsure 35% and agree = 33%

- Q5. The United States government and law enforcement agencies should be prepared to investigate crimes involving anonymous networks.
  - Strongly agree = 41%

- Q6. Anonymous networks should be regulated by the government.
  - Unsure = 30% and somewhat agree = 22%

- Q7. Regulating use of anonymous networks infringes on United States citizen's constitutional right to privacy.
  - Somewhat disagree = 28%, unsure = 28%, and somewhat agree = 23%
Q10. Online marketplaces that only allow digital anonymity are acceptable even if they engage in the selling of items and services that are illegal in the United States.
  o Strongly disagree = 46%

Q11. Online marketplaces that only allow digital anonymity are acceptable as long as they are not used in illegal activity.
  o Somewhat agree = 37%

Q12. The United States government is justified in shutting down online marketplaces and incarcerating the marketplace owners for allowing illegal items to be purchased and sold through the website.
  o Somewhat agree 35%

Table 1

Number of Survey Participants by Demographics

<table>
<thead>
<tr>
<th>Gender</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>22</td>
</tr>
<tr>
<td>Female</td>
<td>61</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Age</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>18 - 20 Years Old</td>
<td>1</td>
</tr>
<tr>
<td>21 - 30 Years Old</td>
<td>6</td>
</tr>
<tr>
<td>31 - 40 Years Old</td>
<td>22</td>
</tr>
<tr>
<td>41 - 50 Years Old</td>
<td>32</td>
</tr>
<tr>
<td>51 - 60 Years Old</td>
<td>12</td>
</tr>
<tr>
<td>61 Years Old and Over</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Education</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Some High School</td>
<td>1</td>
</tr>
<tr>
<td>High School Graduate or Equivalent</td>
<td>7</td>
</tr>
<tr>
<td>Trade School Certificate</td>
<td>2</td>
</tr>
<tr>
<td>Some College</td>
<td>11</td>
</tr>
<tr>
<td>Associate's Degree</td>
<td>11</td>
</tr>
<tr>
<td>Bachelor's Degree</td>
<td>20</td>
</tr>
<tr>
<td>Master's Degree</td>
<td>30</td>
</tr>
</tbody>
</table>
DIGITAL ANONYMITY

<table>
<thead>
<tr>
<th>Employment</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Employed by a Company, Government Agency, or Private Entity</td>
<td>71</td>
</tr>
<tr>
<td>Self-employed</td>
<td>1</td>
</tr>
<tr>
<td>Unemployed and Seeking Employment</td>
<td>0</td>
</tr>
<tr>
<td>Unemployed and Not Seeking Employment</td>
<td>4</td>
</tr>
<tr>
<td>Military</td>
<td>0</td>
</tr>
<tr>
<td>Student</td>
<td>3</td>
</tr>
<tr>
<td>Retired</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer Networking Experience</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>10</td>
</tr>
<tr>
<td>Only Studied It or Read About It</td>
<td>9</td>
</tr>
<tr>
<td>Novice</td>
<td>35</td>
</tr>
<tr>
<td>Mid-level</td>
<td>24</td>
</tr>
<tr>
<td>Expert</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Anonymous Networking Experience</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>51</td>
</tr>
<tr>
<td>Only Studied or Read About Them</td>
<td>24</td>
</tr>
<tr>
<td>Have Used Them</td>
<td>8</td>
</tr>
</tbody>
</table>

Figure 1: Gender Distribution of the Sample Population
Figure 2: Age Distribution of the Sample Population

Figure 3: Education Distribution of the Sample Population
**Figure 4:** Computer Networking Distribution of the Sample Population

**Figure 5:** Employment Distribution of the Sample Population
Table 2

**Qualitative Questions**

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Indicate your opinion towards the following statements regarding the use of anonymous networks. [Anonymous networks are a useful tool to conceal one's identity while using the internet.]</td>
</tr>
<tr>
<td>Q2</td>
<td>Indicate your opinion towards the following statements regarding the use of anonymous networks. [Anonymous networks provide total online anonymity.]</td>
</tr>
<tr>
<td>Q3</td>
<td>Indicate your opinion towards the following statements regarding the use of anonymous networks. [Anonymous networks should be standard practice for all online users.]</td>
</tr>
<tr>
<td>Q4</td>
<td>Indicate your opinion towards the following statements regarding the use of anonymous networks. [Anonymous networks are useful for government agencies and law enforcement to conduct investigations.]</td>
</tr>
<tr>
<td>Q5</td>
<td>Indicate your opinion towards the following statements regarding the government's involvement of anonymous networks. [The United States government and law enforcement agencies should be prepared to investigate crimes involving anonymous networks.]</td>
</tr>
<tr>
<td>Q6</td>
<td>Indicate your opinion towards the following statements regarding the government's involvement of anonymous networks. [Anonymous networks should be regulated by the government.]</td>
</tr>
<tr>
<td>Q7</td>
<td>Indicate your opinion towards the following statements regarding the government's involvement of anonymous networks. [Regulating use of]</td>
</tr>
</tbody>
</table>

**Anonymous Networking Experience**

![Chart showing distribution of anonymous networking experience among the sample population.](chart.png)

*Figure 6: Anonymous Networking Distribution of the Sample Population*
anonymous networks infringes on United States citizen's constitutional right to privacy.

Q8 Indicate your opinion towards the following statements regarding the use of online marketplaces. [Private anonymous peer-to-peer networks are acceptable even if they are used to engage in illegal activity to include sharing of copyrighted material and selling of items and services that are illegal in the United States.]

Q9 Indicate your opinion towards the following statements regarding the use of online marketplaces. [Private anonymous peer-to-peer networks are acceptable as long as they are not used to engage in illegal activity.]

Q10 Indicate your opinion towards the following statements regarding the use of online marketplaces. [Online marketplaces that only allow digital anonymity are acceptable even if they engage in the selling of items and services that are illegal in the United States.]

Q11 Indicate your opinion towards the following statements regarding the use of online marketplaces. [Online marketplaces that only allow digital anonymity are acceptable as long as they are not used in illegal activity.]

Q12 Indicate your opinion towards the following statements regarding the use of online marketplaces. [The United States government is justified in shutting down online marketplaces and incarcerating the marketplace owners for allowing illegal items to be purchased and sold through the website.]

Figure 7: Qualitative Response Distribution Per Question
Impact of Gender and Age

There were few significant differences with how females and males responded. The largest differences between the two were with question 7. While the average consensus was unsure males tended to lean closer toward strongly agreeing that regulating the use of anonymous networks infringes on U.S. citizen’s constitutional rights. The females solidly remain unsure for that particular question. Males also tended to vary noticeably differently with question 1, 6, and 8. While women tended to lean towards unsure, males leaned closer to somewhat agree that anonymous networks are a useful tool to conceal one’s identity while using the internet.

Both genders somewhat disagreed with the question of private anonymous peer-to-peer networks are acceptable even if they are used to engage in illegal activity to include sharing of copyrighted material and selling of items and services that are illegal in the U.S. However females leaned closer towards strongly agreed while males leaned closer to unsure. With regards to the question if anonymous networks should be regulated by the government, females solidly answered unsure while males leaned closer to strongly disagree.

The largest variance of responses to each question was realized in the age category. The 21 – 30 and 31 – 40 age groups leaned towards strongly agree that anonymous networks provide total online anonymity and the 51 – 60 and 61 and over groups leaned closer to unsure. The average for all respondents for this questions was unsure with it being close to somewhat agree. Question 3 asks if anonymous networks should be standard practice for all online users. The 61 and over age group somewhat disagreed while the average of the remainder of the participants were unsure. The 21 – 30 age group somewhat disagreed that anonymous networks should be regulated by the government with the average of the remainder of participants being unsure.
The 41-50 age group felt unsure if regulating anonymous networks infringes on U.S. citizen’s rights while the rest of the population leaned closer to somewhat agree. The 18 – 20 age group dramatically varied from the remainder of the population on questions 9 and 11. The respondents from that group strongly agreed that private anonymous peer-to-peer networks, as well as online marketplaces using anonymous networks, are acceptable as long as they are not used to engage in illegal activity. The remainder of the participants leaned more toward being unsure and somewhat agreeing to both questions. Finally, the 51 – 60 age group strongly agreed that the U.S. Government is justified in shutting down online marketplaces and incarcerating the marketplace owners for allowing illegal items to be purchased and sold through the website while the rest of the population somewhat agreed.

Figures 8 and 9 illustrate the responses to all of the qualitative questions. The responses include the average for all participants as well as the average for each group of participants.
Impact of Education

Education didn’t appear to make much of an impact on the responses given for the qualitative questions. Again, there were some outliers. For answer 12, the participants with the doctorate degree strongly agreed that the U.S. Government is justified in shutting down online marketplaces and incarcerating their owners for allowing illegal activates to occur on them. The same participants answered lower than average for questions 2, 3, 7, 8 10, and 11. Participants with a trade school certificate answered higher than average on questions 5, 7, 11, and 12. The drastic fluctuation responses are believed to be due to the few participants with these particular degrees or certificates. All other education levels were fairly consistent with one another. The average of all responses based on education is illustrated in Figure 10.
Most of the responses for the qualitative questions were relatively even based on employment with a few exceptions. The self-employed participants averaged lower than the rest of the population for questions 1, 2, 3, 4, and 6. They also scored higher than average for questions 7, 8, 10, and 12. As did the 18 – 20 age group, the student population stood out as having a higher than average response to questions 9 and 11. The significant fluctuation may be due to the few responses received for those particular categories. The majority of the participants were employed by a business or government entity. The responses from that category closely
align with the average from all participants. The comprehensive average responses per questions are illustrated in Figure 11.

**Figure 11:** Employment Impact of Qualitative Survey Questions

**Impact of Experience**

The average answers for the qualitative questions from the survey remained constant for the most part regardless of computer networking background. There were a few exceptions. The participants that consider themselves experts answered higher than average for questions 1, 4, 7, 10, and 11. The same category averaged lower than the rest with regards to question 2. Other noticeable outliers are prevalent with the group that has only studied or read about computer networking. This group tended to responded lower than average for questions 2, 4, 5, 6, and 12 as well as higher than average for questions 7, 10, and 11.
The participants who have actually used anonymizing technology tended to respond to some of the questions differently while those who have read about the technologies or have no experience with them tended to answer similar. The participants that have used the technologies showed fairly drastic differences in responses for questions 6, 7, 8, 10, and 12. This group felt that anonymous networks should not be regulated by the government while the rest of the participants were unsure. They also agreed that regulating anonymizing technologies would infringe on the constitutional rights of U.S. citizens while the rest of the population was unsure. The users of the technology was unsure if private anonymous peer-to-peer networks are acceptable if they are used to engage in illegal activity while the rest of the population felt that it was unacceptable. They were also unsure if the U.S. Government is justified in shutting down online marketplaces that engage in illegal activity and incarcerating their owners while the rest of the population agreed that it should be done. Figures 12 and 13 illustrate the comprehensive average of all participants as well as each individual group.
Figure 12: Networking Experience Impact of Qualitative Survey Questions

Figure 13: Anonymous Networking Impact of Qualitative Survey Questions
Discussion

The survey that was conducted as part of this research helped confirm many of the assumptions outlined in the hypothesis. The survey also helped solidify many of the items outlined in the literature review to include the average computer user’s knowledge of anonymous networks as well as the government’s involvement and use of this technology.

Though the number of expected participants fell slightly less than expected, a good sampling of participants were recognized. There were some outliers that made some of the results appear to be significantly different from others. There was only one participant in the 18 – 20 age range, one participant that was self-employed, and one participant having a Doctorate degree. Because there was only being one participant for these categories, they represented the entire category. This indicates a personal preference as opposed to the preference for a group.

The consensus from the participants taking the survey was that many were unsure regarding the questions that asked for their opinions of anonymous technologies. Two of the questions asked if they felt anonymizing tools were useful in concealing one’s identity and if they feel that the technology provides total anonymity for online users. The demographic responses also demonstrated that 61% of the survey participants had no experience with anonymous networking technologies. These responses prove that hypothesis 2 (H2) is correct as there is statistical evidence that the majority of common computer users are not familiar with digital anonymizing technologies. The literature review emphasizes this conclusion as well. The majority of the articles discussed many using anonymizing technologies in an effort to conduct illegal activities online. The review also indicates that anonymizing technologies are useful in concealing one’s identity however they often don’t provide total anonymity for a user. User’s
often install software to provide that provide anonymity however it isn’t configured correctly or to optimum settings resulting in lack of anonymity. If implemented correctly, the technology can prove to be quiet useful however there is often a trade-off in the form of network performance. Often in order to achieve a high level of anonymity, multiple hops need to be deployed. With the introduction of additional hops come higher degrees of latency and packet loss resulting in network degradation.

The second most discussed topic in the literature review was the government and law enforcement’s use of the technology to conduct certain activities to collect intelligence. The survey indicates that 41% of the population feels that anonymizing software is a useful tool for government and law enforcement officials. The literature review reinforces this opinion with the government acknowledging the use of anonymizing software as well as illustrating cases where law enforcement officials were able to successfully use anonymizing tools to conduct investigations and other operational activities.

There was also minimal discussion regarding particular computer users who have, at one time, been a victim of certain online abuse to include cyber-bullying and cyber-stalking. There was no documentation found of common computer users simply using anonymizing technology to conduct every-day online activities. These results can be used to conclude that the majority of U.S. citizens who are also computer users are not involved in illegal online activities, not involved in cyber operations in an official government or law enforcement capacity, nor have they been a victim of a cybercrime to the extent that they feel the need to deploy anonymizing technologies.
The survey indicates that 42% of the population is unsure if anonymous networks provide total online anonymity. One thing to consider is that the majority of survey participants had little to no experience with computer technology. Those who responded as being an expert in computer networking disagreed that the technology provided a total anonymizing solution. The participants who have studied or used the technology also disagreed that current anonymizing technologies provide total anonymity. Those who understand the principles behind network technologies generally understand the principles behind anonymizing technologies. They understand that the technology isn’t perfect and that there are opportunities for failure with the technology, especially if it is implemented incorrectly. The responses received prove that hypothesis 1 (H1) is correct that there are limitations to anonymizing technologies that users aren’t familiar with which may not make user’s online sessions as covert as expected.

Because there are two specific groups with regards to anonymizing technologies, those who understand it and those who don’t, it is expected that there are varying opinions toward the software with regards to regulation. Those who had no prior experience with anonymizing technology was unsure if the technology should be regulated while the participants who have used it felt that the technology should not be regulated. The results from the survey indicate that hypothesis 3 (H3) is correct with there being statistical evidence that the majority of common computer users, 43% of the population according to the survey, believe that anonymizing technologies should be regulated with 31% of the population being unsure. It also indicates that hypothesis 4 (H4) is correct with there being statistical evidence that the majority of users of digital anonymizing technologies, 88% of the population according to the survey, believe that anonymizing technologies should not be regulated.
It was previously discussed that there is reason to believe that there are three specific user groups for anonymizing technologies with that being those who use it to conduct illegal activities, government and law enforcement, and victims of cyber-crime. It is obvious that those who use the technology to commit a crime would not want the technology to be regulated. As previously discussed, the U.S. Department of the Navy developed the technology used by TOR. It was also released that U.S. Government entities to include the National Security Administration (NSA), Department of Defense (DoD), and the State Department provides approximately 60% of the TOR Project’s funding. Because of this, many speculate that the U.S. Government already regulates this specific technology to an extent to include placing backdoors into the software that is used (Fung, 2013). Some of these agencies have responded to many of these various allegations admitting that they do use the software in the course of their business. The reason for the funding is so that they have the technology available for use in operational environments and not to gain an advantage over criminals. The U.S. Government and law enforcement agencies also know that if they announced involvement to include placing backdoors into this software that many users would cease in using that particular technology making any advantage they had in combating crime conducted using the software disappear.

The overall consensus of the survey participants is that strongly agree that online marketplaces using anonymizing technologies are acceptable only if they are not used by their users to sell or purchase items or services that are illegal in the U.S. They also agree that the U.S. Government is justified in shutting down online marketplaces and incarcerating their owners for allowing illegal items to be purchased and sold through the website. This proves that hypothesis 5 (H5) is correct with there being statistical evidence that the majority of U.S. citizens, 52%
according to the survey, believe that online marketplaces that operate solely via anonymous networks and are involved in illegal activities should not be in operation.

One of the survey questions asked the participants if they felt that the use of anonymous networks should be standard practice for those who use the internet. The majority of the respondents were unsure with 35% of them answering in this manner. This response may be a result of the majority of the respondents also not being familiar with the technology. Those who didn’t answer “unsure” had a tendency to disagree, 33% according to the survey, that the use of the technology should be standard practice. This response may be a result of anonymizing technology being cumbersome to implement with a strong understanding of computer networking being necessary to implement it as well as the trade-offs of using the technology.
Summary

The survey and literature review used for this research were conducted for two primary purposes. First, it was used to gauge the knowledge level of computer users in the U.S. Second, it was used to determine the readiness of the U.S. Government and law enforcement agencies in combatting cyber-crimes using anonymizing technologies.

The results of this study show that there are three primary users of anonymizing technology with that being those who use it to commit cyber-crimes or other illegal activities, government and law enforcement, and individuals who wish to be anonymous because they have been victimized online. It also illustrates that the majority of computer users aren’t familiar with anonymizing technology. This proves that users aren’t typically concerned with concealing their online identity and that the technology is usually used for concealment for a particular reason other than general computer and user security. Those who are familiar with anonymizing technology or have used it have a distinctive opinion opposing government regulation of the technology while the population who is not familiar with the technology is in favor of regulations. The overall consensus is that anonymizing technologies should not be used for conduction illegal activities and that the government and law enforcement agencies are within their rights to shut down websites that use the technology for illegal purposes as well as incarcerate the website’s owners. The overall opinion from the participants also believes that anonymizing technologies should be used for anyone who wishes to remain anonymous online as long as they are not participating in illegal activities.

The literature review illustrates that there is a never ending process in technology. Law enforcement and government agencies often have a difficult time in staying abreast of recent
technologies used in cyber-crimes. Even though government and law enforcement agencies often fall behind the curve, it is apparent that they are getting better at not only understanding the various technologies used, but also using them to capture criminals and better understand the patterns criminals use to obfuscate their identities and network traffic. This is demonstrated by the recent major online marketplaces that were heavily involved in illegal transactions being shut down. Not only were the websites identified, the owners were as well enabling law enforcement agencies to make arrests of the owners and bring them to justice.
Recommendations

Government and law enforcement agencies should continue their never-ending quest to stay current with technologies. Not only should they be aware of the technologies, but also be well trained to know the underlying means in how the technology works. By thoroughly understanding how it works, they will be better prepared in responding to threats with criminals using the technology. They should also be diligent in knowing when technologies have become obsolete in the criminal world and know what they are using as a replacement.

The schedule and scope for this research were very narrow. The survey should be expanded on to allow for more time and more participants. It would be beneficial to conduct this survey to participants who weren’t well represented with this effort to include college students. It would also be beneficial to interview U.S Government and law enforcement personnel who use the technology what their thoughts are on the technology and how they have been able to use it to conceal their identities as well as capture criminals that have used the technology.

The major question that remains unanswered is the confidence level of users of anonymizing technologies. Because of the recent closures of online marketplaces such as the Silk Road, do users feel that the technology is better understood or that law enforcement has an advantage over them? Further research should be conducted to understand not only the confidence level but also if there has been a decline in using the technology over the past year.
List of References


Retrieved from
http://web.a.ebscohost.com.ezproxy1.apus.edu/ehost/detail/detail?sid=f972fe85-6ca9-482b-b8c8-373ae72a6584%40sessionmgr4002&vid=0&hid=4106&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=aph&AN=93911125


Rapoza, J. (2004). Who am I? ; There are lots of good reasons for 'net anonymity. *EWeek,* 21(33), 41. Retrieved from
http://search.proquest.com/docview/198532669?accountid=8289


Appendix A

Digital Anonymity Survey

Dear Participant,

My name is Derrick Rumer and I am a student of American Public University in the Information Technology Department under the supervision of Dr. Novadean Watson-Stone. You are invited to participate in a research project entitled: Digital Anonymity: Investigating the Open Threat by the Hidden User. This study is being conducted to determine the American public’s opinion regarding technologies that conceal a computer user’s identity and the government’s involvement in regulating these technologies. This study has been approved by American Public University’s Institutional Review Board.

The following survey was developed to ask the participant a series of questions regarding anonymizing technologies. It is our hope that information obtained from this survey can be used to identify potential improvements to policies pertaining to this technology as well as areas for improvement regarding investigations of crimes using this technology. There are no identified risks from participating in this research. To learn more about anonymous networks, there are many sites on the internet to include the Tor Project. The Tor Project is the world leader of anonymous web browsing technologies and provide an overview of anonymous networks located at: https://www.torproject.org/about/overview

All participants must be 18 years of age or older. This survey is anonymous and participation is voluntary. You may refuse to participate in the survey entirely as well as elect to not answer every question without consequence. The survey will take approximately 10 minutes to complete. No compensation will be received for participating in this survey and responses will only be used in aggregated form to complete a Master’s level thesis. Neither the researcher nor the University has a conflict of interest with the results. The data collected from this study will be kept in a secure file until the completion of graduation requirements.

If you should have further questions regarding your rights as a participant of this study, please contact the IRB Chair, Patricia J. Campbell at pcampbell@apus.edu or the Office of the Academic Dean at academicdean@apus.edu.

Participation in this survey implies consent to the terms outlined. Thank you for considering my request.

Regards,
Derrick Rumer

Definition of Terms
Digital anonymity: Using a process or technology to conceal a computer user’s identity or destination in an attempt to remain anonymous or to bypass security filters in place to otherwise block access to a user.

Anonymous networks: Software or a system that is used by computer users to conceal their identity.
Peer-to-peer networks: Computer systems that are interconnected in an attempt to share resources without the use of a centralized administrative system.

Demographics

The following section includes non-identifiable questions about you to categorize your responses.

Indicate your gender
Choose your gender
- Male
- Female
- Other

What is your age?
Choose the range that your age falls into
- 18 - 20 years old
- 20 - 30 years old
- 31 - 40 years old
- 41 - 50 years old
- 51 - 60 years old
- 61 years old and over

What is the highest level of education you have completed?
Choose only one
- Some high school
- High school graduate or equivalent (GED)
- Trade school certificate
- Some college
- Associate's degree
- Bachelor's degree
- Master's degree
- Doctorate degree

What is your employment status?
Choose only one
- Employed by a company, government agency, or private entity
- Self-employed
- Unemployed and seeking employment
- Unemployed and not seeking employment
- Military
What is your level of computer networking experience?
Choose only one
- None
- Only studied it or read about it
- Novice
- Mid-level
- Expert

What is your experience with anonymous networks?
Choose only one
- None
- Only studied or read about them
- Have used them

Anonymous Networks Questions - Quantitative

The following questions will be used to determine your opinions regarding anonymous networks.

Indicate your opinion towards the following statements regarding the use of anonymous networks
Mark only one answer for each statement

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Somewhat Disagree</th>
<th>Unsure</th>
<th>Somewhat Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous networks are a useful tool to conceal one’s identity while using the internet.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous networks provide total online anonymity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous networks should be standard practice for all online users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous networks are useful for government agencies and law enforcement to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Indicate your opinion towards the following statements regarding the government's involvement of anonymous networks

Mark only one answer for each statement

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Somewhat Disagree</th>
<th>Unsure</th>
<th>Somewhat Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>The United States government and law enforcement agencies should be prepared to investigate crimes involving anonymous networks.</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Anonymous networks should be regulated by the government.</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Regulating use of anonymous networks infringes on United States citizen's constitutional right to privacy.</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
</tbody>
</table>

### Indicate your opinion towards the following statements regarding the use of online marketplaces

Mark only one answer for each statement

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Disagree</th>
<th>Somewhat Disagree</th>
<th>Unsure</th>
<th>Somewhat Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private anonymous peer-to-peer networks are acceptable even if they are used to engage in illegal activity to include sharing of copyrighted material and selling of items and services that are illegal in the United States.</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Private anonymous peer-to-peer networks are acceptable as long as they are not used to</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
</tbody>
</table>
engage in illegal activity.

Online marketplaces that only allow digital anonymity are acceptable even if they engage in the selling of items and services that are illegal in the United States.

Online marketplaces that only allow digital anonymity are acceptable as long as they are not used in illegal activity.

The United States government is justified in shutting down online marketplaces and incarcerating the marketplace owners for allowing illegal items to be purchased and sold through the website.
I, Derrick Rumer, owner of the copyright to the work known as Digital Anonymity: Investigating the Open Threat by the Hidden User hereby authorize APUS to use the following material as part of his/her thesis to be submitted to American Public University System.

<table>
<thead>
<tr>
<th>Page</th>
<th>Line Numbers or Other Identification</th>
</tr>
</thead>
</table>

________________________

Signature
May 7, 2015

Dear Derrick Rumer,

The APUS IRB has reviewed and approved your revised application # 4.2015-41 (submitted April 16, 2015). The approval covers one calendar year. Should you need an extension beyond the one year timeframe, an extension request will have to be submitted. However, this does not mean your research must be complete within the one year timeframe. Should your research using human subjects extend beyond the time covered by this approval, you will need to submit an extension request to the IRB.

Sincerely,

[Signature]

Patricia J. Campbell
Chair, IRB
School of Science, Technology, Engineering, and Math

MS in Information Technology

The thesis for the master's degree submitted by

Derrick Rumer

under the title

Digital Anonymity: Investigating the Open Threat by the Hidden User

has been read by the undersigned. It is hereby recommended

for acceptance by the faculty with credit to the amount of

3 semester hours.

(Signed, first reader) (Date) _____June 19, 2015_____

(Signed, second reader, if required) ______________________ (Date) ______________

Recommended for approval on behalf of the program

(Signed) ______________________ (Date) __________

Recommendation accepted on behalf of the program director

(Signed) ______________________ (Date) __________

Approved by academic dean
This capstone has been approved by Dr. Novadean Watson-Stone for submission, review, and publication by the Online Library.

Author’s name: Derrick B. Rumer

Title: Digital Anonymity: Investigating the Open Threat by the Hidden User

Professor: Dr. Novadean Watson-Stone

Second reader, if required: ____________________________

Program: Master’s of Science in Information Technology with a concentration in Digital Forensics

Pass with Distinction: YES

Keywords/Descriptive Terms: digital forensics, forensics, security, investigate, investigation, TOR, Darknet, anonymous, anonymous networks, digital anonymity

[ ] Contains Security-Sensitive Information