2016

I Got It On Silk Road: An Examination of Knowledge and Attitudes Towards Tor and the Dark Web

Zachary Mitchell
University of Mississippi. Sally McDonnell Barksdale Honors College

I Got It On Silk Road: An Examination of Knowledge and Attitudes Towards Tor and the Dark Web

By Zachary Dylan Mitchell

A thesis presented in partial fulfillment of the requirements for completion
Of the Sally McDonnell Barksdale Honors College
The University of Mississippi
University, Mississippi
May, 2016

Approved by:

_____
Advisor: Dr. Bart L. Garner

_____
Reader: Dr. Brian J. Reithel

_____
Reader: Dr. Dwight D. Frink

Abstract

As communication technology has grown, so has the potential for crimes to be committed with the new technology. The United States government has attempted to stay current with the times by introducing legislation to increase federal power to detect and stop these crimes, but some feel that some of these new laws and acts reduce personal freedoms and liberties. Enter Tor and the Dark Web, a set of often misunderstood tools and web-based resources designed to make users' data and behavior on the Internet anonymous. This paper describes the aforementioned laws, how Tor and the Dark Web work, and examines how attitudes towards privacy impact knowledge and attitudes towards the Dark Web and Tor.

Acknowledgements

First, I would like to thank Dr. Bart Garner for advising me on this research project. His advice, knowledge, and guidance made this thesis possible. I would also like to thank Alexis Jaffe for sticking by me and encouraging me along the way, even when I was too down about my results or the insurmountable research ahead of me to listen.

INTRODUCTION

In recent years, news headlines seem like they are ripped straight from science fiction novels. Many believe that George Orwell's predictions in *1984* have come true, that Big Brother is truly watching us all. One can prattle off names of hot button issues involving the government harvesting private citizens' data: Eric Snowden's leaks, the National Security Administration, Tor and the "deep web." Software manufacturers are told by the government to put backdoors into their programs that allow easy access to data. As cliché as it is, every citizen is slowly becoming their own Winston Smith, whether they know it or not. What sounds like the ravings of a tinfoil hat wearing man on a street corner has suddenly become the featured story on the nightly news.

To what end is the government collecting data on its citizens? The argument is that it keeps us safe. With this data, the NSA will be able to stop crimes before they happen or catch terrorists in the act just by the search terms they enter on Google. Maybe they are right. Maybe it is completely possible to justify the (up until recently) secretive databases of previously encrypted data acquired through surveillance systems like PRISM or by implanting malware into phones to collect text messages.

This makes sense to some; the innocent have nothing to hide, and, even though their data is being mined, what real harm is there in the government seeing a few work e-mails or a few quick texts to invite friends out for drinks? Some are willing to sacrifice their personal freedom in order to gain a sense of safety. Yes, there is the old adage about those willing to give up privacy for freedom deserving neither, but this is a different time. We live in an age where enemies of freedom, both from the United States and outside of it, can communicate with incredible ease and carry out acts of cyber terrorism in the blink of an eye. This begs the question: should there be information that the government cannot access through subpoena? Furthermore, do citizens have the innate right to privacy for all of their data? Do citizens truly care about their right to privacy enough to seek out methods to circumvent or escape government surveillance? To answer this question, we must look at the laws in place regarding information privacy, the surveillance technology the government is using to gather data, and theencryption technologies that are used to secure data.

REVIEW OF LITERATURE

The Omnibus Crime Control and Safe Streets Act of 1968

According to the 2013 U.S. census, between 73% to 84% of American homes have a computer in their homes with Internet access (Raine and D'Vera). The United States is a nation of "plugged in" people, with gigabytes upon gigabytes of data being transmitted every day, whether it is through home computers, public computers, work computers, or smartphones. The Internet has changed the way people communicate, both in person and across long distances, but beyond that, it has become a part of almost every facet of an average citizen's life. The normal morning paper and coffee routine has been replaced by checking e-mails and reading news site headlines. Text messages seem to have replaced the need for actual, physical conversation. Purchases are made every day over the Internet, whether they are for consumer or business purposes. Current society is truly the best argument for the Singularity becoming a reality.

It follows that, with such sensitive information floating out in cyberspace, the government may feel the need to protect their own interests and the safety of citizens by regulating communication. Although there are many laws governing communications, *The Omnibus Crime Control and Safe Streets Act of 1968*, specifically Title III regarding wiretaps, laid the basic framework for government power in acquiring citizen's private communications. The act stated that the nothing

contained within the document itself, nor previous laws, would limit the president's power to "protect the nation from actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities" (U.S. Select Committee to Study Government Operations 289). At this point, while the president's power seemed virtually unlimited to tap wires without a warrant, the laws were structured around protecting the United States from foreign attack and only foreign attack. The act simply states that these powers do exist, but does not truly define them in any way.

Before Title III, wiretaps (whether under warrant or not) were a gray area in the eyes of the Fourth Amendment, which protects citizens from unlawful search and seizure of property. Since there is no physical invasion in a wiretap, the definition of "search" in the Fourth Amendment was contested, and in 1928, the United States Supreme Court allowed wiretaps for suspected bootleggers because the Fourth Amendment "did not apply unless the G-men physically invaded the defendant's premises" (Swire 12). By 1968, times had changed, and a further Supreme Court case ruled that any attempt to search, including wiretaps, would have to meet the Fourth Amendment standards before being legal. Title III was an attempt to codify that sentiment into law. The Fourth Amendment requires that searches be reasonable, defined as "balancing the degree of intrusion against the need for it" (Swire 13). While Title III is large in scope, it only allows warrantless wiretaps in situations that involve a foreign power or protecting the government from being completely overthrown. Again, there is no discussion of exactly what

these powers entail, but just a broad statement that they do exist. At the time, small acts of domestic terrorism seemed negligible in the eyes of this law.

The Foreign Intelligence Surveillance Act of 1978

The next large-scale piece of legislation to deal with information privacy was the Foreign Intelligence Surveillance Act of 1978 (FISA). As the name implies, the act focused on foreign intelligence. The FISA helped define exactly what a "foreign power" is, specifically that the definition now included a foreign government not recognized by the United States, "factions of a foreign nation", or "a group engaged in international terrorism or activities in preparation therefor," as per section 1801. The aforementioned foreign powers "certainly included the Communist states arrayed against the United States in the Cold War" and were specifically worded to target satellite nations of the USSR, according to cyberlaw expert Peter Swire (24). The FISA drew distinct lines between United States-persons and non-United States persons, but was not so clear-cut on who could be watched. All agents of a foreign power could be targets of surveillance and the criteria was as simple as being an employee of a non-United States nation. United States citizens could only be declared an agent of a foreign power if they were "knowingly engaged in a listed activity, such as clandestine intelligence activities for a foreign power" (Swire 25). This definition fed off of Cold War panic and allowed KGB agents (or suspected agents) acting domestically to be spied on even if they were technically living in the United States.

One large change from Title III to FISA was that, under Title III, targets of surveillance would be notified after they had been spied on that information had been taken. The FISA, however, was "cloaked in secrecy," only notifying the target when the evidence was used in court against them but not even guaranteeing them the right to see what that evidence was (Swire 28). The FISA allowed the President, through the Attorney General, to authorize electronic surveillance without a court order for up to a year on communications used by the foreign powers. The FISA also created a Foreign Intelligence Surveillance Court to grant orders for surveillance on foreign powers, effectively creating a checks and balances system. In addition, the Attorney General was required to report to the House and Senate Intelligence Comities every six months and yearly to the general public about the total number of applications for wiretaps and the number that were actually approved.

However, wiretaps could still be granted on United States citizens through a court order, pursuant to section 1805, which requires that the court find "probable cause" that the surveyed individual or individuals are a foreign power or an agent of a foreign power. Furthermore, they must also adhere to "minimization procedures," which, according to Section 1801(h)(1) are designed to reduce dissemination, acquisition, and retention of material collected from United States citizens.

While the FISA did regulate wiretaps with bureaucratic pressure, it also dismissed the Fourth Amendment right to be notified of any seizure of property in the case of a wiretap. It also legitimized secret wiretaps, even going so far as to provide a path to legally approve them. The laws, while seemingly open ended, still

required that investigations' primary purpose be gaining intelligence on foreign powers.

The USA PATRIOT Act

After the tragic terrorist attack that took place on September 11th, 2001, the next large privacy legislation, the USA PATRIOT Act (PATRIOT Act) was set into law. The Act was designed to both provide preventative measures against future terrorism attacks and bring information privacy laws up to date with the increasing amount of Internet access and telecommunication in the United States. The PATRIOT Act, specifically Titles II, VII, and IX, dealt with how information could be collected and the reasons why it could be collected. As stated above, the FISA required orders for wiretaps to certify that "the purpose of the surveillance is to obtain foreign intelligence information" (Swire 39). The PATRIOT Act changed this to just a "significant" purpose, meaning that the surveillance did not have to explicitly look into foreign communication. The change, while small, highlighted the paradigm shift after the events of September 11th. "Terrorism," as a whole, was more broadly looked at when determining threats to American life, not just large-scale foreign espionage. While Title 18 of US Code already defined domestic and international terrorism, the PATRIOT Act broadened these terms, adding assassination, mass destruction, and kidnapping to both forms. Some politicians, such as congresswoman Tammy Baldwin, have expressed outrage over the expansion of the definition of terrorism, deeming the definition too expansive and

implying that it could make American citizens who display their dissent in a peaceful manner out to be terrorists (Moore, *Fahrenheit 9/11*).

Particularly important to information privacy is section 814, which redefined terms dealing with cyberterrorism, creating laws that could label those that commit computer crimes as terrorists. According to Ellen Podgor of the American Bar's *Criminal Justice Magazine*, computer damage can only be claimed as a terroristic act if the action "be knowingly committed and the damage intentional."

Title II is where these definitions start to take effect. Entitled "Enhanced surveillance procedures," the section greatly enhances the power to intercept communications (oral, wire, and electronic) relating to terrorism and computer fraud. While other acts attempted to limit the scope of whom the surveillance could target, the PATRIOT Act, born from post-9/11 fear, broadened the spectrum of terrorism and thus widened the scope of how much and what kind of information could be intercepted. One large, sweeping motion is found in Section 215, which changes FISA laws from focusing just on electronic communications to any "tangible" form of intelligence, including records, documents, and papers. According to Swire, this allowed FISA orders to supersede previous laws and target information that is "generally subject to privacy protections" (40). In addition, the FISA was amended so that the orders only have to prove that the information is pertinent to an authorized investigation, not that the target is a foreign power or an agent of a foreign power.

While the explicit purpose of the PATRIOT Act seems to be combating terrorism, this change allows anyone to be subject to a FISA order as long as it can

be reasonably argued that the information gathered is relevant to an investigation. There are virtually no limits to the type or amount of data gathered. Section 206 goes even further by providing a legal path for "roving" wiretaps. Previously, FISA acts were tied to a specific telephone, but, to adapt to changing times and new technology like cell phones, the PATRIOT Act allowed wiretap requests to be tied to an individual person instead.

Section 212, titled "Emergency disclosure of communications to protect life and limb," details when a communications provider can disclose information about a customer's communications. Previously, providers could never do this, but now if they "reasonably" believe that death or injury is imminent, they can do so to an investigative agency. In addition, when a government agency has a court order for this information, they must disclose it. This, in tandem with section 213, which allows the notification of search warrants to be delayed, presents a government with access to both consumer and personal information without having to tell targets when they are being searched.

While the FISA orders may have been gathered in secret, the FISA included a clause that allowed some of the targets to be notified that they were being spied upon. The PATRIOT Act gets around this with Section 215, one clause of which states "no person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things." When taking the law literally at its word, the FBI can target anyone for surveillance, for virtually any reason, and obtain any amount of any information they want.

Strangely enough, in a scene from director Michael Moore's controversial documentary *Fahrenheit 9/11*, a news clip from small town America has citizens extolling the virtues of the PATRIOT Act, calling it "a good thing" and something "that needed to be done." In a fit of Cold War-esque paranoia, working class American citizens from all over the country had started to become suspicious of terrorist activity. The definition had expanded so much that anything could become a target for terrorists and anyone could be a terrorist. One man lived out a textbook Orwellian experience after being turned into the FBI by his friends because he spoke out against the War on Terror.

One major safety provision of the PATRIOT Act is that is still allows the protections offered by the First Amendment (freedom of the press, speech, assembly, religion, etc.) to remain untouched. Section 214, "Pen register and trap and trace authority," expressly forbids investigations from violating the first amendment. However, it also lays out guidelines for electronic surveillance on anyone suspected of terroristic activities. According to congressman John Conyers, "there had to be a surrendering of certain […] rights" in order for citizens to feel safe from terrorism (Moore, *Fahrenheit 9/11*).

Homeland Security Act

A little over a year after the PATRIOT Act was passed, Congress felt that some of the new powers given to the government were a bit too broad in scope. Thus, the following year, the Homeland Security Act of 2002 (HSA) was passed. According to

President George W. Bush, the purpose of the HSA was to "defend the United States and protect citizens from the dangers of a new era" (Kirkpatrick and Lockhart LLP 1). The HSA is most known for creating the Department of Homeland Security, but Title II of the Act, "Information Analysis and Infrastructure Protection," deals directly with cyberterrorism and information security. This title is divided into four subtitles: Subtitle A – Directorate for Information Analysis and Infrastructure Protection; Access to Information, Subtitle B – Critical Infrastructure Information, Subtitle C – Information Security, and Subtitle D - Office of Science and Technology.

Subtitle A created an Under Secretary for Information Analysis and Infrastructure Protection who is responsible for analyzing law enforcement and intelligence information to detect potential acts of terrorism against the United States. The Under Secretary must also develop a plan for "securing the key resources and critical infrastructure of the United States," which, as defined in this law, includes information technology and satellite systems, effectively giving the Under Secretary power over these areas. The Under Secretary can also develop policies and procedures designed to protect these areas of interest, using data-mining and "advanced analytical tools" to carry out these measures. According to the Homeland Security practice group of Kirkpatrick & Lockhart LLP, the Secretary of the Department of Homeland Security is "broadly authorized" to gain information from the private sector relating to terrorism or suspected terrorist activities (2). The information is broken down into three broad categories: any assessment or analytical data regarding threats of terrorism to the United States, any information

relating the infrastructure of the United States to terrorism, or any unprocessed data on other subjects that relate to the duties of the Secretary.

Subtitle B is aimed at encouraging, but not requiring, the private sector and state and local governments to share information with the Department of Homeland Security. Section 213(3) defines critical infrastructure information as "information not customarily in the public domain and related to the security of critical infrastructures or protected systems." This explicitly includes any actual, threatened, or potential computer attack or misuse of electronic communications systems. However, any information voluntarily submitted through this act is not subject to any type of disclosure, even if it would fall under the Freedom of Information Act. As long as the information was knowingly, voluntarily submitted and the submitter knew ahead of time that the information would not be disclosed, no disclosure is required. However, without written consent from the submitter, the information cannot be used directly in any civil action. The information can still be used to start an investigation or used to build evidence against a suspected terrorist.

Subtitle C provides some limitations for the information collected by Title II of the HSA. Section 221 ensures the confidentiality and security of the information, as well as limits unauthorized redistribution of information. Furthermore, it attempts to protect "constitutional and statutory rights" of targeted individuals. Section 225 creates another sub-act of sorts within the HSA, entitled "Cyber Security Enhancement Act of 2002." While a sizable portion of this act deals with stricter penalties for those convicted of cyber crimes, one of the more interesting details is the striking of Section 212 of the PATRIOT Act, broadening it's detailed powers and

allowing easier access to information. This section changed the wording from "reasonable belief" to "good faith belief" that injury or death may occur, lowering the bar for gaining information on telecommunication providers' customers. In addition, the word "immediate" was dropped and any mention of an expiration date was stricken, making this permanent.

Even though the Department of Homeland Security was established in this act, the need for a specific governing body for new laws regarding computer crimes still remained. Subtitle D established an Office of Science and Technology within the Department of Justice, tasked with developing new law enforcement technology. This included both physical weaponry and "monitoring systems […] capable of providing precise location information" and tools to aid prevention of computer crime.

Considering the great power afforded by the PATRIOT Act and the HSA, it seems that it could be easy for a government agency to misuse this power and manipulate the law. The Electronic Frontier Foundation actually cites two incidents of this happening: one where a Department of Justice attorney used the pretense of a terrorism threat in order to investigate a bank robbery and another where information used to prevent a "bio-terrorism" threat was used in a drug sting ("Let the Sun Set on PATRIOT: Section 212 and Homeland Security Act Section 225: 'Emergency Disclosure of Electronic Communications to Protect Life and Limb"). Critics of these laws feel that American liberties are being stripped away in order for citizens to feel freer. At what cost are Americans gaining a perceived sense of

security? This is a question critics have grappled with for years as these powers have expanded with each passing act or law.

As shown in this thesis, the scope of both who can be targeted for unwarranted surveillance and how much information can be gleaned from that surveillance have increased greatly. Each of the major laws or acts affected information privacy are a product of their time, from the FISA's concerns about American citizens working as agents of Soviet forces to the PATRIOT Act's obsession with broadening the definition of terrorism to a near all-encompassing point. As such, the laws are reactionary responses to the perceived threats against the structure of United States way of life. They are not so much preventative measures to determine who will become a threat and combat it ahead of time, as they are ways of increasing government power by using fear as a catalyst. This begs the question: how far is too far? Where is the line between the citizens' right private information and the government's need to have it?

Tor and the Dark Web

Some feel that there should be information on the Internet that cannot be peered into through normal means. Those wanting to escape from the all-seeing eyes of big brother have created Internet sites based around keeping their information anonymous. These sites, collectively known as the Dark Web, are defined by BrightPlanet (a website that collects content and resources about the Dark Web) as a portion of websites "that have been intentionally hidden and [are]

inaccessible through standard web browsers." They make up a small portion of the Deep Web, which is further defined as "anything a search engine can't find" ("Clearing Up Confusion – Deep Web Vs. Dark Web"). While the Deep Web includes "normal" websites used every day, such as business' intranets, Dark Web websites are typically only accessible by using a specialized browser called Tor, and these sites utilize the extension .onion instead of the ordinary .com or .net. These websites, accordingly, live in the Tor network.

As expected, a fully functional "second internet" based in anonymity has its illicit uses. The most famous Dark Web website, Silk Road, was a marketplace where consumers could use Bitcoin (an Internet currency also rooted in anonymity) to purchase illegal drugs, fake passports, and "illegal services" such as computer hackers, according to USA Today (Leger). This is the "face" of the Dark Web to the American public: it is scary, illegal, and national newspapers and magazines can use it to explain why having an anonymous Internet is a bad idea. When spun like this, it seems like the government wants to have personal information solely to stop legitimate crime from happening. However, Tor and the Dark Web can be used for far less insidious purposes.

Tor's official website defines the network as "a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet" ("Tor: Overview"). Tor's use of outside servers means that a user does not have to make a direct connection to the website; their connection is routed through a series of hidden virtual passages, guarding their identity. Tor can be used to circumvent censorship firewalls or to communicate about sensitive information (such as abuse

and rape) without giving any sort of personal information about the user's whereabouts or computer. Moreover, Tor can also be used to connect to and create Dark Web sites, which do not give out any location info about the website. Since Tor is not a public network, it is not susceptible to "traffic analysis," which is the capability to see who is talking to who on a public network ("Tor: Overview").

When data is sent over the Internet, it contains two parts: a data payload and a header. The payload contains, to put it succinctly, the "information" of the packet, such as the text of an e-mail or the content of a video. The header contains routing information and this is the part targeted in traffic analysis. In layman's terms, as long as someone can sit between the sender and receiver of the information, they can look at the header and see where the information is coming from and where it is going. Tor routes the sent communication to different points on the Internet, similar to action movie villains that bounce illegal funds from hidden bank account to hidden bank account. In order to achieve this and maintain a speed that most users would deem usable, Tor must have a large number of nodes. According to Roger Dingledine, Nick Mathewson, and Paul Syverson of The Free Haven Project, this was actually a goal in the design choices of Tor. To achieve this capacity, Tor must be usable, flexible, and simple. The authors argue that a complex system will have too few users, and because "anonymity systems hide users among users, a system with fewer users provides less anonymity" (Dingledine, Mathewson, and Syverson). At a certain point, due to the mass of users that Tor is able to use to hide information, the information's origin becomes nearly impossible to discern. The Tor network creates a private pathway by "incrementally [building] a circuit of encrypted connections

through relays on the network" with only the current relay point knowing where the information directly came from (one step back) and where the information is going (one step forward) ("Tor: Overview"). The client computer has a different set of encryption keys than the node computers do, so no node ever has the complete picture. The circuits are refreshed over time, making them even harder to pin down.

The Tor network encrypts the data sent using Transport Layer Security (TLS) encryption ("Tor FAQ"). According to T. Dierks and E. Rescorla of the Internet Engineering Task Force, the TLS protocol allows clients to communicate with servers "in a way that is designed to prevent eavesdropping, tampering, or message forgery." The protocol consists of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides two basic functions: it guarantees that the connection is private and that the connection is reliable. Symmetric cryptography is used to guarantee privacy; the keys are generated separately for each connection based on a separate protocol and each set of keys is unique. The TLS Handshake protocol acts before "the application protocol transmits or receives its first byte of data" and allows the client and server to negotiate an encryption algorithm (Dierks and Rescorla 4). The Handshake Protocol provides a secure and reliable connection for negotiating the secret encryption. In addition, it also allows each party to identify each other using asymmetric (public key) cryptography in order to authenticate that the information is being sent to the correct place.

Each node in the Tor system has it's own onion key, which is a public decryption key used to authenticate it's status as a true Tor relay point ("Tor FAQ").

As the Tor client determines its data path, it stops at each relay point and uses the key to prove the authenticity of the node. Each relay also has its own distinct identity key, which is checked against the directory authority's directory signing key, essentially a master list of all known Tor relays. Furthermore, Tor sends data in packets of 512 bytes each, no matter the actual size of the data being transmitted, making it hard to determine exactly how much data is actually being sent.

At first glance, Tor seems like every black market cliché come to life. What criminal would not want a virtually untraceable, anonymous way to sell their wares and communicate about illicit activities? However, Tor and the Dark Web present a new way for average American citizens to communicate about sensitive subjects without revealing their IP address to prying eyes. According to the Tor Project's website, the Friends Service Committee and other environmental groups are becoming more and more aware of government surveillance of their activities ("Tor Users"). Their activities, while peaceful, can easily be construed as terrorism under the PATRIOT Act; thus Tor provides a way to circumnavigate the risk of their personal information becoming exposed. Furthermore, government whistleblowers, whose rights are being stripped away more and more as their information disseminates further to American citizens, can use Tor to report their findings without exposing their location. Journalists, law enforcement, bloggers, and business executives (among others) are all groups that use Tor for legal purposes ("Tor Users").

The Tor Project's FAQ on abuse states that only a "handful" of complaints have been lodged against the service since its creation in 2003 ("Abuse FAQ").

Currently, Tor is not illegal in any part of the world, and the Tor Project claims that the service's good parts outweigh its bad ones ("Tor FAQ"). Tor has no backdoor in their software, which would allow government agencies to peek into the flow of data despite its supposed anonymity. The Tor Project says that putting in a backdoor would be "tremendously irresponsible to [their] users, and set a bad precedent for security software in general" ("Tor FAQ"). Because of the way data packets sent through Tor skip around from computer to computer, Internet service providers (ISPs) cannot collect any sort of information on their customers that use Tor and thus they cannot supply any information in the event of a subpoena. All an ISP can see is that the user is interacting with Tor servers.

As stated before, Tor browsers can access special sites with the top-level domain name .onion, colloquially referred to as "onions." These sites are part of the Dark Web, and thus the Tor directory server must provide the look-up service to get to these websites ("Tor FAQ"). These websites function differently from normal website in that there is no IP address associated with them due to how Tor works. To access the site, the user must manually enter in the long, complex strings of letters and numbers, followed by ".onion." While many of these onions are used for illegal purposes (such as the aforementioned Silk Road), others are used for less insidious purposes, such as hosting a backup of government-transparency website Wikileaks. The interesting part about onions is not the content that they contain, but their mere existence and the questions they pose. Onions allow information to be stored on the Internet but not stored in any one location. While the sites can be shut down (again, as was the case with Silk Road) the information is not subject to the

same rules that the rest of the Internet must follow. Onions are a way to build websites, and therefore an Internet, in a way that circumvents government traffic monitoring.

RESEARCH METHODS AND PROCEDURES

Method

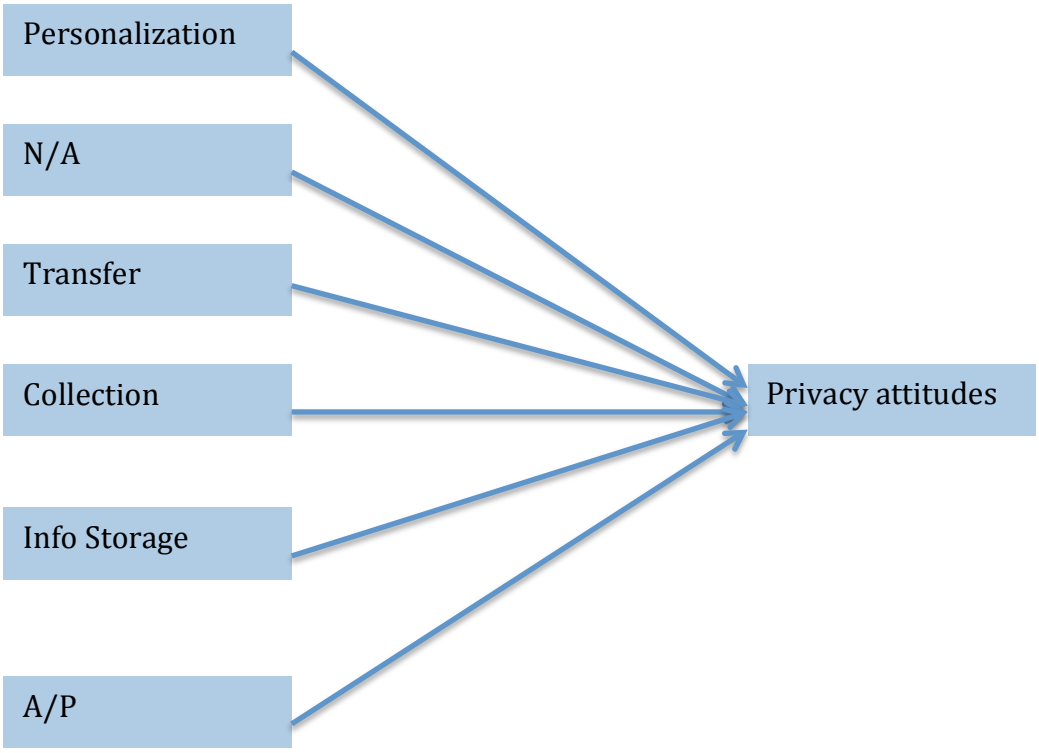
The overall objective of this study is to determine if levels of Dark Web awareness rise when levels of government surveillance awareness rise. I am hypothesizing that they do, so as a person's awareness of government surveillance rises, the more likely they are to have some sort of knowledge about the Dark Web. It stands to reason that a person aware of government surveillance would want to take steps to protect their information and identity online, and thus would seek out tools to do so. Government surveillance has become such an ingrained part of life that citizens are constantly reminded of. Citizens may want to fight back and do something to protect their anonymity. While Tor may not be the easiest tool to seek out, it is one of the more effective ones. This study takes the form of a questionnaire, given to management information systems students at the University of Mississippi. They were given the option to take the survey in class.

Instrument

The study itself is in two parts. The first part is based on a survey created by Dr. Annie I. Anton and Dr. Julia B. Earp in their paper "Examining Internet Privacy Values within the Context of User Privacy Values." The survey measures attitudes towards various issues in information privacy which are broken down into six factors: personalization (the use of cookies and personally identifying information (PII) to customize advertisements or other facets of users' online experience),

notice/awareness (websites making users aware of their PII being used in different ways), transfer (users' PII being transferred to a third party), collection (different sorts of information, such as browser configuration or information about browsing habits being gathered), information storage (unauthorized personnel, including hackers, gaining access to a user's information), and access/participation (users being involved in the process of their PII being collected). This instrument is modeled in Figure 1. Anton and Earp's six independent variables, the six factors,

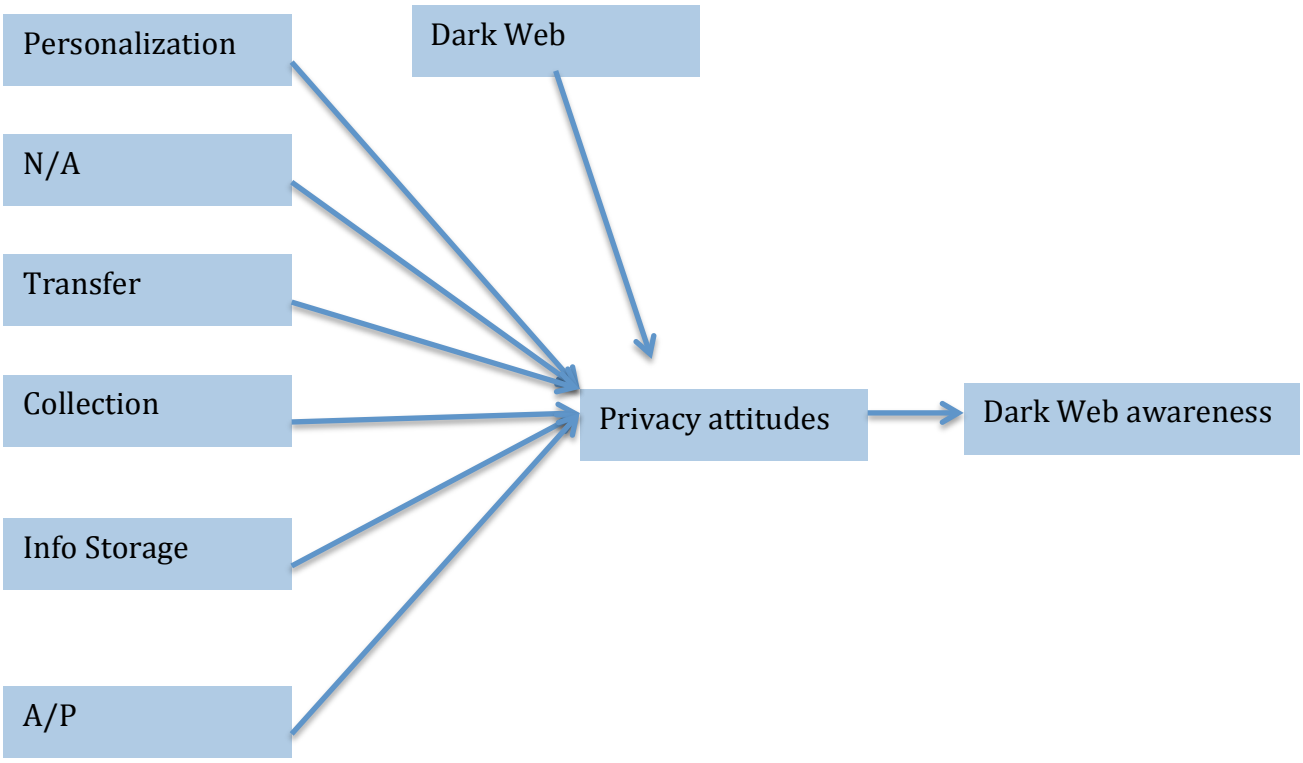
Figure 1: Anton and Earp's Instrument



directly impact the dependent variable, attitudes towards information privacy.

I have added a seventh factor into the study, Dark Web. As the name implies, this section measures Dark Web awareness and the participant's intent to use the Dark Web in the future. This is modeled in Figure 2. The six independent variables are joined by another variable, Dark Web. All seven of these independent variables affect the original dependent variable, privacy attitudes, which in turn impacts a new dependent variable, Dark Web awareness. Each of these factors is further broken down into multiple questions, which are rated by the participant on a scale of how much the participant agrees with each statement, from "strongly agree" to "strongly disagree." While many

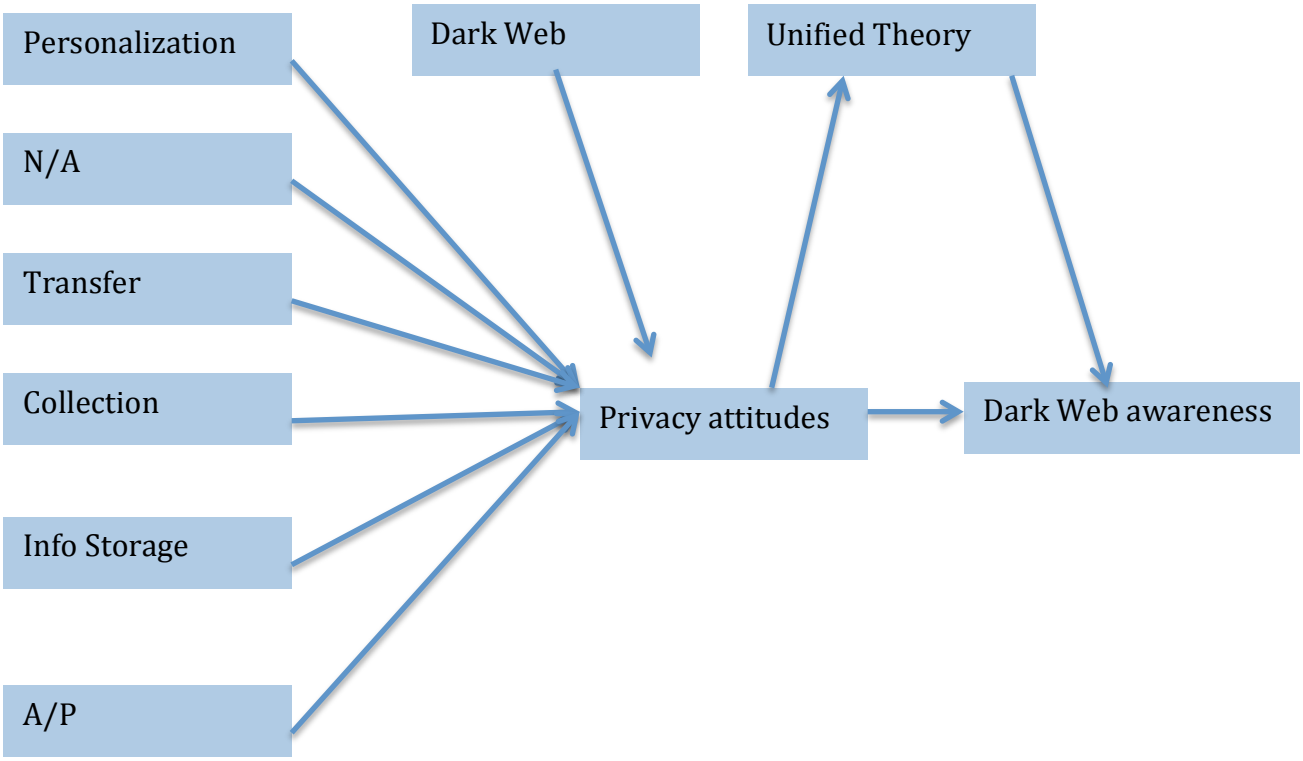
Figure 2: Anton and Earp's Instrument With the Dark Web Variable



of the questions in Anton and Earp's survey are focused on examining the use of PII by marketers, it will be interesting to see how attitudes towards a perceived "good" use (customization of web experience) will differ from a perceived "bad" use (government surveillance), even though both involve the use of similar information. The advantage of using this scale over others is that participants find the different factors relatable (Preibusch 1141). This means that the participants will have more knowledge and understanding of the factors and will hopefully lead to more accurate answers. This is the main reason why Anton and Earp's instrument's was chosen as opposed to others; the current study is founded on that breaking the complex privacy issues brought upon by government act after government act into smaller, more relatable pieces will result in the respondents truly examining their own values and attitudes towards information privacy and thereby yielding more accurate data for analysis in this study.

Anton and Earp created this instrument by splitting different websites' privacy policies into smaller phrases to analyze trends (Earp, Anton, Aiman-Smith, and Stufflebeam 229). These statements were then placed into one of twelve categories dealing with information privacy. The categories were consolidated into the six aforementioned factors, designed specifically to "tap into the user's value in terms of privacy policies" (Earp, Anton, Aiman-Smith, and Stufflebeam 231). In a follow up paper, "How Internet Users' Privacy Concerns Have Changed Since 2002," Anton and Earp noted that Internet users seemed primarily concerned with information transfer, notice/awareness, and information storage, which are also of primary concern in the current study (Anton, Earp, and Young 1).

Figure 3: Instrument with Optional Unified Theory Section



The second section of the survey is taken from the Unified Theory of Acceptance and Usage of Technology, developed by Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis for the article "User Acceptance of Information Technology: Toward a Unified View." This specifically measures the participants' perceived usefulness and intent to use the Dark Web. This section of the survey is only accessible to those who indicate that they have previously used Tor to access the Dark Web. The second section acts as a moderator to the Dark Web awareness variable, providing more insight into users' perceived value of the Dark Web and Tor, as shown in Figure 3. These results, combined with the results

from the first part of the survey, should provide a better idea of how information security awareness impacts Dark Web usage and awareness.

Figure 4: Data Model Summary

Factor 1: Personalization	Personalization deals with how much users would like their PII to be used customize their web experience.
Factor 2: Notice/Awareness	Notice and awareness deal with how much users would like to be notified that their PII is being used.
Factor 3: Transfer	Transfer deals with a user interest in who their PII is transferred to after a website collects it.
Factor 4: Collection	Collection deals with the kinds of information that are collected from a user and the value they place on each type.
Factor 5: Information Storage	Information storage deals with the user's interest in unauthorized personnel gaining access to their data.
Factor 6: Access/Participation	Access and participation deal with the user being involved in the process of their PII being collected.
Factor 7: Dark Web	Dark Web deals with the participant's knowledge of the Dark Web.
Unified Theory of Acceptance and Usage of Technology	When the participant responds that they have used Tor to access the Dark Web, they are taken to this section to measure their attitudes and opinions about the Dark Web.

DATA ANALYSIS AND RESEARCH RESULTS

Anton and Earp's Seven Factors

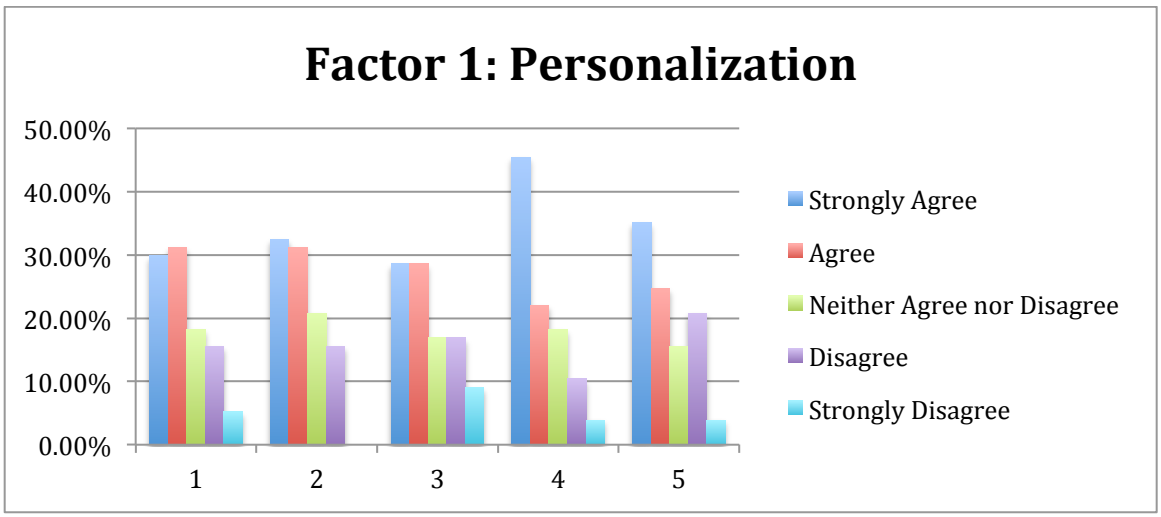


Figure 1.1

Figure 1.1 shows the results of the first factor of the survey, personalization. The users were presented a series of statements regarding the use of their personally identifying information (PII) to customize what they see online. Across the board, most respondents showed some level of concern over their information and purchasing habits being used to customize their web experience. The first statement read that they minded their PII being used to customize their browsing experience, to which 29.87% strongly agreed. The second statement dealt with cookies, to which 32.47% of respondents strongly agreed that they minded cookies on their computer. The third statement dealt with purchasing history, and 28.57% strongly agreed that they minded their purchasing history being used to customize

their web experience. The main cause of concern was statement four, which said that they minded their PII being used for marketing and research activities. 45.45% responded that they strongly agreed. Finally, the fifth statement said that the respondents minded a web site monitoring their purchasing activities, to which 35.06% strongly agreed. While customization of web experience could be considered a positive outcome of PII or purchasing history collection, it is evident that most respondents are still wary of it, with few disagreeing with the statements (and in the case of question two, no one strongly disagreeing).

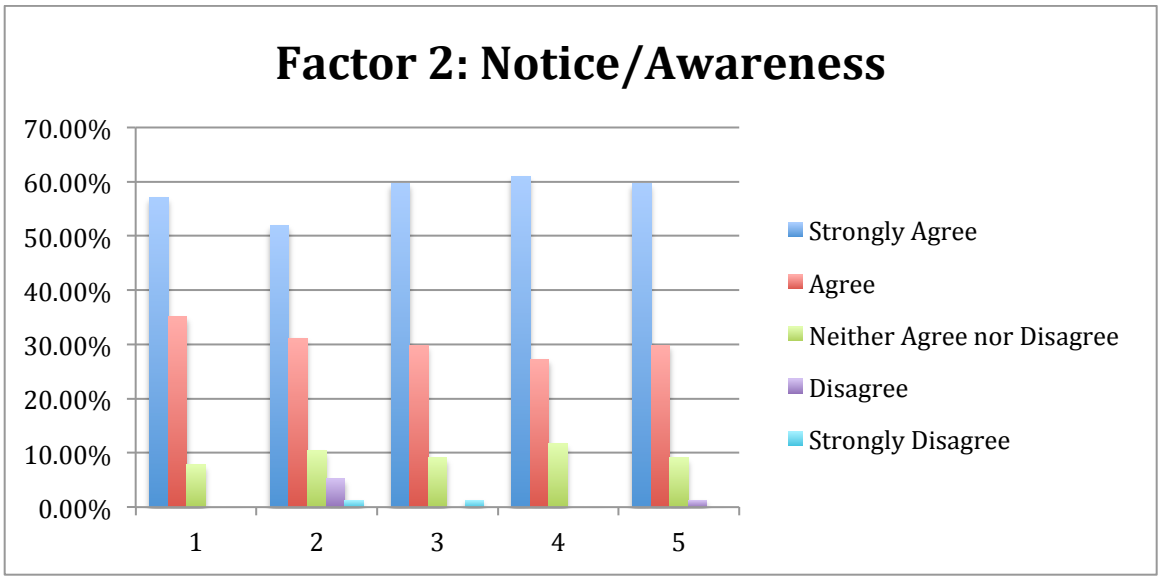


Figure 1.2

Figure 1.2 shows the results of the second factor in the survey, notice/awareness. In this factor, respondents were presented with statements about being notified that their PII is being used or that it is being collected. Notably, two of the statements had no one strongly disagree with them, and statement four had no disagreement at all. The first statement, which 57.14% strongly agreed with, stated that the respondents wanted the option to decide how their PII is used. The

second statement stated that they wanted a website to disclose security safeguards in place to protect their PII, which 51.95% strongly agreed with. The third statement dealt with websites disclosing how their PII would be use, which 59.74% strongly agreed with. The fourth statement, which had the highest strongly agree percentage at 61.04%, stated that they wanted a website to tell them when the website would use their PII in a way not previously disclosed. Finally, the fifth statement said that the respondents wanted to be informed of changes to a website's privacy practices, which 59.74% strongly agreed with. Again, as with factor 1, most of the responses to this section were positive, almost overwhelmingly so.

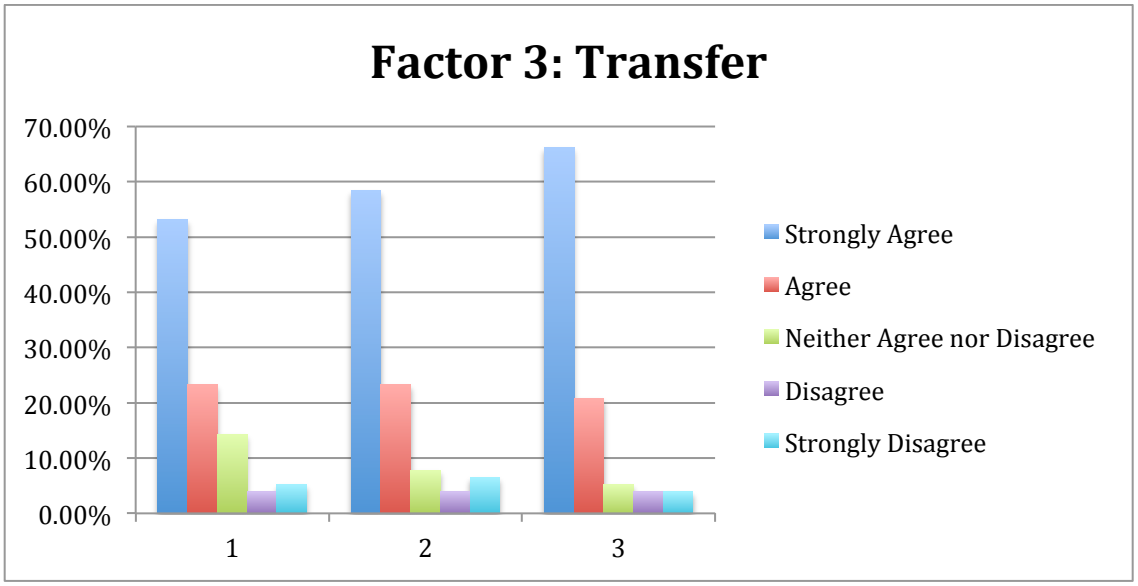
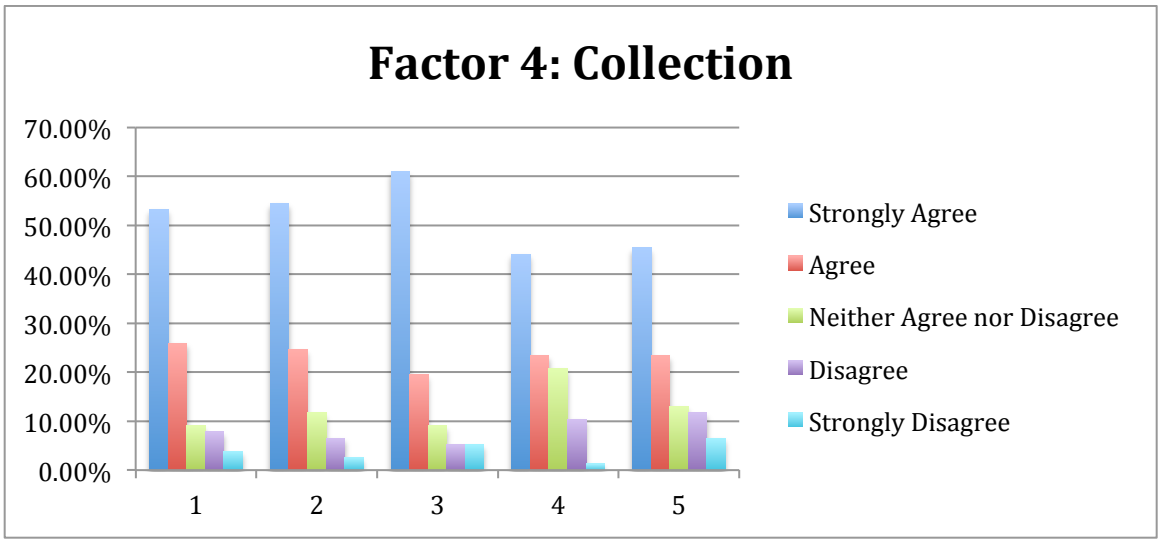


Figure 1.3

Figure 1.3 shows the results of the answers from the third factor, transfer. These statements were about the respondents' PII and purchasing habits being transferred from the website that collected them to a third party. The first statement said the participants minded when their purchasing habits were transferred to a third party, which gathered a 53.25% strongly agree response rate. The second

statement, which dealt with their "information" in a general sense being shared with third parties, had 58.44% strongly agree. Finally, the third statement said that the respondents minded when their PII was bought by or traded to third parties, which got the highest strongly agree response of this factor at 66.23%. Again, the responses trended mostly positive, with only a small portion disagreeing with the statements each time. Interestingly enough, a smaller number of respondents strongly agreed with the marketing and research questions in Factor 1 than they did for the first question in this section. This could be attributed to the first section dealing with web experience customization, a potentially positive outcome of PII sharing, while this section only deals with it in vague terms of sharing.



Factor 1.4

Factor 1.4 contains the results of the responses to the fourth factor, collection. In this portion, respondents were provided a series of statements about the kind of information a website may collect from a user. The first statement said that the participants mind when a website gathers (without their permission)

information about their browsing patterns. This garnered a 53.25% strongly agree response rate. The second statement, which dealt with a website gathering information about the user's browser configuration, gathered a 54.55% strongly agree response. The third statement said the users minded when a website collected their IP address without their permission, which 61.04% strongly agreed with. The strongly agree responses finally dip in the fourth statement, with only 44.16% strongly agreeing with minding a website collecting information about the computer or operating system they are using. The fifth and final statement said the respondents minded a web site recording the previous websites that they had been to, and only 45.45% of participants strongly agreed with it.

The strongly agree numbers tended to trend down in this section, as more responders began to feel neutral about the statements. Statement four's neutrality rate was 20.78%. This may be because websites routinely need information about operating system or browser configuration to display content completely and accurately (for example, a website showing a different program download to OSX users than Windows users). Interestingly, less users tended to agree with the statement from factor 1 dealing with cookies, another accepted part of internet browsing and website functionality.

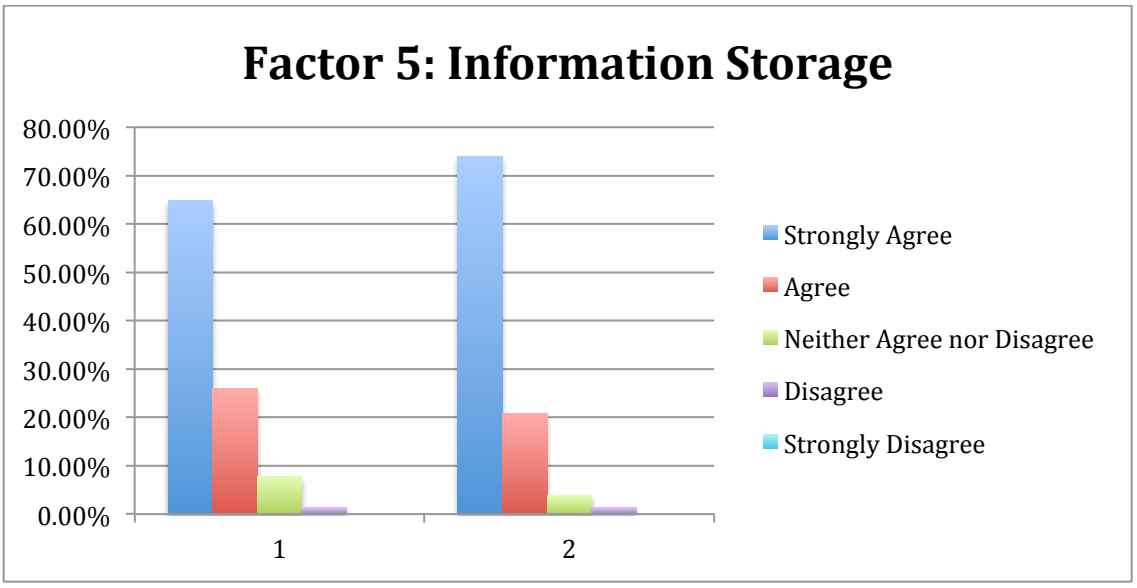
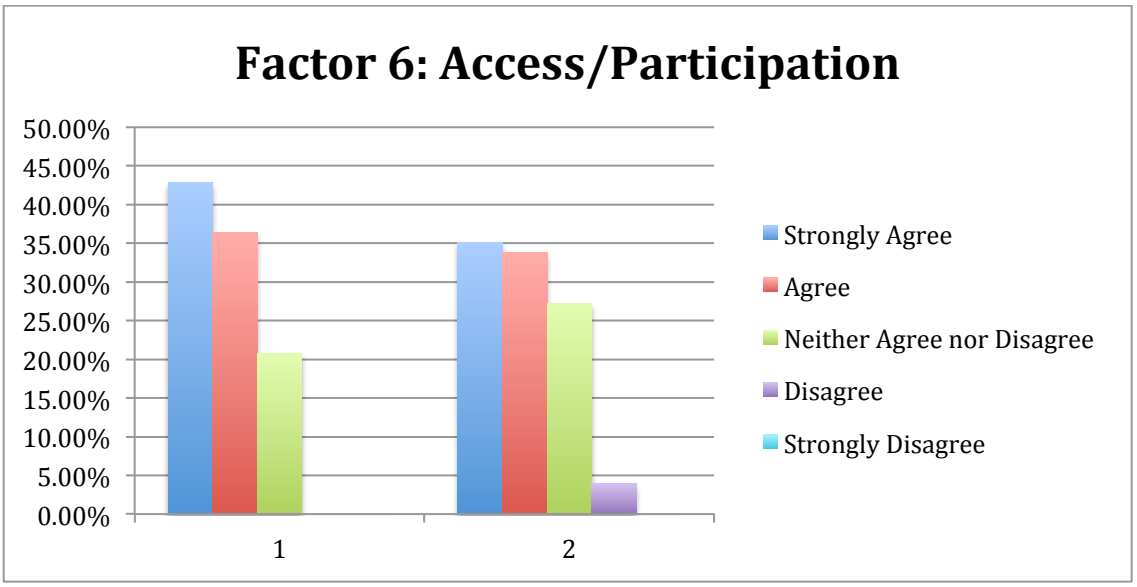


Figure 1.5

Figure 1.5 shows the results of the fifth factor, information storage. This factor contained two statements about who is actually accessing the data stored by websites. The first statement said that the participant was concerned with unauthorized employees gaining access to their information, which 64.94% strongly agreed with. The second statement said that the respondents were concerned with unauthorized hackers doing the same, and 74.03% strongly agreed with that. Almost no one responded negatively to either statement. These are very easy statements to agree with, as both are genuine concerns over data privacy and safety.



Factor 1.6

Factor 1.6 contains the results of the answers to the third factor of the survey, access/participation. The two statements in this factor dealt with what a user could do with their PII after a website has captured it. The first statement said that the users wanted to be able to check their PII for accuracy, which 42.86% agreed with. The second and final statement said that the participants wanted to be able to modify their PII, which gathered a 35.06% strongly agree rate.

This section had the smallest gap between strongly agree and agree of any of the original six factors. It is also the only factor to deal with how a user interacts with their data after it is collected, which may explain some of the apathy and the high neutrality rate. Still, barely any participants disagreed with wanting to be able to change their PII.

Factor 7: Dark Web

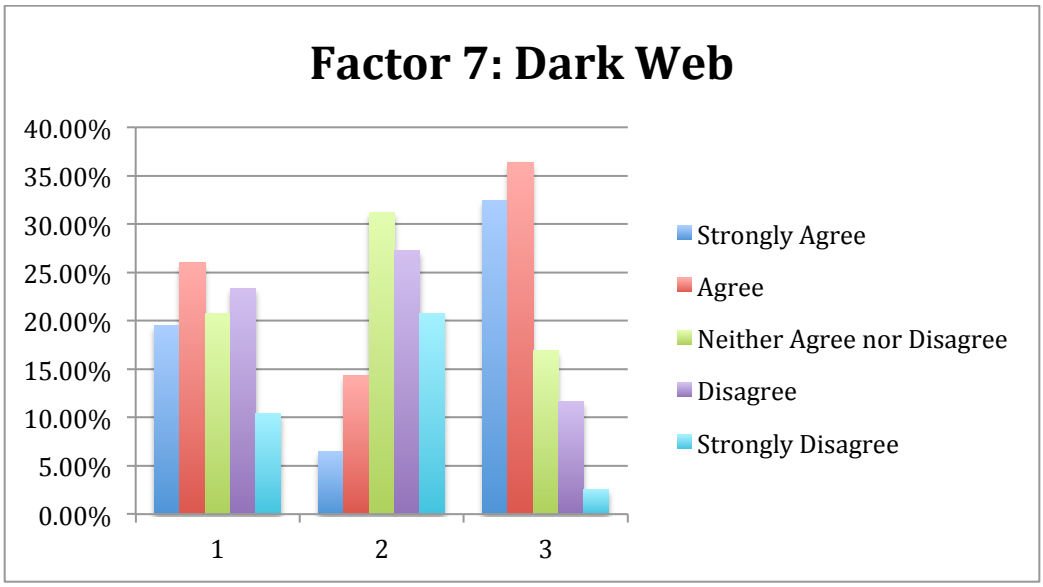


Figure 1.7

Figure 1.7 contains information about the seventh factor, dark web. This is one of my own design that I added to the end of the original instrument. Its purpose is to test knowledge of the dark web, and the responses varied greatly from the rest of the survey. The first statement succinctly said that the participant was knowledgeable about the dark web and its uses. Interestingly, 25.97% agreed with the statement followed by 23.38% disagreeing. The second statement said that the participant has accessed the Dark Web through the Tor browser at some point in the past or will in the future. 31.17% neither agreed nor disagreed with the statement, while 27.27% disagreed and 20.78% strongly disagreed. The final statement in the survey and this factor is an inverse of the first statement in this factor. It states that the participant has limited knowledge of the deep web. Strangely, 36.36% actually

agreed with this statement versus the 23.38% that disagreed with being knowledgeable.

Unified Theory of Acceptance and Technology

The results from the Unified Theory of Acceptance and Usage of Technology (included in Appendix #1) sheds some light how the respondents that answered that they had used Tor for browsing the Dark Web. While negative response rates for every statement were low, of note is statement 9, "using the system is a bad idea." 54.55% neither agreed nor disagreed with the statement, meaning that, overall, most respondents that had used Tor to access the Dark Web did not assign a moral value to it. The same amount neither agreed nor disagreed with the statement that Tor was fun. The statement "I am apprehensive about using the system" actually garnered the most respondents strongly disagreeing, with 18.18%, but a high number also agreed, with 45.45% responding that they agreed in some capacity. Even Tor users (frequent and infrequent) view Tor and the Dark Web as something that might not be the best idea. There could be many reasons for this, from media stereotyping to the users potentially seeing something illicit while using the Dark Web.

Analysis

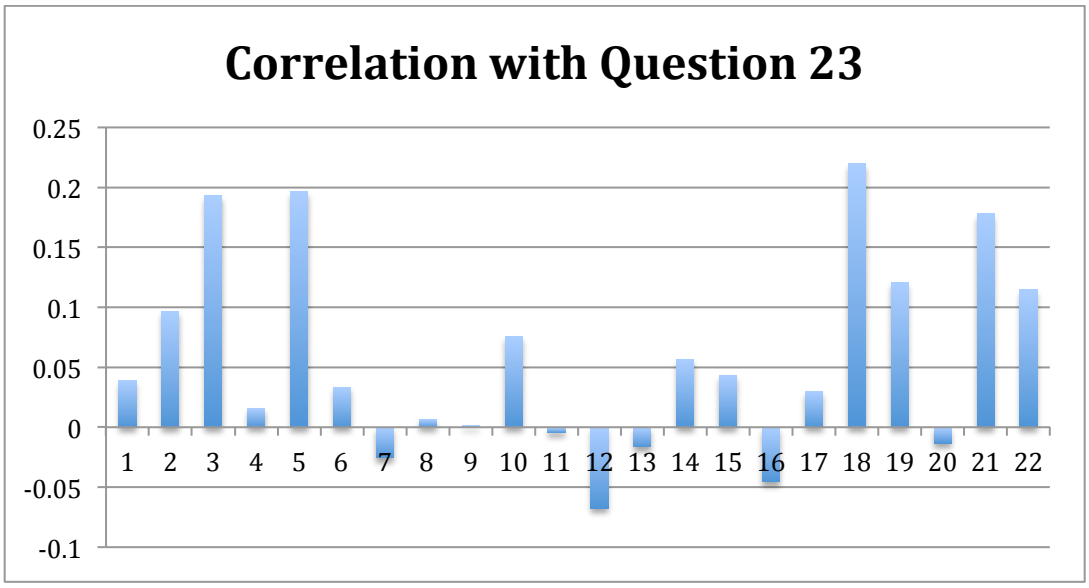


Figure 2.1

Overall, 45.45% either agreed or strongly agreed that they had knowledge of the Dark Web and its uses but only 20.78% agreed that they had used it or would use it in the future. The objective of this study was to determine if an increase in privacy concern would lead to an increase in attitudes regarding the Dark Web. One way to determine this is correlation, which examines how two variables move in tandem. A score of 1 is perfect positive correlation, meaning that as one variable increases the other variable always increases with it. Likewise, a score of -1 is perfect negative correlation, meaning that as one variable increases, the other

always decreases. In this case, the independent variable is any one of the questions about privacy (taken separately) and the dependent variable is Dark Web knowledge.

Figure 2.1 contains the correlation results for statement 23, "I am knowledgeable about the Dark Web and its uses." The highest variable positively correlated with this statement is statement 18, "I mind when a website records the previous website I visited" with 0.22 correlation. Other highly positively correlated variables include statement 3, "I mind when a website uses cookies to customize my browsing experience" (0.19) and statement 5, "I mind when a website monitors my purchasing patterns" (0.20). A few statements dip into negative correlation, the lowest of which being statement 12, "I mind when my information is shared with third parties" (-0.067). There is not much information to glean from this; the three highest positively correlating statements do not have a trend running through them (besides the first and the last both dealing with internet browsing habits, albeit tangentially on the last) and they are not highly positively correlated with the dependent variable. This implicitly means that an increase in attitudes towards Internet privacy does not lead to an increase in Dark Web knowledge. The two variables do not have much positive impact on each other and at worst they are negatively correlated.

The second method of analysis chosen was the t-test, which examines two groups to see if they are statistically different from each other. It compares the means of both groups to see how similar they are, which goes to show how much overlap there is in each section. I wanted to test each variable individually against

Factor 7, “I am knowledgeable about the Dark Web and its uses.” To do this, I selected the first question of each factor to use as the first group (as the first question was generally the most explanatory for the entire factor) and used the first question of Factor 7 as the second group. In this case, the null hypothesis is that the two variables measured in the test have no relationship to each other. I used the standard alpha of 0.05 for all of the tests.

t-Test: Two-Sample Assuming Unequal Variances

	Variable 1	*Variable 2*
Mean	2.350649	2.792208
Variance	1.467532	1.666781
Observations	77	77
Hypothesized Mean Difference	0	
df	151	
t Stat	-2.18858	
P(T<=t) one-tail	0.015082	
t Critical one-tail	1.655007	
P(T<=t) two-tail	0.030164	
t Critical two-tail	1.975799	

Figure 3.1

Figure 3.1 shows the first question of Factor 7 tested against the first question of Factor 1, “I mind when a website uses my PII to customize my browsing experience.” The alpha of these results, 0.030164, is less than the alpha used to conduct the test, 0.05, the null hypothesis is rejected, meaning that the two variables have a statistically significant relationship.

t-Test: Two-Sample Assuming Unequal Variances

	Variable 1	*Variable 2*
Mean	1.506494	2.792208
Variance	0.411141	1.666781
Observations	77	77
Hypothesized Mean Difference	0	
df	111	
t Stat	-7.82664	
P(T<=t) one-tail	1.6E-12	
t Critical one-tail	1.658697	
P(T<=t) two-tail	3.19E-12	
t Critical two-tail	1.981567	

Figure 3.2

Figure 3.2 shows the first question of Factor 7 tested against the first question of Factor 2, "I want the option to decide how my PII is used." Again, the variables are statistically significant, as the alpha is far less than 0.05.

	Variable 1	*Variable 2*
Mean	1.844156	2.792208
Variance	1.291183	1.666781
Observations	77	77
Hypothesized Mean Difference	0	
df	150	
t Stat	-4.83706	
P(T<=t) one-tail	1.62E-06	
t Critical one-tail	1.655076	
P(T<=t) two-tail	3.24E-06	
t Critical two-tail	1.975905	

Figure 3.3

Figure 3.3 shows the first question of Factor 7 tested against the first question of Factor 3, "I mind when a website discloses my buying patterns to third parties." Again, the alpha value of the results is much lower than the alpha used to conduct the test, so we can reject the null hypothesis.

t-Test: Two-Sample Assuming Unequal Variances

	Variable 1	*Variable 2*
Mean	1.831169	2.792208
Variance	1.273753	1.666781
Observations	77	77
Hypothesized Mean Difference	0	
df	149	
t Stat	-4.91783	
P(T<=t) one-tail	1.14E-06	
t Critical one-tail	1.655145	
P(T<=t) two-tail	2.29E-06	
t Critical two-tail	1.976013	

Figure 3.4

Figure 3.4 shows the results of the testing done on the fourth factor. Once again, the alpha is less than 0.05, so we can reject the null hypothesis.

t-Test: Two-Sample Assuming Unequal Variances

	Variable 1	*Variable 2*
Mean	1.454545	2.792208
Variance	0.488038	1.666781
Observations	77	77
Hypothesized Mean Difference	0	
df	117	
t Stat	-7.99625	
P(T<=t) one-tail	5.11E-13	
t Critical one-tail	1.657982	
P(T<=t) two-tail	1.02E-12	
t Critical two-tail	1.980448	

Figure 3.5

Figure 3.5 shows the first question of Factor 5 tested against the first question of Factor 7. Once again, the alpha is lower than 0.05, so we can reject the null hypothesis

t-Test: Two-Sample Assuming Unequal Variances

	Variable 1	*Variable 2*
Mean	1.454545	2.792208
Variance	0.488038	1.666781
Observations	77	77
Hypothesized Mean Difference	0	
df	117	
t Stat	-7.99625	
P(T<=t) one-tail	5.11E-13	
t Critical one-tail	1.657982	
P(T<=t) two-tail	1.02E-12	
t Critical two-tail	1.980448	

Figure 3.6

Figure 3.6 holds the results for the final test in which the first question of Factor 6 was tested against the first question in Factor 7. Once again, we cannot reject the null hypothesis.

Suggestions for improvement

The statements regarding privacy in the first section of the survey are very broad and easy to agree with. For example, most Internet users are probably worried about hackers on some sort of broad level or most users would like to be notified when their PII is being used in ways they had not previously agreed to. The fact that several early questions (especially in factor 4) had little to no disagreement proves this. These broad, generally agreeable statements may not have probed deep enough to prove any sort of deeper investment into privacy issues and therefore agreeing with them does not prove that the respondents would seek out ways to remedy their fears. Using more pointed, direct statements may be more effective. PII is also a broad term that could potentially have a connotation from person to person, which could also skew the results. Finally, this study was also done exclusively with management information systems students. Perhaps widening the scope to those outside of college as well could provide more enlightening answers.

CONCLUSION

Tor and the Dark Web are tools to circumvent government surveillance and prying eyes. They exist to maintain anonymity on the Internet and could be considered a form of peaceful, civil disobedience (depending on what that communication is used for). Findings from the research conducted suggest that concern with internet privacy issues and the use of personally identifying information by websites and third parties is not correlated to dark web knowledge or usage. Most respondents agreed or strongly agreed with the statements regarding privacy but those concerns did not translate to a need or want to circumvent them with Tor.

Why could that be? 45.45% of respondents that used Tor at all said that they were apprehensive about using the system, even though responses to other questions indicate positive attitudes towards using Tor. It stands to reason that the number of those that are apprehensive about Tor that have never touched it could be higher. Could it be the social stigma? The term "Dark Web" is generally associated with buying drugs on the internet or viewing illicit pornography, two acts that most people do not want to be associated with. Or could it perhaps be that they are frightened of being put on the ever present "watch list" that the government holds? Regardless of the reason, my hypothesis that a higher concern with Internet privacy leads to higher Dark Web awareness is incorrect. However, each of the representative questions for the factors were statistically significant in some way. Taken individually, each of the factors seems to have some sort of an effect on Dark

Web knowledge, but across the board they aren't correlated. It is possible that the impact that each of the variables has on Dark Web awareness is small, albeit significant, meaning that my hypothesis is indeed correct, but a simple glance at the numbers seems to prove that wrong. All that was tested for is that the variables were statistically significant in their impact, not that the impact was positive or negative.

Even though I was wrong, this leads to even more questions and more opportunities for research. Could it be that Tor is just too much for the average user? Has the media stigmatized it too much? It is very interesting that concerns with Internet privacy do not lead to a need to circumvent it. Perhaps some citizens have just given in and felt like there is nothing they can do to protect themselves.

Limitations

This research was subject to limitations. The first limitation of this project was the demographic. While the sample size of 79 is reasonable, the study was only conducted with management information systems students, most above the age of 20 and below 30. While opening the demographics up to people out of college may just make the variables even less correlated, it could also provide a more true to life picture.

In addition, the thesis was limited by the instrument chosen. While the instrument provided valuable insight into attitudes regarding internet privacy issues, it contains questions about marketing research and other topics that are

slightly outside the scope of the study. The original instrument was created by examining health care websites' privacy policies. That may give some insight into the kinds of privacy invasions that people agree to, but does not exactly fit the standards of government surveillance.

While those attitudes are included within the broad umbrella of "privacy issues," they may be a little too broad to lead to the expectation that the respondents would use Tor; that is to say, just because you are concerned that Facebook is changing its ads to reflect what you have looked at on Amazon, that does not mean you are going to seek out Tor. Many of the issues brought up by the statements have solutions outside of accessing a new network, such as ad blocker software or browser extensions like NoScript. The Dark Web factor may have also been not extensive enough to really grasp the question of "why," even though that was not necessarily a part of the hypothesis. Even the nature of a survey itself (given in class, no less) lends itself to potentially less than honest answers.

Further Research

For further research, I would first suggest expanding the scope of the research to include those out of college. If the focus remains people who are computer savvy (as is the assumption when dealing with management information systems students), possibly expand it out to IT professionals. I would also recommend expanding the instrument to include more questions about specific

government surveillance, possibly in an entirely new factor, and expanding the Dark Web section to include some of the ideas from the Unified Theory.

REFERENCES

Raine, Lee, and D'vera Cohn. "Cenus: Computer ownership, Internet connection varies widely across U.S." *Pew Research Center*. 14 Sept. 2014. 17 March 2015.

United States. Select Committee to Study Government Operations. *Supplementary Detailed Staff Reports of Intelligence Activities and the Rights of Americans*. Washington: GPO. Web. 18 March 2015. <http://www.aarclibrary.org/publib/church/reports/book3/html/ChurchB3_0001a.htm>.

Monnat, Daniel E., and Anne L .Ethen. "A Primer on the Federal Wiretap Act and Its Fourth Amendment Framework." *Kansas Trial Lawyers Association Journal* March (2004): 12-15. Web. 18 March 2015. <http://www.monnat.com/wpcontent/uploads/2012/03/Wiretap.pdf>.

Foreign Intelligence Surveillance Act of 1978. Pub. L. 95-511. 92 Stat 1783. 25 October 1978. Web. 20 March 2015. < http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf>.

Swire, Peter. "The System of Foreign Intelligence Surveillance Law." *George Washington Law Review*. 72 (2004): 1-104. Web. 20 March 2015.

USA PATRIOT Act. Pub. L. 107-56. 115 Stat 272. 26 October 2001. Web. 1 April 2015. <http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf>.

Podgor, Ellen S. "Computer Crimes and the USA PATRIOT Act." *Criminal Justice Magazine* 17.2 (2002). Web. 2 April 2015. <http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_17_2_crimes.html>.

"Clearing Up Confusion – Deep Web Vs. Dark Web." *Brightplanet*. n.p. 27 March 2014. Web. 15 April 2015. <http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/>.

Leger, Donna Leinwand. "FBI Cracks Silk Road." *USA Today* 15 May 2014. Web. 15 April 2015. <http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/>.

Tor: Overview. Tor Project. n.d. Web. 16 April 2015.

<https://www.torproject.org/about/overview.html.en>.

Tor Users. Tor Project. n.d. Web. 16 April 2015.
<https://www.torproject.org/about/torusers.html.en>.

Abuse FAQ. Tor Project. n.d. Web. 16 April 2015.
<https://www.torproject.org/docs/faq-abuse.html.en>.

Tor FAQ. Tor Project. n.d. Web. 16 April 2015.
<https://www.torproject.org/docs/faq.html.en>.

Dierks, T. and E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.2." Internet Engineering Task Force. August 2008. Web. 20 April 2015. <http://tools.ietf.org/html/rfc5246?as_url_id=AAAAAAVBehpzRqATU5xWpMSTPjTY4oV6aOnai43OyHdsdcjqdSlYu0y-i_wtuyMcDhdfR_le_fBCnWW1xu50YwXZ7oot>.

Kirkpatrick and Lockhart LLP. "The Homeland Security Act of 2002 – A Summary." *Homeland Security Bulletin*. March 2003. Web. 20 April 2015. <http://www.martindale.com/matter/asr-8824.pdf>.

Homeland Security Act of 2002. Pub. L. 107-296. 116 Stat 2135. 25 November 2002. Web. 25 April 2015. <http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf>.

"Let the Sun Set on PATRIOT: Section 212 and Homeland Security Act Section 225: 'Emergency Disclosure of Electronic Communications to Protect Life and Limb." Electronic Frontier Foundation. n.d. Web. 25 April 2015. <https://w2.eff.org/patriot/sunset/212.php>.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The Second-Generation Onion Router." Tor Project. n.d. Web. 25 April 2015. <https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>.

Fahrenheit 9/11. Dir. Michael Moore. Lionsgate Films, 2004.

Earp, J.B.; Anton, A.I.; Aiman-Smith, L.; Stufflebeam, W.H. "Examining Internet privacy values within the context of user privacy values." IEEE Transactions on Engineering Management. 2005. 6 December 2015. <http://ieeexplore.ieee.org.umiss.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=1424412>.

Anton, Annie I.; Earp, Julie B.; Young, Jessica D. "How Internet Users' Privacy Concerns Have Evolved Since 2002." IEEE Security and Privacy. 29 July 2009. 6 December 2015. <http://theprivacyplace.org/blog/wp-content/uploads/2009/07/tr_2009_16.pdf>.

Preibusch, Soren. “Guide to measuring privacy concern: Review of survey and observational instruments.” Int. J. Human-Computer Studies. 71 (2013) 113-1143. 15 September 2015.

Venkatesh, Viswanath, Micheal G. Morris, Gordon B. Davis, and Fred D. Davis. “User Acceptance of Technology: Towards a Unified View.” MIS Quarterly. September 2003. 6 December 2015. < http://nwresearch.wikispaces.com/file/view/Venkatesh+User+Acceptance+of+Information+Technology+2003.pdf>.

APPENDIX 1: INSTRUMENT

Factor 1: Personalization

1. I mind when a website uses my personally identifying information (PII) to customize my browsing experience.
2. I mind when a website uses cookies to customize my browsing experience (A cookie is information that a website puts on your hard disk so it can remember something about you at a later time).
3. I mind when a website uses my purchasing history to personalize my browsing experience (e.g. by suggesting products for me to purchase).
4. I mind when my PII is used for marketing or research activities.
5. I mind when a Web site monitors my purchasing patterns.

Factor 2: Notice/Awareness

1. I want the option to decide how my PII is used.
2. I want a Web site to disclose security safeguards used to protect my PII.
3. I want a Web site to disclose how my PII will be used.
4. I want a Web site to inform me before using my PII in a manner that it had not previously disclosed to me.
5. I want a Web site to keep me informed of changes to its privacy practices.

Factor 3: Transfer

1. I mind when a Web site discloses my buying patterns to third parties.
2. I mind when my information is shared with third parties.
3. I mind when my PII is traded with or sold to third parties.

Factor 4: Collection

1. I mind when a Web site that I visit collects (without my consent) information about my browsing patterns.
2. I mind when a Web site that I visit collects (without my consent) information about my browser configuration
3. I mind when a Web site that I visit collects (without my consent) information about my IP address (a number that identifies you computer from all other computers on the Internet).
4. I mind when a Web site that I visit collects (without my consent) information about the type of computer/operating system I use.
5. I mind when a Web site records the previous Web site I visited.

Factor 5: Information Storage

1. I am concerned about unauthorized employees getting access to my information.
2. I am concerned about unauthorized hackers getting access to my information.

Factor 6: Access/Participation

1. I want a Web site to allow me to check my PII for accuracy.

2. I want a Web site to allow me to modify my PII.

Factor 7: Dark Web

1. I am knowledgeable about the Dark Web and its uses.
2. I plan on accessing the Dark Web through the TOR network in the future or have in the past.
3. My knowledge of the Dark Web is limited.