To the Graduate Council:

I am submitting herewith a thesis written by Rhonda Marisa Clossum entitled "Information Privacy: A Quantitative Study of Citizen Awareness, Concern and Information Seeking Behavior Related to the Use of the Social Security Number as a Personal Identifier." I have examined the final this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Information Sciences.

Suzie Allard, Major Professor

We have read this thesis
and recommend its acceptance:

Dwight L. Teeter, Jr.

Kimberly Louise Black-Parker

Accepted for the Council:

Carolyn R. Hodges
Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

INFORMATION PRIVACY:
A Quantitative Study of Citizen Awareness, Concern and Information Seeking Behavior Related to the Use of the Social Security Number as a Personal Identifier

A Thesis Presented for
the Master of Science
Degree
The University of Tennessee, Knoxville

Rhonda Marisa Clossum
May 2010

ACKNOWLEDGEMENTS

First, I would like to thank Dr. Suzie Allard for accepting my topic as a viable area of research for the information sciences profession and serving as committee chair. I want to thank Dr. Dwight Teeter, committee member, for sharing my indignation and providing us all with levity throughout the process. I want to thank Dr. Kimberly Black, committee member, for her endless encouragement and support. And, finally, I want to thank Cary Springer, University of Tennessee statistician, for her expertise and patience with me in devising the survey and analyzing the results.

ABSTRACT

Information technology has transformed the manner in which personal identifying information is collected, stored and shared in government agencies and private businesses. The social security number has become the de facto identifier for individuals due to its notable qualities: a nine-digit number assigned to one person by the United States government. As individuals are increasingly asked to disclose personal information, the question arises: How does the lack of awareness of social security number laws contribute to the loss of privacy, loss of control of personal information and the threat of identity theft? This study examines awareness levels of social security number laws and policies that affect individuals' daily lives from the perspective of the information science profession. This study also examines concerns relative to widespread usage of the social security number. A quantitative research method using an online survey was employed using convenience and snowball sampling of adult university students and other community members. Survey results were analyzed by age, gender, educational achievement and student status. Awareness levels were shown to differ significantly by age. There were no differences in overall concern found to exist by any demographic. Survey results showed libraries were consulted for privacy information less often than search engines. Study findings support increasing awareness levels of privacy laws by encouraging use of library resources.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure Page

Chapter 1: The Social Security Number and Individual Privacy

Introduction

The 1936 legislation enacted by the Social Security Administration established the Social Security Number (SSN) as a means to track worker earnings to determine future Social Security benefits (GAO-07-1023T, 2007).[1] At the time of its inception, the SSN was expressly established so as not to be used as identification (Strum, 1998). Since then, the SSN has evolved into the key identifier for virtually all persons by public and private entities (Strum, 1998; Hendricks, 1990; GAO-HEHS-99-28, 1999; GAO-06-495, 2006). Use of the SSN has escalated to the point that it is requested for most financial transactions and in many instances where the SSN was not previously requested in situations common to everyday living (*Social Security Numbers in Commerce*: *Reconciling Beneficial Uses with Threats to Privacy*, 2006). The SSN has become what many consider to be the de facto identifier for individuals because of its notable qualities: a nine-digit number assigned to one person by the United States government (GAO/HEHS/AIMD-00-253R, 2000; GAO-02-830T, 2002; *Protecting the Privacy of Consumers' Social Security Numbers*, 2004; *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves*, 2002; Strum, 1998; Hendricks, 1990; Solove, 2004). Information technology has transformed the manner in which personal information is collected, stored and shared between government and private agencies (Klosek, 2007; Nicoll, 2002.; Solove, 2008; Strum, 1998). Gone are the days when paper files containing

---

[1] The Government Accountability Office (GAO) publications are listed by report number and date of publication. A listing of GAO reports used throughout this study is found in Appendix C.

personal information are kept in a locked file cabinet at a single location (Miller, 1971; Solove, 2004). Today, personal information is collected, stored and shared electronically which provides easier access to more parties while simultaneously removing protection for individuals which resulted from maintaining files in a single physical location. Electronic data storage provides convenience in accessing personal information such as SSNs for processing of applications for goods and services but may result in reducing personal control over its dissemination. United States citizens must chronicle significant life events such as marriage, voting, adoption, and professional licensing at the state level and are thus obliged to divulge personal information to obtain these services (Tenn. Code Ann. §§ 68-3-402 (2007); 2-2-116 (Supp. 2008); 36-1-126 (2008); 36-5-1301 (2005)). School enrollment, medical care, and commercial transactions may involve revealing personal information to public agencies, private agencies or both types of agencies (*Social Security Numbers in Commerce*: *Reconciling Beneficial Uses with Threats to Privacy*, 2006; *Protecting the privacy of consumers' social security numbers.* 2004; *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves*, 2002).

The SSN has come to be used as the most common identifier because it is permanent, ubiquitous and unique to each individual (*Security in Numbers: SSNs and ID Theft*, 2008, p.2). Identifiers such as name and date of birth are often widely known and often lack uniqueness. Consequently, SSNs are often used in place of name as the primary identifiers in many databases (Strum, 1998). However, the SSN is often used as an authenticator. Authentication is the process by which a person verifies that he or she is who they purport to be (*Security in Numbers: SSNs and ID Theft*, 2008, p.4). The use of the SSN as an authenticator is where identity theft, the criminal act of using another person's means of identification, such as name, date of birth and SSN to violate federal, state or local law, most often occurs (*Security in Numbers: SSNs and ID Theft*, 2008). To be effective, authenticators must be secret and are best used for a limited purpose; much like a computer password would be used (*Security in Numbers: SSNs and ID Theft*, 2008). With the passage of the Privacy Act in 1974, Congress recognized the dangers of widespread use of SSNs as a universal identifier in the public and private sectors by stating it is *"one of the most serious manifestations of privacy concerns in the Nation"* (http://epic.org/privacy/ssn/). Awareness of SSN laws with regard to disclosure of SSNs is vital for persons to better protect themselves.

Purpose of the Study

The focus of this thesis is information privacy and security from the perspective of the information science profession and of individual citizens as well. Information privacy is defined as the legal and political relationship between collection and dissemination of personal data (Hendricks, 1990; Strum, 1998). Information security is defined as the protecting of information and information systems from unauthorized access, use, disclosure, modification or destruction. (44 U.S.C. § 3542(b)(1). Information security is a multi-step process to protect personal information which entails:

- Identifying and assessing risks;
- Establishing and implementing policies and controls;
- Promoting awareness and providing security-related training; and
- Monitoring and evaluating established policies and controls, and addressing known security vulnerabilities (GAO-03-44, 2003).

This study on individual awareness of federal and Tennessee state Social Security Number (SSN) laws that govern disclosure examines the information seeking behavior pertaining to information privacy and explores how awareness of privacy laws influences a person's decision to disclose his SSN. In addition, this study explores concerns related to the disclosure of SSNs to learn if individuals are more likely to disclose their SSN depending on the agency or business. Differences in awareness, concern and information seeking behavior will be analyzed by age, gender and education.

For this study, information seeking behavior is defined as a conscious effort to acquire information in response to a need or gap in knowledge. This study encompasses the concept of information seeking behavior in relation to how individuals seek and utilize privacy information and privacy laws. Findings from this study will help to gauge privacy literacy and are important because study results could be used for the development of the framework to increase privacy literacy. The survey instrument was developed to help answer the research questions to further the understanding of information privacy.

Significance of the Study

Past information seeking research has focused on the acquiring of information with the affective symptoms of uncertainty, confusion and frustration that are present in the early stages of the research process (Kuhlthau, 1993b; Case, 2007) has found the greater the number of people who are affected by a decision, the more importance is to afforded to research on a particular topic. For instance, medical research of treatment of a heart condition that may affect billions is given more research time and funding than is given for research into a singular car purchase (Case, 2007, pp. 10-11). This study of SSN law literacy is an important research topic because although people may think of SSNs as being disclosed on an individual level, the scope of disclosure of this powerful individual identifier affects millions of Americans, essentially everyone.

A research gap exists in the awareness and concerns of individuals disclosing their private information in the era of information technology where personal information is often maintained indefinitely. This study approaches the topic from several perspectives: an individual's awareness of SSN privacy laws at the federal and state levels; an individual's concerns regarding the disclosure of one's SSN and information seeking behavior of persons seeking privacy information.

As citizens are increasingly asked to share personal information routinely placed in shared databases, the question of how the lack of awareness of SSN legislation contributes to the loss of privacy, lack of control of personal information and the threat of identity theft arises. A study of the awareness of relevant laws; concerns regarding the impact of disclosure; and information seeking behavior will help to explain the gap that exists between privacy laws and awareness of those laws. A review of literature regarding information privacy literacy and libraries revealed very little data on individual awareness or information seeking behavior regarding SSN laws. Informal anecdotal accounts from librarians suggest this topic is not the subject of common inquiry from users.

Statement of the Problem

The awareness of applicable privacy laws and the ability to understand the impact of those laws on common activities will allow a person to act with informed consent in sharing his or her personal information. Not every question about SSNs calls for the assistance of a legal professional. Much like the void filled by health sciences librarians in response to medical questions from patrons either before or after a visit to a physician, librarians and other information professionals at public and specialized information agencies are called upon to assist information seekers by providing them with tools needed to locate useful information that is applicable to their specific circumstances.

Examples of information privacy reference questions that may be presented to librarians are:

- Where can find out if I can still register to vote in Tennessee if I refuse to give my Social Security Number?
- I want to get internet service at home. I was told by the Internet Service Provider (ISP) agent that I need to give my Social Security Number because of the Patriot Act. How can I find out if this is true?
- I have a toothache. I went to one of those storefront dental offices but they wouldn't help me without my Social Security Number even though I was going to pay in cash. Where are the laws found on private medical offices' right to my Social Security Number?
- Somebody's been using my Social Security Number. I want to know how I can get a new one.

These types of reference questions suggest there are significant gaps in library patrons' knowledge of privacy laws. To better understand the nature of the knowledge gap, the following research questions were developed for this study.

Research Questions

This study is an exploratory, descriptive research project. Research questions have been designed to examine what individuals know about privacy laws, what their concerns are and how individuals go about finding information on privacy and SSN laws.

Awareness

- What are the levels of awareness of federal and state of Tennessee privacy laws pertaining to Social Security Numbers?

Concern

- What are the levels of concern pertaining to the disclosure of one's Social Security Number?

Information Seeking

- What sources are used to find information on laws pertaining to the disclosure of the Social Security Numbers?

Chapter 2: Literature Review

The relevant literature for this study forms the basis for the research questions and the survey instrument. Included in the literature review is examination of the uses of the SSN from its inception, applicable laws germane to issues related to the uses of the Social Security Number (SSN) and prior information seeking behavior research.

Federal laws examined are Fair and Accurate Credit Transaction Act (FACTA); Fair Credit Reporting Act (FCRA); Family Education Rights and Privacy Act (FERPA); Gramm-Leach-Bliley Act (GLBA); Health Insurance Portability and Accountability Act (HIPAA); Drivers Privacy Protection Act (DPPA); Privacy Act of 1974; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot Act); and the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments of the United States Constitution.

In Tennessee, the Tennessee Code Annotated controls the collection of SSNs at the state level. These laws apply to all aspects of a citizen's life literally from birth to death.

The monographs reviewed provide the foundational concepts of privacy and security of information. One author stands out in the literature, privacy expert and George Washington Law School Law Professor, Daniel J. Solove. Professor Solove has written five books (including a law school textbook) on the subject of privacy, published in leading law reviews and appeared before the U.S. Supreme Court in privacy appeals.   His books, *Understanding Privacy* and *The Digital Person: Technology and Privacy in the Information Age* will be highlighted in this study.

Increasingly active are the privacy protection watchdog groups which assist in the dissemination of information pertaining to privacy rights and legislation. These grass-roots organizations help to close the gap of knowledge and understanding of complicated laws and policies that request or compel the disclosure of private information.

History of the Social Security Number

The examination of the uses of the SSN from a historical perspective shows how the identifier came into widespread usage. The Social Security Board was started in 1935 by President Franklin Delano Roosevelt as part of the New Deal. The 1936 legislation enacted by the Social Security Board (renamed the Social Security Administration in 1946) began enumeration of SSNs solely as a means to track worker earnings to determine eligibility for future social security benefits (GAO-07-1023T, 2007). At the time of its inception, the SSN was expressly established so as not to be used as identification (Strum, 1998). Imprinted on the original cards and through the 1960s was the inscription "FOR SOCIAL SECURITY PURPOSES – NOT FOR IDENTIFICATION," (see, Appendix A, Figure 2, *Original Design of Social Security Card*).

But in 1937, expanded use of the SSN began when individual states started using SSNs for unemployment insurance. In 1943, President Roosevelt gave authorization through Executive Order 9397 to use SSNs for data systems requiring permanent account numbers for individuals, in essence giving federal agencies permission to expand the use of the SSN beyond its original purpose (Hendricks, 1990, pp.62-63). In 1961, the Internal Revenue Service (IRS) designated the SSN as the taxpayer identification number and in 1962 the IRS mandated that all taxpayers include their SSN on their tax return (Strum, 1998; Hendricks, 1990).

In 1976, the Tax Reform Act granted states permission to collect SSNs for additional uses including motor vehicle registration, driver licensing, administration of local and state laws and public assistance (Hendricks, 1990). The year 1976 also brought implementation of the Parent Locator Service to collect delinquent child support payments. The Interest and Dividend Tax Compliance Act of 1983 was enacted to ensure that taxpayers were correctly reporting their interest income to the Internal Revenue Service by requiring bank depositors to disclose their SSN to financial institutions (26 U.S.C. 1).

The Tax Reform Act of 1986 required children over the age of five who are claimed as dependents to have their SSN listed on tax returns. Two years later, the Tax Reform Act of 1988 required that children of any age claimed as dependents on tax returns are identified with their SSN (Hendricks, 1990; Strum, 1998). Now, parents have the option of applying for both a birth certificate and a Social Security Card for a newborn in the hospital at the time of the child’s birth eliminating a need to visit to the Social Security office (*Social Security Numbers for Children*, 2009).

When the use of the SSN became pervasive in the early 1970s, one of the two major complaints by the citizenry was that people would now be known as a numbers, not as individuals. During the administration of President Jimmy Carter, an investigation in 1977 by the Privacy Protection Study Commission found this labeling of individuals to be the major objection. The other objection to the expanded use of the SSN was the distrust of the government agencies compiling and sharing files without the knowledge or control of citizens, (*Personal Privacy in an Information Society*, 1977). There was no mention of identity theft as a potential threat in that study. Identity theft has in recent years been the highest growing crime in America resulting in financial loss to businesses and consumers with the concurrent inconveniences associated with correcting business files and repairing consumer credit (GAO-05-1016T, 2005; GAO-07-737, 2007; GAO-02-363, 2002). The Government Accountability Office (GAO) has found inclusion of SSNs in business databases and online commerce for individual identification and authentication purposes increases the risk of identity theft whereby all aspects of a person's life could be adversely affected including loss of financial solvency; denial of employment opportunities; access to health care; threat to personal reputation and, potentially, one's own liberty (GAO-05-59, 2004; GAO-06-833T, 2006; GAO-02-691T, 2002).

There has been alarm in recent years regarding increasing requests for disclosure of the SSN for identification: The use of SSNs has escalated to the point where it is requested for most financial transactions and in many instances where it was not previously requested in situations common to everyday living. A new bank account, cell phone and Internet service, purchase or rental of a home, or obtaining medical services are just some examples of instances that often include the perfunctory request for an SSN (*Social Security Numbers in Commerce*: *Reconciling Beneficial Uses with Threats to Privacy*, 2006). Instances of requests for SSNs in commercial transactions include applying for credit, employment, utilities (gas, electricity, and telephone), bank accounts, brokerage accounts, insurance, medical and dental services, health plan reimbursement, and enrollment in educational institutions (Strum, 1998). Testimony by Florida Congressman E. Clay Shaw, Jr. in a congressional hearing held in September 2004 relayed an instance when a refusal to provide an SSN to open a department store credit account resulted in denial of credit and the loss of a twenty percent discount on the cost of the merchandise, (*Protecting the Privacy of Consumers' Social Security Numbers*, 2004).

The original purpose of the SSN has yielded to demands for a consistent means of identification requisite with the universal use of electronic recordkeeping (Solove, 2004). Aside from the superior means of documentation, SSNs carry a lot of power with the capability to allow persons to verify identity in order to obtain loans and employment, open and close accounts and to engage in many other consumer transactions. This power in turn presents opportunities for threats to privacy and loss of control over personal affairs (GAO-07-1023T, 2007).

In addition to the federal and commercial uses of the SSN, states collect and use this unique label to administer many state-regulated activities (Hendricks, 1990). SSNs are used widely in state databases for administrative purposes prompting several states to enact legislation addressing SSN security more than others (GAO-06-586T, 2006; GAO-1016T, 2005). In the state of Tennessee, SSNs are required to obtain state benefits and participate in many state-legislated activities including marriage, divorce, establishing paternity, driver licenses, adoption, fishing licenses and registering to vote (Tenn. Code Ann. §§ 36-5-1301; 36-4-106; 36-2-311; 5-50-321; 36-1-126; and 2-2-127). Consequently, if an individual chooses not to comply with mandatory SSN disclosure requirements in the state of Tennessee, he will be denied the right to engage in the aforementioned activities, among many others (see Appendix B, *Selected Tennessee Social Security Number Laws*).

Federal Privacy Legislation

The Privacy Act of 1974 (Privacy Act) addresses the collection, use, and disclosure of personal information by government agencies. This legislation came about in response to concerns of federal government collection and sharing of personal information and the burgeoning computer matching capability of government agencies. The Privacy Act, still valid today, is applicable only to the collection of personal information in public databases. Under this Act, agencies that collect SSNs must inform individuals if the disclosure is mandatory or voluntary; the principal purpose or purposes for which the SSN is intended to be used; the routine uses which may be made of the SSN; and the effects of not providing the SSN (5 U.S.C. Sec. 552a). Although it is unlawful for any federal, state or local government agency to deny any rights, benefits, or privileges provided by this law because of a refusal to disclose one's SSN, the Privacy Act does not apply to any federal, state or local agency which collected SSNs prior to the January 1975 effective date (5 U.S.C. Sec. 552a; http://epic.org/privacy/laws/privacy_act.html). The Privacy Act deliberately excluded private businesses from compliance with the Privacy Act, the rationale being that consumers could always decline to share personal information with a business that demanded an SSN (5 USC Sec. 552a). The problem with that lack of foresight is the empirical fact that collection of SSNs has now become the standard for tracking clients in just about every industry (Hendricks, 1990).

Subsequent to the Privacy Act, other legislation has been introduced at the federal level by concerned legislators who have taken an interest in the problems related to the proliferation of Social Security Number use. Included are:

- Drivers Privacy Protection Act (DPPA). The DPPA was enacted in 1994 in response to instances of stalking, assault and murder that occurred when private information was retrieved at a small cost by anyone who requested such information from a state Department of Motor Vehicles (DMV). This Act prohibits obtaining or disclosing SSNs and other personal information from a motor vehicle record except as expressly permitted under the law. States routinely collect SSNs when issuing driver and vehicle licenses, with some states offering the choice of whether to display the SSN on front of the driver license (18 U.S.C. § 2721, 1994; GAO-05-1016T, 2005; and http://epic.org/privacy/drivers).

- Fair Credit Reporting Act (FCRA) enacted in 1970 and amended by FACTA controls the collection, use and dissemination of consumer information. Under FCRA, credit reports generated by consumer activity regulate consumer reporting agencies (CRAs) and other gatherers and users of consumer reports (15 U.S.C. § 1681 et seq.).
- Fair and Accurate Credit Transaction Action (FACTA) is a tool for citizens to fight the threat and occurrences of identity theft. This law originally enacted in 2003 and amended in 2007 gives consumers the right to challenge accuracy in credit reports, disclosure of personal information and sharing of information between consumer agencies. Under this law, more protections are provided than are offered under FCRA, e.g., a yearly credit report is provided free of charge upon request (15 U.S.C. 1601 note).
- Family Education Rights and Privacy Act (FERPA) guarantees students the right to view their educational records; to request amendments of inaccuracies in their record; to control the release of personal information; and to have the ability to file a complaint with the Department of Education at the federal level of allegations of failure to comply with the law (20 U.S.C. 1232g 1974).
- Gramm-Leach-Bliley Act (GLBA) enacted in 1999 granted banks the authority to consolidate and, in doing so, made personal information the shared information of those institutions. Privacy of information became a major component of the legislation mandating that financial institutions establish a privacy policy and provide consumers

with annual written notice (12 U.S.C. 1811 note 1999).

- Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to protect patient privacy. The Privacy Rule and the Security Rule were both added in 2003 with varying mandatory compliance dates. These rules complement each other in order to help regulate the use and disclosure of confidential patient information, (45 C.F.R. § 160 and 164 1999).
- USA PATRIOT Act enacted six weeks after the terrorist acts of September 11, 2001 and amended in 2006 does not specifically mention the requirement for the Social Security Number in government or consumer transactions (18 U.S.C. 1 note 2001). However, the Patriot Act has recently been used by private industry as a justification to require the disclosure of one's SSN (http://consumerist.com/5053222/comcast-the-patriot-act-mandates-we-need-your-ssn).
- U.S. Constitution does not explicitly guarantee a "right" to privacy. Privacy rights are invoked to address specific circumstances through the application of the amendments contained in the Bill of Rights and the Fourteenth Amendment. (Strum, 1998, pp. 3-15; Bielefield & Cheeseman, 1994, pp. 38-39).

The First Amendment - *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or the press, or the right of the people to assemble, and to petition the Government for a redress for grievances.* Commonly referred to as the *freedom of the press amendment* or the *privacy of beliefs amendment*, the stated language of the First Amendment is explicit: Congress was forbidden from abridging freedom of the press, religion, speech, assembly, and redress for alleged wrongs. The First Amendment was not extended to prevent state actions until the third decade of the 20^{th} Century (Teeter & Loving, 2008, pp. 20-22, 52-54). Interpreted into the First Amendment and the other constitutional amendments are the penumbral rights or those found in the shadows that emanate from history, purpose and interpretation (Bielefield & Cheeseman, 1994). Two key cases applicable here are *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684 (1961), and *Griswold v. Connecticut*, 381 U.S. 479, 85 S.Ct. 1678 (1965). *Mapp* was a search and seizure decision; *Griswold* overturned a state law regulating birth control practices of married couples. In *Mapp*, Justice William O. Douglas wrote for the majority that a constitutional right to privacy existed in "penumbra" emanating from various provisions of the Bill of Rights. Although privacy is not mentioned in the Constitution, Justice Douglas found privacy protection in the first eight Amendments and the Fourteenth Amendment. Taken together, those provisions include the right to be secure against unreasonable searches and seizures in one's home, plus the underlying principle of due process of law as stated in both the Fifth and Fourteenth Amendments (Teeter & Loving, 2008, p. 381). It must be kept in mind that the Constitutional right of privacy is rather narrow and protects the public against government excesses, not intrusions by fellow citizens (Dwight. L. Teeter, personal communication, March 9, 2010).

The Third Amendment – *No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner* ... With this quartering of soldiers amendment, a constitutional zone of privacy of the home is created (Bielefield & Cheeseman, 1994).

The Fourth Amendment – *The right of people to be secure in their* *persons, houses, papers, and effects against unreasonable searches and seizure, shall not be violated* … This search and seizure amendment grants citizens privacy rights pertaining to their home and person.

The Fifth Amendment – *No person shall be …compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty or property without due process of law…* This amendment against self-incrimination in criminal cases allows individuals to the right to "take the fifth" to avoid accusing oneself.

The Ninth Amendment – *The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people*. This "implied rights" amendment is, effectively, a statement that other rights not otherwise enumerated are to be retained by the people.

The Fourteenth Amendment - *No State deprive any person of life, liberty, or property, without the process of law.* In this Civil Rights amendment, Section 1, the Due Process Clause ensures cities have constitutional protections at the federal and state levels.

Federal Agencies and Social Security Number Use Research

There are several government agencies involved in the research and protection of the SSN. Included are:

- The Government Accountability Office (GAO) is a nonpartisan agency in the legislative branch of the federal government operating as support to Congress. The GAO conducts research on the proper use of tax dollars and the effectiveness of government policies and operations. Additionally, GAO issues legal opinions and advises Congress of steps to take to improve efficiencies (see Appendix C, *GAO Privacy Reports*). The GAO research into the use and misuse of the SSN figures prominently into privacy information literature research (http://www.gao.gov).
- The Federal Trade Commission (FTC). The FTC's motto is "Protecting America's Consumers." In addition to its *Deter-Detect-Avoid ID Theft* campaign against identity theft, the FTC has a comprehensive website with links for consumers, businesses, law enforcement, military personnel, and the media. There is also a Reference Desk, "Identity Theft Resource Library," with links to state and national statistical data; reports on testimony before legislative bodies; current federal and state laws pertaining to identity theft; federal rules and educational materials for community activism (http://www.ftc.gov).
- The Social Security Administration (SSA) issues social security cards upon application with approved identification. Recently, the SSA has revised some its policies, including limiting the number of replacement cards to three per year and ten per lifetime to thwart misuse (http://www.ssa.gov/pubs/idtheft.htm). However, the

SSA has no legal authority to regulate the use or sale of SSNs which are routinely purchased from consumer reporting agencies and Internet resellers (GAO-06-495, 2006).

Tennessee Privacy Legislation

The state of Tennessee has enacted laws which reference to the SSN in everyday situations that impact its citizens' lives. These laws govern the collection, dissemination and retention of the SSNs in public records and are found in the Tennessee Code Annotated. Listed below are some of the Tennessee statutes that pertain to the collection of SSNs: The laws are divided from the general to the specific subject by title, section and chapter:

1. Title 2 Elections, Voter registration cards, § 2-2-124; Voter registration records, §2-2-127
2. Title 4, State Government: Dissemination of state citizens numbers, § 4-4-125
3. Title 10, Public Libraries, Archives and Records: Public records
   - Military discharge, § 10-7-513
   - Placement on documents, § 10-7-515
   - Redaction from electronic databases, § 10-7-515
4. Title 34, Guardianship: Conservators for disabled, § 34-1-109; Guardians for minors, § 34-1-109
5. Title 36, Domestic Relations: Licenses, § 36-5-1301; Records concerning divorce, paternity, etc., § 36-5-1302; §§ 68-3-401, 402
6. Title 39, Criminal Offenses: Identity theft, § 39-14-150
7. Title 55, Motor and Other Vehicles: Drivers' licenses, § 55-50-321

8. Title 68, Health, Safety and Environmental Protection: Death certificates, § 68-3-502

Tennessee Policies and Current Studies

Offices of Research and Education Accountability headed by the Tennessee Comptroller of the Treasury released a report, *Safeguarding Social Security Numbers in Tennessee Government Records,* in October 2008 on the use, collection and dissemination of SSNs. This report outlines the collection and processing of SSNs in public records from input garnered from custodians of personal information in the various state agency departments. The report offers recommendations for improving Social Security Number security.

Tennessee judicial findings from cases filed in state courts also have impact on the collection and use of SSNs by state agencies. For example, a lower court's summary judgment to deny a Tennessee resident the right to register to vote for failure to disclose his SSN was affirmed by the U.S. Court of Appeals, Sixth Circuit in September 2000. The requirement to provide an SSN was found not to have violated any part of the U.S. Constitution or the Privacy Act of 1974. Tennessee first made the SSN mandatory for voter registration in 1972. The Privacy Act of 1974 permits any federal, state, or local government agency requiring SSN disclosure prior to the January 1, 1975 cutoff date to continue to do so thus granting that agency the legal authority to deny benefits to a citizen who fails to provide his SSN, see McKay v. Thompson, 226 F.3d 752 (2000).

In February 2002, the Tennessee Attorney General, Paul G. Summers, issued a legal opinion, *Opinion No. 02-016, Confidentiality and Disclosure of Social Security Numbers,* in response to questions related to Tenn. Code Ann. § 4-4-125, Dissemination of state citizens numbers. In its opinion, the Attorney General's Office *found no general authority under which a* *state agency may coerce an individual to give permission to disseminate her social security number in exchange for a state service.* Yet, as noted above, a state agency may refuse services in certain circumstances to an individual if an SSN is not provided to the requesting agency.

Information Privacy in Practice

Current periodical articles in library and information science publications including the *Information Management Journal* and *Information Tod*ay give insight into how information professionals handle information privacy in practice. These articles show how information professionals must contend with the inherent conflict of protecting client and patron privacy while complying with privacy laws. An article in a 2007 edition of Information Management Journal reported that the Office of Management and Budget ordered all federal agencies to eliminate the unnecessary collection and use of SSNs by 2009 to combat data breaches and identity theft. (Agencies take steps to safeguard data, 2007). In a 2008 article in the American Libraries magazine entitled Delusions of Privacy, the author Leonard Kniffel grapples with the dichotomy of the importance of privacy in society and the need for the free flow of information in his career as a librarian.

Information Privacy

Privacy is a term with various meanings depending on the circumstance. The concept of privacy is complex because of the emotional aspects (Miller, 1971. p. 25). Privacy in early English language meant the state or condition of being withdrawn from the society of others, or from the public interest (Shattuck, 1977, p. xiii). Privacy involves one's relationship to society; in a world without others, privacy does not exist (Solove, 2008, p. 20). Privacy is intertwined with society as privacy would not be necessary without the existence of others (Strum, 1998, 7). Political scientist Rhoda Howard notes, “Without privacy, one cannot develop a sense of the human individual as an intrinsically valuable being, abstracted from his or her social role" (Strum, 1998, p. 5). Solove (2008) adds, “Privacy involves one’s relationship to society; in a world without others, claiming that one has privacy does not make much sense.”

Another definition of privacy, the right to control information about oneself, is in constant struggle with the efforts to preserve individual freedom and autonomy in an increasingly complex, technological and manipulative society (Shattuck, 1977, p. xiii, xv).

In legal parlance, privacy legislation is divided into four torts or civil wrongs as defined by legal scholar, William Prosser:

1. (Unwanted) Public disclosure of facts;
2. Intrusion into a person’s seclusion or private affairs;
3. Publicity that places a person in a false light in the public eye; and
4. The appropriation of a person’s name or likeness for commercial or other advantage.

(Sheenhan , 1998, p.9; Solove, 2008, pp. 58-61).

With disclosural privacy, there are limitations and exceptions to privacy expectations. Courts have specified zones of privacy that must not be crossed by the government. These are: marriage, procreation, contraception, family relationships, right of association; child rearing and child education (Bielefield & Cheeseman, 1994). The protections afforded by these zones do not prevent the inevitable interference into personal affairs by the government as the right to privacy is not absolute. Disclosure of information held by the government about its citizens frequently prevails over individual expectations of privacy when the interests of the government and individual interests conflict (Bielefield & Cheeseman, 1994).

The focus of this study is information privacy which is defined by Hendricks (1990) as the legal right of individuals to determine what information about them is to be communicated to others. Specifically examined is the awareness, concerns and information seeking behavior of persons relative to the use of their Social Security Number (SSN) within the many contexts in which a person's Social Security Number (SSN) is required or requested for identification or authentication. The paradox of the use of the SSN for identification is its efficiency in tracking individuals in public and private databases and the inherent conflict between information privacy and the surrender of private information for the receipt of public and private services and benefits (Shattuck, 1977; Strum, 1998). Commercial activities, social services, and overall involvement in society are somewhat at odds with the notion of privacy. Insurance, employment, welfare, medical treatment, credit, and legal matters all require the surrender of privacy to some degree (Shattuck, 1977; Security in Numbers: SSNs and ID Theft, 2008; *Safeguarding Social Security Numbers in Tennessee Government Records*, 2008).

Information Seeking and Privacy

Seeking information on legal requirements to disclose one's SSN can be intimidating and overwhelming. Not knowing where or to whom to turn to answer privacy questions can be paralyzing. Yet uncertainty is a requirement that initiates the process of information seeking (Kuhlthau, 1993b). When a person needs to make a decision or resolve an uncertainty, information is needed to fill a gap in understanding (Kuhlthau, 1993b). To answer a question, locate a fact, solve a problem or understand something, an information need must be resolved within context and cannot be separated from the situation or the individual who perceived the need (Chen, 1982, p. 9). Information is considered to be the principal commodity of our society and as such is the source of most of the conflict between social control and privacy (Shattuck, 1977; Solove, 2004; Solove, 2008). Information seeking is a conscious effort to acquire information in response to a need or gap in knowledge (Case, 2007, p.75). With information seeking to satisfy an information need, one may or may not be aware that the information exists. Information seeking differs from information awareness in that with the latter, one may be aware that the information exists but may not have a complete or in-depth understanding.

Information sharing pertains to the sharing of information amongst government agencies and commercial businesses and with each other (GAO-07-1023T, 2007; GAO-06-586T, 2006). The information science literature is lacking this area. One may argue that information science professionals are essentially charged with providing or sharing information. However, information technology has changed the manner in which practitioners perform their duties. Information professionals are now charged with maintaining confidentially of clients' electronically stored personal information (Kniffel, 2008). Information disclosure by individuals can be defined as the mandatory or voluntary providing of information to others. Like information sharing discussed above, information science literature does not explore the concept of information disclosure. Instead, much of the information science literature has focused on information seeking and information retrieval (Kuhlthau, 1993; Case, 2007; and Dervin, 1976).

Situations where an SSN many be required are many and often "on-the-spot" requests may leave a person feeling powerless with no other reaction but to comply. Chen notes, "*A free and open democratic society depends upon the ability of its citizens to make fully informed decisions about the choices that affect their lives. Access to information is power, and that in* *our democratic society people themselves want to decide how to use that powe*r" (1982, p.2).

The ability of a person to locate applicable privacy laws, understand the impact of those laws well enough to apply those same laws to common activities such as registering to vote, applying for a new job, or obtaining insurance will allow a person to act with the knowledge of both the advantages and consequences of sharing his or her personal information.

Government agencies which promulgate privacy information related to SSNs are the Federal Trade Commission, the General Accountability Office and the Social Security Administration. In the state of Tennessee, state laws which control the collection, storage and dissemination of SSNs are found in the state's official codebook, the Tennessee Code Annotated.

Prior research has found that library use primarily involves eight major categories: Consumer Issues; Education and Schooling; Employment—Getting/Changing Jobs; Health; Housing; Job-related: Organizational Relations; Job-Related: Technical; and Recreation and Culture. That study posits that libraries are perceived as useful for definite, recognized categories (Chen, 1982). Libraries are often intimidating and information searches are frequently ended before obtaining satisfactory results (Kuhlthau, 1993, Chen 1982). Looking for information in a traditional library can be intimidating (Case, 2007, p. 23). Information seeking of legal requirements to disclose one's SSN may necessitate the use of a law library simply because specialized legal databases such as Westlaw and LexisNexis are often too costly in public, academic or in a number of law libraries. These databases are potentially useful when searching for recent case law and current federal and state statutes. In some circumstances, laypersons with limited training to locate legal decisions and statutes require the assistance of a trained professional to locate pertinent information. Unfortunately, law libraries are not available in every community and when privacy information is found in those institutions, clarification is often needed for statutes that are not easily interpreted.

Lack of awareness may not be the only hurdle information seekers face when confronted with a request to provide their SSN to a public or private agency. Too much information may be as problematic as a dearth of information. Information technology has increased the number of search possibilities beyond the four walls of the traditional library setting. Web searches for SSN information can result in information overload. Recent searches for *social security number* or social *security number laws* on the search engine Google returned tens of millions results. See Appendix D, *Google Social Security Number Search Results*.

Avoidance of Information

Information behavior encompasses information seeking as well as the totality of other unintentional or passive behaviors (such as glimpsing or encountering information), in addition to purposive behaviors that do not involve seeking, such as actively *avoiding* information (Case, 2007, p. 5). Also noted is the phenomenon that increased knowledge does not always change behavior and informed behavior does not necessarily follow exposure to information (Case, 2007). An aspect of information seeking related to this study is that of avoidance behavior. There is a tendency to avoid exposure to information that causes anxiety or conflicts with prior knowledge, beliefs, and opinions (Case, 2002, p. 97).

One may avoid new and potentially upsetting information by choosing not to know or use information, much like a person who decides not to learn if they carry a gene for a specific illness or any other circumstances in which a person may feel powerless to challenge (Case, 2007). Laypersons may feel powerless in maneuvering through the morass of legal literature.

Individuals tend to acquire more information on a topic where there is personal interest. Instead of reducing the uncertainty that accompanies a lack of information, acquiring new information can sometimes heighten anxiety and increase uncertainty (Kuhlthau, 1993b, p. 109).

Online Privacy Information Sources

Online databases dedicated solely to providing access to information directly related to privacy may be more appropriate than popular search engines such as Google or the traditional library setting. Some examples of such websites are noted below:

Electronic Frontier Foundation (EFF) – In 1990, the EFF was founded to address the legal issues related to threats of government violation of the freedom of speech. More recently, EFF aims its sights on industry threats to privacy, consumer rights, freedom of speech and innovation in the electronic environment (http://www.eff.org).

Electronic Privacy Information Center (EPIC) – The prevalence of electronic retention of personal data on individuals has prompted the formation of online watchdog organizations such as EPIC, a Washington, D.C. public interest research center. Established in 1994, EPIC is a non-profit corporation which employs attorneys to scrutinize constitutional and civil liberties issues, legislation and lawsuits arising from challenges to the right to privacy, the First Amendment and the Freedom of Information. Staff attorneys monitor legislation that pertains to privacy. EPIC is funded by individuals, private foundations, publications and litigation awards (http://www.epic.org).

Privacy Rights Clearinghouse (PRC) is another credible online, nonprofit website that provides information on current laws and practices in the area of consumer protection. While EPIC is located in the midst of government regulatory agencies with legally trained advocates in

Washington D.C.; PRC, established in 1992, is based across the country in San Diego, California and provides practical information to consumers on how technology affects the privacy of personal information. Advocacy is a major component of their operation. PRC intercedes in disputes between consumers and business, acts as a liaison between journalists, consumers and policymakers at the local, state (mostly for the State of California which has some of the most progressive identity theft and privacy laws) and federal levels. PRC provides Fact Sheets, hotline assistance and plain language discussion of federal and state laws that pertain to privacy including Health Insurance Portability and Accountability Act (HIPAA), Fair and Accurate Credit Transactions Act (FACTA), Fair Credit Reporting Act (FCRA), and the Privacy Act of 1974. This resource is important for the study of information privacy for assistance to those consumers who are not legally trained or knowledgeable in the area of information privacy. Persons who are commanded to comply with laws compelling the disclosure of personal information are often without immediate recourse other than doing without government or consumer goods or services (http://www.privacyrights.org).

Gaps in the Existing Literature

There is significance of this study in the context of information science due to the gap in the research in information sharing of personal information. There has been much research into the areas of information seeking and information retrieval. Kuhlthau has authored several articles on information seeking including, *A Principal of Uncertainty for Information Seeking* and *Seeking Meaning: A Process Approach to Library and Information Services.* Her Information Search Process (ISP) model outlines six stages from the library user's perspective during information seeking: Initiation, Selection, Exploration, Formulation, Collection and

Presentation. Kuhlthau emphasizes that the process is not a linear one. Uncertainty ebbs and flows throughout the search process, eventually culminating in an end with a sense of relief if the research is deemed successful or disappointment if the outcome falls short of expectations (Kuhlthau, 1993, p. 343).

Dervin's 10 Dubious Assumptions about Information and Information Seeking, noted in *Looking for information* by Donald Case and listed in Appendix E of this study, show the divide that exists between those who seek information and the fulfillment of an information need. Particularly relevant to this SSN privacy study are assumptions 2, 6, 9 and 10.

- Assumption 2 - *More information is always better*.   Information privacy data abounds on popular search engines but that plethora of information may be useless because it lacks relevance to a particular information privacy need.
- Assumption 6 - *Every need situation has a solution*. Legal requirements to provide an SSN may not be clear as technology typically moves at a faster pace than legislation (Miller, 1971). The United States judicial system requires individuals to initiate a lawsuit if a constitutional or legal right is perceived to be denied (Solove, 2008). Costly litigation may be prohibitive to many.
- Assumption 9, *Time and space – individual situations – can be ignored in addressing information seeking and use*: Privacy law related to SSNs affects virtually every United States citizen individually and collectively.
- Assumption 10, *People make easy, conflict-free connections between external information and their internal reality*: In this study, the survey was designed to determine if intimidation (or avoidance of conflict) is a factor in deciding whether

to provide an SSN to a private or public agency.

See Appendix E, *Dervin's 10 Dubious Assumptions about Information and Information Seeking*.

Kuhlthau, Case and Dervin have all conducted research in the area of information seeking (the process of searching for information to fill a knowledge gap) or information retrieval (effectively retrieving desired information) but there has been no known research in information sharing of sensitive personal information by individuals. In the area of information sharing, the context has primarily revolved around businesses sharing personal information with other businesses about individuals often without knowledge or express consent of the individuals through third party (Solove, 2008).

Chapter 3: Research Methods

This chapter presents the research methods used to collect and analyze the data derived from the survey instrument designed specifically for this descriptive research study. The self-administered multiple-choice and short-answer questionnaire (Appendix F, *Survey Instrument*) was available via the web or on paper. Participation of respondents was voluntary and all participants were adults. Snowball sampling was used for gaining online participants who were encouraged to recommend others to participate. Convenience sampling was used for the paper copy of the survey. Requesting respondents to refer the questionnaire to others interested in the topic is an effective method of administering a survey to a larger sample of the population (Sue & Ritter, 2007).

Population and sample

This study specifically examines the SSN laws based on responses primarily from the citizens of Tennessee and from some members of the United States population outside of Tennessee. While most U.S. citizens are affected by information privacy and security, this study focused on people in Tennessee or referred by a Tennessee connection. Convenience and snowball sampling techniques were used to reach participants.

Convenience sample participation was open to adults age 18 and older. A sample size of 184 respondents was achieved using convenience and snowball sampling. Nine respondents (4.9%) ended the survey without entering any demographic data but those responses were included in the survey results to allow respondents who were most concerned with their privacy the chance to participate in the study. Ninety-one of the completed surveys (49.4%) were from students in an upper-division undergraduate class at the University of Tennessee. The majority of the respondents were from the state of Tennessee (71.7%) with 28.3% of the completed surveys from residents of states other than Tennessee including Arizona, Arkansas, Colorado, Delaware, Georgia, Idaho, Maryland, Michigan, New York, North Carolina, Ohio, Oklahoma, Oregon, Texas, Utah, Virginia, Washington, and the District of Columbia.

The sample was recruited using two strategies: one by invitation to participate with a link posted on electronic mailing lists of the researcher's personal Facebook account, the University of Tennessee School of Information Sciences, and the Special Libraries Association, District of Columbia Chapter. The other strategy was a convenience sample from undergraduate journalism students in one upper-division class who were administered a paper copy of the survey.

Instrumentation

The data collection instrument was comprised of 22 multiple-response and short-answer questions including demographic information with Likert scale agreement statements on federal and Tennessee state privacy laws that govern collection, handling and retention of SSNs; information seeking behaviors; and concerns regarding disclosure. The questions were formulated from contextualizing situations from the many federal and Tennessee state SSN laws discussed in the literature review.

Participants answered survey questions by either selecting provided choices or entering text for open-ended questions when indicated. The survey instrument queried awareness, concerns and information seeking behavior using three, four and five-point Likert and Likely measurement scales along with *Yes* or *No* questions (see Appendix G, *Research Variables*). Four open-ended questions in the survey (11, 15, 21 and 22) allowed participants to respond in their own words: one each for listing additional sources of privacy information and reasons for not wanting to disclose the SSN not already listed in the survey; one for listing area of study and the other for offering any general comments. The survey questions related solely to Tennessee laws were a relatively small percentage of the survey (10%), and were only asked of Tennessee residents.

Procedure and Data Analysis

The survey was released in the fall of 2009 for approximately three weeks. The convenience and snowball sample of respondents accessed the survey either through a paper copy of the survey distributed to voluntary participants in an undergraduate journalism class or through electronic mailing lists

The data were collected and analyzed with the PASW Statistics 18.0 (also known as SPSS) statistical software program. Demographic information of respondents was limited to age, gender, state of residence, highest level of education achieved and career field or education focus. This demographic information was collected and used only to compile statistics. The survey did not require any identifying information as it was designed to be anonymous. The only potentially personally identifiable information gathered was that of email addresses for those respondents who chose to enter into the drawing for an incentive for a gift card in the amount of $50. Email information was collected and kept separate from the survey results.

Limitations

This exploratory study does not examine causal relationships to determine whether the widespread use of SSNs contributes to the threat or occurrence of identity theft. Exploration of the causes of identity theft is beyond the scope of this study.

This study does not determine the best sources of privacy laws. Instead, results of the study can be used to alert librarians and other information professionals of the need to develop a program for privacy literacy.

This study does not explore what legal recourse a person has against a government or private agency that refuses to provide goods or services for failure to disclose one's SSN. A disclaimer of legal representation is often given to individuals who seek legal information from individuals who are not practicing attorneys.

This study does not explore people's perceptions of privacy laws, only their awareness that such laws exists. Future research can further seek to determine if there is an understanding of privacy laws in various situations.

There are drawbacks to administering an online survey:

- Access to the survey is limited to those who can access the link. Feedback during the time period of the administration of the survey included complaints that the survey was inaccessible. The hyperlink to access the survey was sometimes broken due to University of Tennessee online security measures.
- Lack of visual verification in an anonymous online distribution can be problematic in that the person who submits answers is assumed to be who he or she purports to be. Consequently, results may skewed by intentional

dishonesty or inaccurate answers (Sue & Ritter, 2007). To avoid multiple submissions, respondents were instructed to submit the survey only once.

- Individuals who choose to participate in an online survey may have a particular interest in the topic and may not be representative of the underlying population (Sue & Ritter, 2007, p. 32)

Other limitations are:

- The distribution of the survey in this study was limited due to time constraints and the narrow segment of the population targeted by the online email postings and university classroom.
- This study covers only selected SSN laws at the state level in the state of Tennessee. However, a separate study could be conducted to ascertain awareness, concerns, and information seeking behavior in other states.

Chapter 4: Analysis of Data

This chapter presents the results of the data collected from the quantitative survey instrument administered both online and during a class period of an undergraduate course. Twenty-eight percent (28%) of the completed surveys were from residents of states other than Tennessee. Approximately half (49.4%) of the completed surveys were from students in the undergraduate class. Overall, one-hundred ninety six people started the survey. Twelve people (6.1%) abandoned the survey without sufficient data to analyze. A sample size of 184 respondents was achieved with 175 respondents completing the entire survey Nine respondents (4.8%) finished the survey without entering complete demographic data. These nine incomplete surveys were included in the survey results because exclusion would deny respondents who were most concerned with their privacy the right to be heard.

This chapter is organized into the following sections:

1. Demographic characteristics of respondents
2. Awareness level of SSN laws subdivided by demographics
3. Concerns pertaining to disclosure subdivided by demographics
4. Information seeking behavior and preferences of respondents
5. Survey results for Tennessee respondents

Table 1 lists the survey variables and the item number of the survey questions referenced throughout this chapter.

Table 1: Survey Variables

Research Variable	Survey Variable Name and Item Number
Awareness. Awareness of federal and state of Tennessee privacy laws pertaining to the Social Security Number (SSN).	SSN (2), TN (2.A), RECORDS (2.B), FEDERAL (3), CIRCUMST1 (4), INSURANCE (5)
Concern. Concern pertaining to the disclosure of one's SSN.	IDENTITY (6), PROTECT (7), CIRCUMST2 (8), ANY_CONCERN (13), RANK_CONCERN (14), OTHER_CONCERN (15), CONCERN (16)
Information Seeking. Sources used to find information on laws pertaining to the disclosure of the Social Security Numbers.	FIND_INFO (9), SOURCES (10), OTHER_SOURCES (11), SEARCHING (12)
Demographic Data. This information is descriptive of the participants in the study.	STATE (1), GENDER (17), AGE (18), EDUCATION (19), CAREER3 (20), STUDY (21)
Comments. Additional comments are solicited for further illumination and opinions regarding survey.	COMMENTS (22)

1. Survey Demographics

1.1 Gender

The majority of the respondents were female (72.3%). Fewer than five percent (4.9%) of respondents revealed no demographic data. Males comprised the remainder of the respondents (22.8%) as reported in Table 2.

Table 2 : Gender

N=184		Frequency	Percent
Completed Surveys	Male	42	22.8
	Female	133	72.3
	Total	175	95.1
Missing Demographics*		9	4.9
Total		184	100.0

*Surveys with incomplete demographics were included in results.

1.2 Age

The age of the respondents ranged from 20s to 70s. The mean age was 29; the median age was 23. More than half (55.5%) of the respondents were in their early 20s (age 20-25) with the majority of those consisting of students from an on-campus, upper-division journalism class.

1.3 Education

The survey allowed respondents to categorize their educational achievement with a large majority (44.6%) listing their highest level of educational achievement as *Some college*. Table 3 presents those results, which are indicative of the sampling of classroom students. Education was collapsed into the groups of *Some college*; *Bachelors*; and *Masters or higher* for statistical comparisons as some of the education sample groups were too small to analyze separately. Respondents who identified themselves as students were included in the student category, whether these students were on-campus in the class that was surveyed or members of the group of online participants.

Table 3: Education

		Frequency	Percent
Completed Surveys			
	High School or GED	2	1.1
	Some College	82	44.6
	Two-year Certificate or Technical Degree	4	2.2
	Bachelor's Degree	48	26.1
	Master's Degree	37	20.1
	Doctorate or other Professional Degree	2	1.1
	Total	175	95.1
Missing Demographics *		9	4.9
Total		184	100.0

*Surveys with incomplete demographics were included in results.

1.4 State

Persons identifying themselves as residents of the state of Tennessee comprised the majority of respondents at 71.7%. In addition to the state of Tennessee, 28.3% of respondents in eighteen other states and the District of Columbia were represented in the study.

Survey Variables

2. Awareness of SSN Laws

In all awareness questions, the values of *strongly agree, agree, disagree, strongly disagree*, *yes* or *no* are different depending on whether a survey statement is true or false as indicated in Table 4.

Table 4: SSN Awareness Answer Grid

Relationship for Awareness Statements in Survey				
Answer Options	**If Statement is True**		**If Statement is False**	
Strongly Agree	X		X	
Agree	X		X	
Disagree		X		X
Strongly Disagree		X		X
Don't know / Not sure		X	X	
Yes	X		X	
No		X		X
	Respondent is Aware	**Respondent is Unaware**	**Respondent is Unaware**	**Respondent is Aware**

- If a respondent answered *strongly agree, agree* or *yes* to a true statement, then that response indicated awareness.
- If a respondent answered *strongly agree, agree* or *yes* to a false statement, then that response indicated respondents were unaware or uninformed.
- If a respondent answered *strongly disagree, disagree* or *no* to a true statement, then that response indicated respondents were unaware or uninformed.
- If a respondent answered *strongly disagree, disagree* or *no* to a false statement, then that response indicated awareness.
- If respondents answered a question with *don't know* or *not sure*, then those responses also indicated unawareness.

2.1 SSN (Social Security Number) - Awareness of Legal Requirements to Provide SSN

The first substantive inquiry of knowledge of the existence of SSN laws began with survey question 2 as reported in Table 5. This set of questions asked respondents to *agree* or *disagree* with statements on the use of the SSN in four scenarios:

A. Ability to get a new SSN if used by another

B. Whether utility companies can charge a deposit in lieu of an SSN

C. Federal law requirements on use of the SSN in financial institutions

D. The Patriot Act legal requirements to provide the SSN to obtain internet service

Table 5: Awareness of legal requirements to use SSN (Item 2.1)

	Unaware		Aware		Correct Answer*
N=184	Count	Percent	Count	Percent	
A. 'If my Social Security Number (SSN) is used by another person without my consent, I can obtain another SSN.'	152	82.6%	32	17.4%	True
B. 'Utility companies (electricity, sewer, water, gas, etc.) can charge a deposit fee if I refuse to provide my SSN.'	158	85.9%	26	14.1%	True
C. 'For consumer transactions, federal law requires consumer identity authentication (proof of identity) only in the financial sector (banks, credit unions, investment firms, etc.)'	99	53.8%	85	46.2%	True
D. The USA PATRIOT Act requires that I provide my SSN to obtain internet service.	86	46.7%	98	53.3%	False

*For example, statement A is true. Respondents indicated awareness at a rate of 17.4% and unawareness at a rate of 82.6%.

To determine awareness in this set of SSN law questions, survey respondents were asked if they agreed or disagreed with statements A, B, C, and D. These four statements have been shown in the literature to be either true or false. Statements A, B, and C are true; statement D is false. When respondents correctly answered a true statement (A, B, or C) with either s*trongly agree* or a*gree,* that response indicated awareness. If respondents answered with *disagree, strongly disagree* or d*on't know,* then that response indicated unawareness. A response of *disagree, strongly disagree* to statement D indicated awareness; whereas a response of s*trongly agree,* a*gree* or d*on't know* to statement D indicated unawareness.

EXPLANATION:

A – The correct answer to the statement on obtaining a new SSN in case of unauthorized use by another is true. The Social Security allows issuance of a new SSN with proof of criminal use of one's SSN. Respondents were only 17.4% of the aware of this policy.

B – The statement on whether utility companies may charge a deposit in lieu of providing an SSN is true. There is no law at the federal or state level that requires disclosure of an SSN to obtain utility service. Respondents were only 14.1% aware that utility companies will accept a deposit if a person refuses to disclose their SSN.

C – This statement is true. With the Interest and Dividend Tax Compliance Act of 1983, the federal government requires consumer disclosure of SSNs only for financial transactions with institutions such as banks, credit unions, and investment firms. Respondents were 46.7% aware of this legal requirement.

D – The statement on the Patriot Act requirement to disclose one's SSN to obtain Internet service is untrue. There is no language in the Patriot Act that requires United States citizens to provide their SSN for Internet service or for any other purpose. Survey results show that respondents were 53.3% aware that the Patriot Act has no provision for disclosure of an SSN to obtain Internet service.

2.2 FEDERAL - Awareness of Federal SSN Laws

This set of questions on Federal SSN laws in survey question 3, reported in Table 6, asked respondents to indicate their belief in the legitimacy of the statements pertaining to the SSN in the following scenarios:

A. Federal law authorization for free yearly credit reports
B. Required notification of privacy policy for customers of financial institutions
C. Patriot Act requirement to disclose SSN to obtain lottery winnings
D. Legal authority of federal agencies to refuse services for refusal to disclose SSN
E. Legal authority of retail businesses to refuse goods or services if customer declines to provide SSN

Table 6: Awareness of Federal SSN Laws (Item 2.2)

	Unaware		Aware		Correct
	Count	Percent	Count	Percent	Answer*
A. 'By federal law, yearly credit reports are available free of charge to everyone with a SSN.'	62	33.7%	122	66.3%	True
B. Notification of privacy policy must be given in writing to all customers of financial institutions.	48	26.1%	136	73.9%	True
C. The USA PATRIOT Act requires that I provide my SSN to obtain lottery winnings.	167	90.8%	17	9.2%	Never True
D. Federal government agencies can legally refuse to grant services if I refuse to provide my SSN.	90	48.9%	94	51.1%	True**
E. Retail businesses can legally refuse goods or services if I decline to provide my SSN.	157	85.3%	27	14.7%	True

*For example, statement A is true. Respondents indicated awareness at a rate of 66.3% and unawareness at a rate of 33.7 %.
**Federal government agencies may be authorized to deny services in circumstances where the SSN was required prior to the enactment of the 1974 Privacy Act or if the request does not violate any other federal or state law.

To determine awareness of Federal SSN laws, survey respondents were asked if they believed statements A, B, C, D and E were *always true, sometimes true*, or *never true*. Respondents could also answer that they were not sure. These five statements have been shown in the literature to be *always true*, *sometimes true* or *never true*. Statements A, B, and E are true. Statement D is sometimes true and statement C is never true. When respondents correctly answered statements A, B, D, or E with either *always true* or *sometimes true,* those responses indicated awareness. If respondents answered those four statements with *never true,* or *not sure,* then those responses indicated unawareness. A response of *never true* to statement C indicated awareness. A response to statement C of *always true*, sometimes *true,* or *not sure* indicated unawareness.

EXPLANATION:

A - Respondents were 66.3% aware of the availability of a free report which is permitted by FACTA, The Fair and Accurate Credit Transactions Act.

B - The federal law, Gramm-Leach-Bliley Act (GLBA), requires financial institutions to provide customers with written notice of the institution's policy for addressing privacy issues upon establishment of an account and on a yearly basis thereafter. Respondents were 73.9% aware.

C - Respondents were 9.2% aware that there is no legal requirement in the Patriot Act to disclose one's SSN to obtain lottery winnings.

D - Federal agencies can sometimes legally refuse services for failure to disclose one's SSN, respondents were 51.1% aware. Federal agencies have the authority to decline services for failure to provide an SSN in circumstances where the SSN was required prior to the enactment of the 1974 Privacy Act and if the request does not violate any other federal or state law.

E - Respondents were 14.7% aware that retail businesses can legally refuse goods or services for refusal to provide an SSN as there is no law prohibiting denial of services for failure to provide an SSN.

2.3 CIRCUMST1 – Awareness of legal requirements to disclose SSN in certain circumstances

In survey question 4 as reported in Table 7, respondents were asked, "*In each of these circumstances, are you required to disclose your SSN*?"

A. Applying for a library card

B. Establishing a bank account

C. Applying for credit

D. Receiving medical or dental services at a private office

Table 7: Awareness of disclosure SSN in hypothetical circumstances (Item 2.3)

	Unaware		Aware		Correct Answer*
	Count	Percent	Count	Percent	
A. Applying for a library card	56	30.4%	128	69.6%	Not required
B. Establishing a bank account	18	9.8%	166	90.2%	Required
C. Applying for credit	182	98.9%	2	1.1%	Not required
D. Receiving medical or dental services at a private office	153	83.2%	31	16.8%	Not required

*For example, providing an SSN to obtain a library card is not required by federal or state law. Respondents indicated awareness at a rate of 69.6% and unawareness at a rate of 30.4%.

To determine awareness of requirements to disclose their SSN in hypothetical circumstances, respondents were asked of requirements to disclose their SSN. The four statements listed in Table 7, are shown by the literature to be either true or false. The only circumstance of the four statements listed in Table 7 in which the SSN is required by law is when establishing a bank account, statement B. The other three circumstances (A, C, and D) do not require disclosure of an SSN. When respondents correctly answered statement B with a response of *always true* or *sometimes true*, that response indicated awareness. A response to statement B of *never true*, or *not sure* indicated unawareness. If respondents answered statements A, C, or D, with the choice of *never true* then that response indicated awareness. A response to statements A, C, or D, with always true, *sometimes true*, or *not sure* indicated unawareness.

EXPLANATION:

A – There is no federal or Tennessee state law that requires disclosure of an SSN to obtain a library card. Respondents indicated awareness by answering that an SSN is not required at 69.6%.

B – Federal law (as in Item 2.1(C) above) requires disclosing the SSN to establish a bank account. Respondents indicated awareness at 90.2% by agreeing that establishing a bank account requires disclosure of an SSN.

C – There is no federal or Tennessee law that requires individuals to disclose their SSN to obtain credit, yet respondents overwhelmingly indicated unawareness at 98.9%.

D – There is no federal or Tennessee law that requires disclosure of an SSN to receive medical or dental services at a private office. Respondents indicated unawareness of a requirement to disclose their SSN to receive medical or dental services at a private office at 83.2%.

Originally, there were awareness questions asked in the survey on requirements to disclose one's SSN to obtain health care at a public health agency, but on further examination, it was decided to exclude those questions in survey results because the instances where SSNs may be legally required within public agencies may vary. Those questions were excluded to avoid ambiguous results. Also excluded from survey results are survey questions on requirements to disclose the SSN to public health insurance agencies. This is an area for future research.

2.4 INSURANCE – Awareness of legal requirements to disclose SSN to obtain insurance

In survey question 5, reported in Table 8, respondents were asked about federal law requirements to disclose their SSN to obtain several types of insurance:

A. Life Insurance
B. Automobile Insurance
C. Home or Renter's Insurance
D. Business Insurance

Table 8: Awareness of SSN laws and Insurance (Item 2.4)

	Unaware		Aware		Correct Answer*
	Count	Percent	Count	Percent	
A. Life Insurance	179	97.3%	5	2.7%	Not required
B. Automobile Insurance	167	90.8%	17	9.2%	Not required
C. Home or Renter's Insurance	167	90.8%	17	9.2%	Not required
D. Business Insurance	173	94.0%	11	6.0%	Not required

*There are no federal laws that require disclosure of an SSN to obtain insurance from private insurance companies; however, beyond the scope of this survey question, the Internal Revenue Service may require insurance companies to obtain an SSN for income tax purposes only.

To determine awareness of SSN laws and insurance, survey respondents were asked if they believed federal law requires the disclosure of the SSN to obtain several types of insurance. As shown in Table 8, federal law does not require disclosure of the SSN to obtain life, automobile, home and renter's or business insurance. When respondents correctly answered statements A, B, C or D with *never true*, those responses indicated awareness. If respondents answered those four statements with *always true*, *sometimes true*, or *not sure*, those responses indicated unawareness.

EXPLANATION:

There are no federal laws that require disclosure of an SSN to obtain the types of insurance listed in Table 8. Respondents overwhelmingly indicated unawareness: life insurance (97.3%); automobile insurance (90.8%); home or renter's insurance (90.8%) and business insurance (94.0%).

2.5 OVERALL AWARENESS – Overall Awareness of legal requirements to disclose SSN To get a measure of overall awareness, the percentage of items from the four survey variables noted above were averaged to obtain an awareness score as shown in Table 9.

Table 9: Overall Awareness of SSN laws (Item 2.5)

	N	Minimum	Maximum	Mean	Std. Deviation
Awareness	184	5.88	76.47	32.4169	13.16037
Total	184				

Respondents' awareness levels ranged from a low of 5.9% to a high of 76.5%. As presented in Table 9, the mean awareness shows that respondents were aware 32.4% of the items queried.

Gender. There were no significant differences in awareness when the responses were analyzed by gender. To determine if awareness differed by gender, a t-test was run. The results of the t-test were t=.722, df=173, p=.471.

Students and Non-students (*Significant results)*. A t-test was run to determine if awareness differed by students and non-students. The results were: t=-2.143, df=173, p=.034 which indicate a significant difference between students and non-students. Non-students are significantly more aware than students of the SSN laws examined in this study. The average awareness for students was 31.14%. For non-students, the average awareness of SSN laws was 35.37%.

Education. There was no significant difference in awareness relative to education. To test if awareness differed by education, an ANOVA was run. The results were: F(2,172)=2.531, p=.083. Because p-value is greater than .05 there are no significant differences. Respondents who achieved a higher level of education did not show a higher level of awareness of SSN laws.

Age (*Significant results)*. To test if awareness was related to age, a correlation was run. The results were a correlation coefficient of .282 (p<.001), which is significant. As age increases, awareness also tends to increase.

3. Concerns Pertaining to the Uses of the SSN for Identification

There were a total of seven *concern* questions in the survey. Respondents' concerns pertaining to disclosure of their SSN were queried in survey questions 6, 7 and 8. Respondents answered questions of likeliness to feel concerns related to use of their SSN. Types of concerns investigated in this study were the threat of identity theft in survey question 6; agency protection of SSNs in survey question 7; and disclosure of the SSN to service providers in certain public and private agencies in survey question 8.

- Survey question 13 asked respondents if they have any concerns with the use of their SSN.
- Survey question 14 asked respondents to indicate their level of concern in three areas: identity theft, denial of services for refusal to provide SSN and belief of a violation of privacy with requests from public agencies and private businesses for their SSN.
- Survey question 15 asked respondents to specify their own personal concerns not otherwise listed in the survey.
- Survey question 16 asked, *Overall, how would you rate your concern over your disclosure of your SSN?* Respondents provided a self-assessment of their concern level with options ranging from *no concern* to *extreme concern*. Overall concern was measured on a five point scale of 1= no concern; 2=very unlikely (slight); 3=unlikely (average); 4=likely (moderate); and 5=very likely (extreme).

3.1 IDENTITY – Concerns with threat of identity theft from the use of the SSN

In survey question 6, respondents were asked, *How likely are you to feel threatened by identity theft if you disclose your SSN in each of the following activities?*

A. Online transactions
B. Schools
C. Health care offices
D. Financial institutions
E. Government offices

Respondents were more likely to feel concern with the use of the SSN in online transactions (Mean=3.36) and less likely to the threat of identity theft with the disclosure of their SSN to government offices (Mean=2.17), as shown in Table 10.

Table 10: Concerns with threat of identity theft (Item 3.1)

	N	Minimum	Maximum	Mean	Std. Deviation	
A. Online transactions	178	1	4	3.36	.763	↑ More concern
B. Schools	175	1	4	2.39	.726	
C. Health care offices	176	1	4	2.32	.750	Less concern
D. Financial institutions (banks, credit unions, investment firms, etc.)'	178	1	4	2.24	.825	↓
E. Government offices	175	1	4	2.17	.781	

Gender (*Significant results*). To determine differences in concern of identity theft by gender, a MANOVA test was conducted. This test found a significant difference, $F(5, 157)=2.790$, $p=.019$. Individual ANOVAs were used to determine in which activity (*online transactions, schools, health care offices, financial institutions, and government offices*) the concern of the threat identity theft differed by gender. The results show the only significant difference with concern of identity theft is related to gender. Females who are more likely to be concerned with identity theft ($p= 3.44$) than are males ($p=3.05$) when making online transactions.

Education. The concern of identity theft does not differ by education. To make that determination, a MANOVA test was conducted. This test found no significant difference, $F(10, 312)=.866$, $p=.566$. Concern of the threat of identity theft does not differ by level of education achieved, i.e., respondents who have attained a master's degree do not feel any differently about the threat of identity theft than someone with less education.

Students and Non-students. The concern of identity theft does not differ between students and non-students. A MANOVA test was conducted to determine any differences in concern of identity theft between students and non-students, resulting in a finding of $F(5, 157)=1.179$, $p=.133$.

Age *(Significant results)*. Concern of the threat of identity theft does differ when the age of the respondent is correlated to the activities listed in survey question 6, "*How likely are you to feel threatened by identity theft if you disclose your SSN in each of the following activities*?" Schools were the only category with a significant relationship. A Pearson correlation of .159 indicates that as age increases, the sense of the threat of identity theft also increases when the SSN is disclosed to schools, as reported in Table 11.

Table 11: Identity Theft Age Correlation (Item 3.1 Age)

	Pearson Correlation	P-value
Online transactions	-.128	.094
Health care offices	.141	.068
Schools	.159	.039*
'Financial institutions (banks, credit unions, investment firms, etc.)'	-.044	.568
Government offices	.059	.444

*A Pearson correlation shows a significant relationship in schools category.

3.2 PROTECT – Concerns related to agency protection of SSN

In survey question 7, respondents answered questions on the likeliness of particular types of organizations noted below to protect their SSN:

A. Retail stores

B. Utility companies

C. Cell phone companies

D. Financial institutions

E. Government agencies

Respondents were asked, "*For each of these types or organizations, how likely is each organization to protect your SSN?*" The results show in Table 12 that for a mean of 2.5 and above, respondents believe organizations are more likely to protect their SSN, and conversely, a mean below 2.5 indicates a belief that those organizations are less likely to offer protection.

Table 12: Concern of Agency Protection of SSN (Item 3.2)

	N	Minimum	Maximum	Mean	Std. Deviation	
'Financial institutions (banks, credit unions, investment firms, etc.)'	176	1	4	3.26	.746	↑
Government agencies	177	1	4	3.22	.792	
'Utility companies (electricity, sewer, water, gas, etc.)'	175	1	4	2.69	.702	Believe organizations will protect
Cell phone companies	168	1	4	2.46	.741	Believe organizations will not protect
Retail stores	173	1	4	2.06	.822	↓

Table 12 shows respondents' mean perception of protection of SSN by government and private agencies. Results show that respondents believe financial institutions (Mean=3.26) and government agencies (Mean=3.22) are more likely to protect their SSN while cell phone companies (Mean=2.46) and retail stores (Mean=2.06) are less likely. Utility companies fall slightly higher than mid-range of these extremes on the four-point measurement scale (Mean=2.69).

Gender. The concern of protection of SSN by organizations does not differ by gender. A MANOVA test found no significant difference by gender, F(5, 151)=.179, p=.970.

Education. The concern of protection of SSN by organizations does not differ by education. A MANOVA test found no significant difference by education, F(10, 300)=.1.572, p=.114.

Students and Non-students. The concern of protection of SSN by organizations does not differ between students and non-students. A MANOVA test found no significant difference between students and non-students, F(5, 151)=.1.038, p=.397.

Age (*Significant results*). Concern of the threat of identity theft differs by age only with protection of SSNs by cell phone companies. Correlations were run to determine if a relationship exists between age and concern of protection offered by *retail stores*, *utility companies*, *cell phone companies*, *financial institutions* and *government agencies*. A Pearson correlation of -.166 and a p-value of .036 indicates that as age increases, the concern that cell phone companies are less likely to protect SSNs increases; this finding shows a significant difference as reported in Table 13.

Table 13: Concern - Agency Protection and Age Correlation (Item 3.2 Age)

	Pearson Correlation	Sig. (2-tailed)
Retail stores	-.045	.565
'Utility companies (electricity, sewer, water, gas, etc.)'	-.110	.156
Cell phone companies	-.166	.036*
'Financial institutions (banks, credit unions, investment firms, etc.)'	-.076	.329
Government agencies	-.087	.262

*Correlation is significant at the 0.05 level (2-tailed).

3.3 CIRCUMST2 – Concerns pertaining to disclosure of SSN in certain circumstances

In survey question 8, respondents were asked, "*In each of the following circumstances, how likely would you be to provide your SSN if asked by the service provider*?" Respondents indicated likeliness to provide their SSN in these particular circumstances:

A. Establishing a bank account
B. Applying for credit
C. Receiving medical or dental services at a private office
D. Receiving medical or dental services at a public agency
E. Applying for a library card

As shown in Table 14, for a mean of 2.5 and above, respondents are more likely to provide their SSN. For a mean below 2.5, respondents are less likely to provide their SSN to receive services. Respondents are very likely to provide their SSN when establishing a bank account (Mean=3.39) and applying for credit but unlikely to provide their SSN when applying for a library card (Mean=1.80). Slightly higher than mid-range on the four-point measurement scale are receiving services at a private medical office (Mean=2.91) and receiving medical services at a public agency (Mean=2.90).

Table 14: Concern related to disclosure of SSN in certain circumstances (Item 3.3)

	N	Minimum	Maximum	Mean	Std. Deviation	
A. Establishing a bank account	178	2	4	3.39	.585	↑
B. Applying for credit	177	1	4	3.38	.639	
C. Receiving medical or dental services at a private office	176	1	4	2.91	.883	Believe organizations will protect
D. Receiving medical or dental services at a public agency	167	1	4	2.90	.833	
E. Applying for a library card	178	1	4	1.80	.853	Believe organizations will not protect ↓

Gender. The likeliness to provide one's SSN does not differ by gender. A MANOVA test found no significant difference by gender, $F(5, 152)=.690$, $p=.632$.

Education. The likeliness to provide one's SSN does not differ by education. A MANOVA test found no significant difference by education, $F(10, 302)=1.233$, $p=.269$.

Students and Non-students (*Significant results*). Concern of protection of SSNs by organizations differs significantly between students and non-students as reported in Table 15. A MANOVA test found a significant difference in the likeliness to provide one's SSN between students and non-students, $F(5, 152)=3.837$, $p=.003$.

Table 15: Concerns pertaining to circumstances – Students / Non-students (Item 3.3 Student)

	Mean	
	Non-student	Student
Applying for credit	3.523	3.258
Receiving medical or dental services at a private office	2.723	3.075

To further analyze the data derived from these MANOVA tests, individual ANOVAs were run to determine in which circumstances likeliness to provide the SSN differed. Results indicate differences occur *when applying for credit* (p=.011) and *receiving medical or dental services at a private office* (p=.011). As reported in Table 15, non-students are more likely than students to provide their SSN when applying for credit, whereas students are more likely than non-students to provide their SSN when receiving medical services at a private office.

Age (*Significant results*). Age is correlated only with receiving medical or dental services at a private medical office. Pearson correlation of -.208 and a p-value of .006 indicate that older respondents are *less likely* to provide their SSN when receiving medical or dental services at a private office, as reported in Table 16.

Table 16: Concern pertaining to circumstances - Age Correlation (Item 3.3 Age)

	Pearson Correlation	Sig. (2-tailed)
Applying for a library card	.050	.516
Establishing a bank account	.039	.610
Applying for credit	.080	.299
Receiving medical or dental services at a private office	-.208	.006**
Receiving medical or dental services at a public agency	-.059	.459

**Correlation is significant at the 0.01 level (2-tailed).

3.4 ANY CONCERN – Respondents indicate concerns about using their SSN

In survey question 13, respondents were asked*: Do you have any concerns about disclosing your SSN*? Overall, 86.4% of respondents had concerns while 9.2% had no concerns as reported in Table 17. There were no demographic comparisons made due to the small number of respondents who asserted that they had no concerns.

Table 17: Any Concern (Item 3.4)

		Frequency	Percent
Do you have any concerns about disclosing your SSN?			
Valid	Yes	159	86.4
	No	17	9.2
	Total	176	95.7
Missing Demographics*		8	4.3
Total		184	100.0

*Surveys with incomplete demographics were included in results.

3.5 RANK CONCERN – Respondents indicate their level of concern

For survey question 14, *Which of the following concerns do you have about disclosing your SSN*? In this section, respondents were asked to indicate their level of concern relative to disclosure of their SSN as *Slight* (1), *Moderate* (2), or *High* (3) in three categories:

- Threat of identity theft
- Denial of services
- Violation of right to privacy

On the three-point scale, respondents show a slight concern (1.59) in the category of *Denial of Services* if there is a refusal to disclose their SSN. There is a moderate degree of concern (2.19) in the category of *Violation of Privacy* and a moderate-to-high degree of concern (2.49) of the threat of identity theft, as reported in Table 18.

Table 18: Concerns - Respondent Level of Concern with SSN Use (Item 3.5)

	N	Minimum	Maximum	Mean	Std. Deviation
Threat of identity theft	159	1	3	2.49	.692
Violation of my right to privacy	159	1	3	2.19	.773
Denial of services if I refuse to disclose my SSN	159	1	3	1.59	.722

The survey results show no correlation between any demographic (gender, education, students/non-students or age) to types of concern.

Gender. A MANOVA test determined no significant difference in types of concern by gender, $F(3, 154)=1.811$, $p=.147$.

Education. A MANOVA test determined no significant difference in types of concern by education, $F(6, 306)=.798$, $p=.572$.

Students and Non-students. A MANOVA test determined no significant difference in types of concern between students and non-students, $F(3, 154)=1.034$, $p=.379$.

Age. A Pearson correlation test found no significant correlation between types of concern and age.

3.6 CONCERN – Respondents classify their overall level of concern

In survey question 16, respondents were asked to classify their overall concern of SSN disclosure, *Overall, how would you rate your concern over your disclosure of your SSN*? This section was designed to determine if respondents' self-assessment of their level of concern differed with their demographics. The concern categories are as follows:

1. No Concern
2. Slight Concern
3. Average Concern
4. Moderate Concern
5. Extreme Concern

As reported in Table 19, the overall mean was 3.58, which indicates respondents show an overall concern in the Average to Moderate concern range. A t-test was run to determine if there was a difference in any demographic and overall concern. Overall concern did not differ by any demographic.

Table 19: Overall Concern (Item 3.6)

	N	Minimum	Maximum	Mean	Std. Deviation
Overall, how would you rate your concern over your disclosure of your SSN?	176	1	5	3.58	1.055

Gender. There was no significant difference found to exist in gender and overall concern, t=-.163, df=173 and p=.871.

Education. An ANOVA was run to determine if concern differed by education. The results were F(2,172)=.256, p=.774, which indicate no significant difference relative to educational achievement.

Students and Non-students. Another t-test was run to determine if there was a difference between students and non-students. The results indicate there was no significant difference in overall concern between students and non-students, t=1.089, df=173, p=.278.

Age. A correlation was run to determine if concern differed according to age of the respondent. Pearson correlation of -.012 and a p-value of .872 indicate no correlation between age and overall concern.

3.7 OTHER CONCERN – Respondents indicate whether they have additional concerns

Survey question 15 was an open-ended question in which respondents were asked, "*What other reasons do you have for not wanting to disclose your SSN*?" Respondents were given the opportunity to list concerns that differed from the choices offered in the survey. Several respondents provided examples of additional concerns. Numerous themes emerged from the responses:

1) USE OF THE SSN FOR IDENTIFICATION IS UNNECESSARY

Several respondents questioned the use of the SSN as valid identification.

- *Aren't there plenty of other ways to tell if I am me or not? For example, photo ID.*
- *It's just for social security benefits, not for personal identification in all situations.*
- *It is not necessary information for the majority of transactions.*

- *It is not necessary for most services and some offices really most do not destroy this info correctly or guard it properly*

2) USE OF THE SSN FOR IDENTIFICATION IS SOCIALIST

Respondents suggested repeated requests for the SSN may be a sign of a shift to socialism.

- *I don't want to be a victim of identity theft; I'm not a Communist Sympathizer or a member of the Socialist Workers Alliance.*
- *Why do they need to know? The road to SOCIALISM!*

3) THE SSN IN MULTIPLE RECORDS IS VULNERABLE TO MISMANAGEMENT

Security of private information is another common concern related to the use of the SSN in public and private agencies. Common among the comments was distrust of institutions and lack of confidence in the secure handling of the SSN.

- *I am not always aware of how record keeping works for those people/institutions that request it. At a previous University, medical records were hacked into and thousands of SSNs stolen. Quite a few of those were victims of identity theft thereafter.*
- *Places that I disclose my number to may mismanage their files, or have files stolen or made public.*
- *Safety and confidentiality of the records.*
- *Someone gaining or using the SSN to gain access to other information about me--medical records, banking issues, etc.*

4) PHILOSOPHICAL OBJECTION TO USE OF THE SSN AS A VIOLATION OF PRIVACY

Feelings of intrusion into personal privacy are evident in the several instances in which respondents expressed reluctance to disclose their SSN.

- *My right to privacy is VERY IMPORTANT to me!*
- *Personal information associated with SSN is no one else's business unless I want it to be.*
- *I believe, though I haven't researched this, that SSN's were not meant to be used as they are now. They have been bastardized and now every business and organization acts as if they have the right to have that information. We are told to keep that number to ourselves, yet society will no longer let us. This number can open so many doors for me that I don't want it to be used for trivial things such as setting up my cell phone account.*
- *I've always been told to be careful to whom I disclose it.*
- *I do not disclose any identifying information to any agency except financial, service (utilities, etc.) and medical organizations. Everyone else does not need to know this to provide whatever service I require, and it is more likely that they will not have as rigorous information protection policies as financial/service/medical organizations.*

5) USE OF THE SSN LEADS TO SPAM AND MASS-MARKETING MAILING LISTS

The reduction or elimination of spam or junk mail is a concern of both federal lawmakers and citizens. [2] This concern was articulated by a respondent.

- *Possibility of receiving more unwanted information than I already get (i.e. spam and junk mail).*

---

[2] Social Security Numbers in Commerce, (2006); Legislative Efforts to Combat Spam, (2003)). Spam has captured the attention of federal legislators who have waged efforts to combat Spam by introducing bills in Congress that would criminalize actions that result in voluminous amounts of Spam emails and telephone calls.

4. *Information Seeking Behavior*

4.1 FIND_INFO – Respondents indicate their practice of privacy information seeking

In survey question 9, "Now, we'll ask a few questions about how you find information about privacy or privacy laws," respondents indicated whether they have ever searched for:

- Information about privacy in general
- Government policies on the requirements to disclosure your SSN
- Federal or state laws on the requirements to provide your SSN

Table 20 provides these results.

Table 20: Information Seeking - Privacy Sources (Item 4.1)

	Yes		No	
	Count	Row N %	Count	Row N %
Information about privacy in general	67	36.4%	117	63.6%
Government policies on the requirements to disclose your SSN	13	7.1%	171	92.9%
Federal or state laws on the requirements to provide your SSN	15	8.2%	169	91.8%

More respondents have searched for information on general privacy issues than for privacy information as it relates to the SSN. However, the percentages of respondents reporting privacy seeking were fairly low for all categories. Specifically, only 36.4% reported seeking general information on privacy; 7.1% reported seeking information on government SSN policies and 8.2% of respondents reported searching for federal or state SSN laws.

4.2 SOURCES – Types of sources respondents consult for privacy information

In survey question 10, respondents were asked, "*How likely are you to use each of these sources to find information on legal requirements to provide your SSN*?" As shown in Table 21, for a mean of 2.5 and above, respondents are more likely to use a particular source to find information and for a mean below 2.5 respondents are less likely to use that source. Respondents are very likely to use a government office or website (Mean=3.32); likely to use a search engine (Mean=3.03) but unlikely to use a blog (Mean=1.78). Slightly lower than mid-range on the four-point measurement scale are using a public library (Mean=2.39) and consulting a friend (Mean=2.37). Survey results are shown in Table 21.

Table 21: Privacy Information Sources (Item 4.2)

	N	Minimum	Maximum	Mean	Std. Deviation	
Government office or website (such as Social Security Administration; Federal Trade Commission; or State Attorney General)	173	1	4	3.32	.821	↑
Search engine such as Google or Yahoo	173	1	4	3.03	.889	More likely to use source
Public library	174	1	4	2.39	.960	
Friend	170	1	4	2.37	.954	Less likely to use source ↓
Blog	174	1	4	1.78	.852	

Gender (*Significant results*). A MANOVA test determined sources used by respondents differed by gender, F(5, 163)=3.25, p=.008. Individual ANOVAs were conducted to determine which sources were different. This test found differences in the use of blogs (p=.033) and government offices (p=.033). Females are less likely to use blogs (Mean=1.68) than Males (Mean=2.00) and more likely to use government offices (Females, Mean=3.38 and Males, Mean=3.05).

Education (*Significant results*). A MANOVA test found sources used for privacy information differed by education F(10, 324)=2.130, p=.022. Individual ANOVA tests found the sources used differed only with the use of the public library, (p=.002). Respondents with *Some College* (Mean=2.14) were less likely to use the public library than respondents who possessed a *Bachelor's degree* (Mean=2.45) or *Master's degree or higher* (Mean=2.79).

Students and Non-students (*Significant results*). A MANOVA test was run to determine if sources differed between students and non-students, F(5, 163)=.5.67, p<.001. Individual ANOVAs found sources differed with the use of public libraries (p<.001) and government offices (p=.010) as non-students are more likely to use public libraries (Mean=2.72) and government offices (Mean=3.49). Please see Table 22.

Table 22: Privacy Sources Students / Non-students (Item 4.2 Student)

Dependent Variable		Mean
Public library	Non-student	2.726
	Student	2.115
Government office or website (such as Social Security Administration; Federal Trade Commission; or State Attorney General)	Non-student	3.493
	Student	3.167

Age (*Significant results*). Age is correlated with the use of the library, blogs and government offices. As age increases, the use of libraries and government offices also increases and the use of blogs decrease, as reported in Table 23.

Table 23: Privacy Sources and Age Correlations (Item 4.2 Age)

	Pearson Correlation	Sig. (2-tailed)
Public library	.309	.000**
Blog	-.164	.031*
Government office or website (such as Social Security Administration; Federal Trade Commission; or State Attorney General)	.193	.011*

**Correlation is significant at the 0.01 level (2-tailed).
*Correlation is significant at the 0.05 level (2-tailed).

Other Information Sources

In survey question 11, "*Please list any other sources you may use to find information on legal requirements to provide your SSN," respondents* were asked to list sources of privacy information other than those previously listed in the survey which were: *public library*, *blogs, government offices and websites, search engines* or *friend*. The purpose of the question was to determine exactly where people look for privacy information. For this open-ended question, respondents provided additional sources which were analyzed and categorized in three specific areas: institutions (*law library, bookstore*, and *police station*), persons (*parent* and *professor*) or privacy agreements (*credit agencies and businesses*). The most mentioned source was that of *lawyer* followed by *professors, police*, and *parents*. There was no mention of librarians or other information professionals.

Avoidance of Information

In survey question 12, respondents were asked to indicate why someone might avoid searching for information or laws about providing an SSN. The choices were:

- They don't know where to look
- They trust the government agencies, businesses or people that are given their SSN
- They feel a lack of control over who has access to their SSN
- They may feel intimidated

As presented in Table 24, respondents tended to agree with the statements. A higher percentage of respondents believe people do not look for privacy information or SSN laws because they don't know where to look.

Table 24: Avoidance of Information

	N	Minimum	Maximum	Mean	Std. Deviation
A. They don't know where to look	176	1	5	3.14	.715
B. 'They trust the government agencies, businesses or people that are given their SSN'	176	1	5	3.11	.724
C. They feel a lack of control over who has access to their SSN	176	1	5	3.04	.837
D. They may feel intimidated	176	1	5	3.07	.929

5. Survey Results for Tennessee Residents

In both the online and paper copy of the survey, respondents who did not identify themselves as residents of the state of Tennessee were directed to the Tennessee law questions, survey questions 2.A (TN) and 2.B (RECORDS). These questions specifically measured the awareness level of Tennessee residents.

5.1 TN (Tennessee) – Awareness of Tennessee Privacy Laws

Tennessee residents responded to survey question.2.A on the requirement to disclose the SSN as required by Tennessee Code in three areas:

A. Commercial driver's license

B. Death certificates

C. State scholarship recipients

To determine awareness, survey respondents were asked if they agreed with statements A, B, and C. As indicated in the literature, these statements are either true or false. As shown in Table 25, statements A, B, and C are all true. If respondents correctly answered statements A, B, or C with a response of a*gree* or s*trongly agree,* then that response indicated awareness. If respondents answered with s*trongly disagree*, d*isagree* or d*on't know*, then that response indicated unawareness.

EXPLANATION:

The state of Tennessee requires disclosure of the SSN in all three scenarios.

A – According to Tennessee law (Tenn. Code Ann. § 55-50-321 (Supp. 2008)), SSNs must be included on all commercial driver license applications. Tennessee citizens indicated awareness at 71.2%.

B – Tennessee law (Tenn. Code Ann. § 68-3-502 (Supp. 2008)) requires the SSN of the deceased to be placed on petitions for certification of death. Tennessee citizens indicated awareness for the requirement to disclose the SSN on death certificates at 63.6%.

C – Tennessee law (Tenn. Code Ann. § 49-7-826 (2009)) requires state scholarship recipients to disclose their SSN. Tennessee residents indicated awareness for the requirement to disclose the SSN in order to obtain a state scholarship at 63.6%.

Table 25: Awareness - Tennessee Laws (Item 5.1)

	Unaware		Aware		Correct Answer*
	Count	Percent	Count	Percent	
A. 'According to Tennessee State law, an application for a commercial driver's license requires disclosure of the Social Security Number (SSN).'	38	28.8%	94	71.2%	True
B. 'According to Tennessee State law, death certificates require the disclosure of the deceased's SSN.'	48	36.4%	84	63.6%	True
C. Tennessee state law requires the disclosure of the SSN of a state scholarship recipient.	64	48.5%	68	51.5%	True

***For example, statement A is true. Respondents indicated awareness at a rate of 71.2% and unawareness at a rate of 28.8%.

5.2 RECORDS – Awareness of Tennessee Laws Pertaining to SSNs in government records

Survey question 2.B queries Tennessee residents on state law requirements to disclose the SSN. To determine awareness, survey respondents were asked of Tennessee requirements to disclose the SSN for inclusion in certain court and government records listed below:

A. Divorce decree

B. Paternity record

C. Fishing license

D. Marriage license

According to Tennessee state laws, the SSN must be included in all of these records. Therefore, statements A, B, C and D are all true, as shown in Table 26. Respondents who correctly answered statements A, B, C or D with a response of *Yes*, indicated their awareness of these state laws. When respondents incorrectly answered any of the statements with a response of *N*o or *Don't know*, that response indicated unawareness.

EXPLANATION:

A – Tennessee respondents had an awareness level of 36.4% of the legal requirement to disclose the SSN to file a complaint for divorce (Tenn. Code Ann. § 36-4-106 (2008)). Additionally, the SSN must be entered on the certificate of divorce (Tenn. Code Ann. § 68-3-402 (2007)).

B – Tennessee respondents were 50.8% aware that state law (Tenn. Code Ann. § 36-2-311 (2008)) requires disclosure of an SSN in paternity records.

C – Tennessee respondents were 11.4% aware of the Tennessee state law (Tenn. Code Ann. § 36-5-1301 (2005)) which requires the disclosure the SSN to obtain a fishing license.

D – Tennessee respondents were 56.8% aware of the Tennessee law (Tenn. Code Ann. § 36-5-1301 (2005)) that requires an SSN on a marriage application. Tennessee law also requires inclusion of the SSN on the certificate of marriage (Tenn. Code Ann. § 68-3-401 (Supp. 2008)).

Table 26: Awareness - Tennessee Court Records (Item 5.2)

	Unaware		Aware		Correct Answer*
	Count	Row N %	Count	Row N %	
A. Divorce decree	84	63.6%	48	36.4%	Yes
B. Paternity record	65	49.2%	67	50.8%	Yes
C. Fishing license	117	88.6%	15	11.4%	Yes
D. Marriage license	57	43.2%	75	56.8%	Yes

*For example, statement C is true. Respondents indicated awareness at a rate of 11.4% and unawareness at a rate of 88.6%.

On average, Tennessee respondents showed an awareness level of 48.81% of Tennessee SSN laws.

Gender. A t-test was conducted to determine if awareness differed by gender. The results were $t=.375$, $df=121$, $p=.709$, which shows no significant difference in awareness by gender.

Students and Non-students. A t-test was run to determine if a difference existed between students and non-students. The results, $t=1.65$, $df=121$, $p=.101$, indicate no significant difference in awareness between students and non-students.

Education. An ANOVA was run to determine if there was a difference relative to educational achievement of respondents. The results were $F(2, 120)=.637$, $p=.531$, which signify no significant difference in Tennessee citizen awareness of SSN laws when analyzed by education.

Age. To test if awareness of Tennessee respondents was related to age, a Pearson correlation was run. The correlation coefficient was -.035 ($p=.699$) which shows there is no correlation of age to awareness for Tennessee respondents.

Awareness of Tennessee SSN Laws

Awareness of Tennessee SSN laws appeared to be higher than awareness for federal SSN laws. Consequently, a paired sample t-test was run to compare overall awareness of federal SSN laws with Tennessee SSN laws. The results of the paired t-test were: $t=-7.243$, $df=131$, $p<.001$ with a mean overall awareness of 30.97% and mean Tennessee awareness of 48.81% which indicates Tennessee residents are significantly more aware of the Tennessee SSN laws than the federal SSN laws queried in the survey.

A question on military discharge records was included in the survey in the section on Tennessee law, survey question 2.B. On further analysis, the decision was made to exclude that question from the survey results because although the SSN is required on the documents, former military personnel can petition to have their SSN redacted. Despite the fact that the possibility for redaction of SSNs in military discharge records is clear in the law, this fact was not evident in the survey question (Tenn. Code Ann. § 10-7-513 (Supp. 2008)).

Chapter 5: Discussion

The purpose of this study was to find out what people know about information privacy, how they go about searching for information privacy laws and what their concerns are about disclosing their SSN to government agencies and private organizations. To that end, a quantitative survey was designed to gather statistics. The questionnaire was released to individuals who were presumed not to be legal professionals. That being said, legal research can be challenging for professionally trained persons and laypersons alike as some laws apply in certain circumstances while other laws are considered "absolute." In all cases, laws are considered valid until they are successful challenged in a court of law or otherwise repealed by the legislature.

The multiple-response questionnaire was designed using several measurement scales to determine awareness, concern and information seeking behavior. Take for example survey question 2, on the subject of the Patriot Act: if a company representative asserts that the SSN is required by the Patriot Act to establish an account, does a customer know or believe that the assertion is true? If a customer assumes that the claim is probably true because the customer doesn't know the language of the Patriot Act, is he or she then more likely to disclose their SSN? Also in survey question 2, on the subject of utility companies, an individual may not know that a utility company will charge a deposit fee in lieu of collecting an SSN. The individual may strongly disagree that a deposit is acceptable and simply decide to disclose his or her SSN to obtain services without confirming a legal disclosure requirement.

The survey instrument was an exploratory tool to measure peoples' responses. The survey responses were combined and the results were analyzed collectively, providing a grade for the total number of respondents on a scale of 0%-100% with zero representing a failing grade and 100% indicating excellence. If a score indicated awareness more than not (with a score of 50% or higher) respondents were considered to have met the threshold of awareness.

Discussion of Survey Results

Survey results, in brief, revealed that awareness level of SSN law is low, concern of the potential risk from the use of SSNs for identification is in the average to moderate range. Individuals would rather use search engines than use a library to find information on SSN law. Although the results of low awareness were expected, the researcher expected concern to be higher. In addition, the findings of the information seeking behavior give valuable insight for information professionals into improving citizen awareness.

Awareness

Analysis of the data has provided answers to the research questions presented below.

Research Question 1: What are the levels of awareness of federal and state of Tennessee privacy laws pertaining to Social Security Numbers? **Answer**: Survey respondents have a low level of awareness of federal and state SSN laws. Tennessee residents have an awareness level of 30.97% for federal laws and 48.81% for state laws. For all respondents, the awareness level of federal laws was slightly higher at 32.4%.

The Supremacy clause of the United States Constitution provides that federal laws supersede conflicting state laws; however, state laws directly affect the daily lives of residents of the state in the normal course of their lives. Individuals have contact with state government agencies by engaging in life activities such as marriage, divorce, driver and professional licensing, establishing paternity, voting, and registering the death of a loved one. Consequently, respondents had a lower awareness score for federal SSN laws; while state residents had a statistically higher level of awareness of Tennessee SSN laws. However, both of these scores represent a failing grade, falling below the threshold level of awareness.

When analyzing specific awareness laws and responses, awareness levels differ depending upon the circumstance. Respondents were more aware of the availability of a free, yearly credit report (66.3%), but less aware (9.2%) that the Patriot Act has no SSN disclosure requirement to obtain lottery winnings.

USA Patriot Act and the SSN

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, better known as the Patriot Act, was originally passed on October 26, 2001, 45 days after the attacks of 9-11. A response to the terrorist attacks was definitely necessary in order to hold accountable those persons who were responsible for the devastation and provide the United States government with strategies to prevent future attacks. Yet, the quickly-ratified, reactionary, overly broad legislation that is the Patriot Act is a difficult piece of legislation for Americans citizens to decipher (http://www.eff.org/issues/patriot-act; http://epic.org/privacy/terrorism/usapatriot).

The Patriot Act has been used as what could be characterized as an intimidation tactic because of its perceived power. The validity of the Patriot Act is not often challenged by those who have not researched its contents. The only mention of the SSN in the Patriot Act is located in Section 326, Verification of Identification. In this section, the Secretary of the Treasury sets minimum standards to verify identity of new customers of financial institutions to compare those customers with known terrorists. This provision requires financial institutions to comply with (a)(2)B) "*reasonable procedures to verify a person's identity, including name, address and other identity information*" to obtain valid, personally identifying information when establishing accounts. Section 326 of the Patriot Act further requests a study and report in subsection (b)(2) for recommendations *"requiring foreign nationals to apply for and obtain, before opening an account with a domestic financial institution, an identification number which would function similarly to a Social Security number or tax identification number."* It bears repeating that the only reference to the SSN in the Patriot Act is in relation to establishing a means to track non-Americans who wish to open an account with financial institutions.

Librarians were among the most vocal opponents of the Patriot Act when it was first enacted in 2001 and were instrumental in the amendment of the Patriot Act of 2006, *Sec. 5. Privacy Protections for Library Patrons*. This provision states that libraries are "*not a wire of electronic service provider*" and clarifies that libraries are not subject to the National Security Letter provision of the Patriot Act.[3]

The Patriot Act has been erroneously cited as requiring the SSN to obtain a driver license, to acquire lottery winnings, and to establish a telecommunications account, i.e., telephone, Internet and cable service[4]. Responses to survey question 2, (53.3% awareness level) and survey

---

[3] National Security Letters (NSLs) *are a search procedure which gives the FBI the power to compel the disclosure of customer records. These entities are prohibited, or "gagged," from telling anyone about their receipt of the NSL, which makes oversight difficult. The Number of NSLs issued has grown dramatically since the Patriot Act expanded the FBI's authority to issue them.* Retrieved March 28, 2010 from: http://epic.org/privacy/nsl/

[4] Posting February 24, 2010 on the search engine Yahoo.com incorrectly attributed the Patriot Act as the legal requirement mandating the disclosure of the SSN to obtain a driver license. In 1976, the Tax Reform Act granted states permission to collect SSNs for driver licensing. http://customsites.yahoo.com/financiallyfit/finance/article-108911-4270-3-when-you-should-and-shouldnt-give-out-your-social-security-number?ywaad=ad0035

question 3, (9.2% awareness level) imply respondents will submit to requests for their SSN with the assertion that the Patriot Act is the authorization to compel disclosure as a consequence of their unawareness.

Awareness of Federal SSN Laws

Of the federal awareness scenarios listed in Chapter 4 of this study, ten out of seventeen had responses equaling an awareness level of less than 20%. From Table 5 in Chapter 4, we learn one of the lowest awareness scores was 17.4% on the Social Security Administration's issuance of a new SSN in cases where an individual is plagued with problems that come from the criminal use of his or her SSN. This is not a common practice, as issuance of a new SSN can create a different set of undesirable circumstances. Also from Table 5, utility companies of water, electricity, gas, sewer and garbage collection are not legally authorized to collect SSNs, but routinely do. The awareness level of laws pertaining to disclosure of the SSN to utility companies was 14.1%. Personally identifying information of name, date of birth, current and former addresses, place of employment and SSN are kept in the databases of utility companies. This personal information is often shared with government agencies, upon request written request, sometimes with a court order (Klosek, 2007). This practice is extremely useful for law enforcement purposes but is considerably intrusive for people who are not subject to civil or criminal enforcements. Federal and local police collect personal information from these agencies to find customers who have absconded from criminal prosecutions; are delinquent in child support payments, or who are listed on the voting rolls with felony convictions (*Preserving the Integrity of Social Security Numbers and Preventing their Misuse by Terrorists and Identity Thieves, 2003*).

An occurrence of sharing SSNs was reported in the Knoxville *News Sentinel* on December 30, 2009. The Tennessee Department of Correction provided a list of the SSNs of felons to the Knox County, Tennessee Election Commission. Election officials used this information to purge the voting rolls of convicted felons in Knox County, as voting by felons is prohibited throughout the state by Tennessee Constitution, art. IV, § 2. Fears in the 1970s that government agencies would collect and share personal information of individuals without their knowledge have come to pass.

From Table 6 in Chapter 4, we learn that respondents were only 14.7% aware that retail businesses are not under any legal authority to collect SSNs and more importantly, retail businesses can legally refuse to provide goods or services if an individual refuses to disclose their SSN as there is no law preventing denial of goods or services for refusal to disclose (*Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy*, 2006). Businesses collect and share SSNs in an effort to verify identity and ensure tracking of customers who fail to meet their payment obligations. There are two scenarios in table 7, Chapter 4 where respondents' awareness levels were extremely low: receiving medical or dental services at a private office and applying for credit. Private medical and dental health offices routinely collect SSNs from customers without any legal authority to do so. Respondents' awareness level that there is no legal requirement to disclose their SSN was 16.8%. For privately funded health care, private insurance companies obtain SSNs not only from patients but also from employers who in turn share SSNs with health care providers.

There is no law that mandates the disclosure of the SSN when applying for consumer credit, yet individuals readily hand over the number, thinking that the SSN it is legally required.

Respondent awareness level of the legal requirements to disclose the SSN to obtain consumer credit was 1.1%. Personal identifiers of name, SSN, date of birth, address, employer and account number are sufficient to establish a person's identity (Hendricks, 1990). The SSN is a key piece of personal information used by persons committing identity theft (GAO-08-343, 2008). SSNs are available to many, including identity thieves and those intent on committing fraud (Solove, 2004). Anyone who possesses another's SSN could potentially use it to open and close accounts, obtain loans, change addresses, access medical records and assume another's identity as SSNs are found in many public databases, on consumer applications, and as an employee identification number.

Awareness of Tennessee SSN Laws

Tennessee residents show low awareness levels of two state laws in particular which require SSN disclosure to obtain a divorce (36.4%) and a fishing license (11.4%). Students in their early twenties are presumably less likely to have been divorced; hence, the low score is not surprising. Also not surprising is the low score pertaining to a fishing license. Even though it is understandable that the goal of the state government is to regulate fishing, it is not so clear that the state needs the SSN to accomplish that goal. The literature review revealed additional SSN legislation that was not included in the survey questionnaire, notably, registering to vote. The state of Tennessee requires disclosure of the SSN, but other states, e.g., Louisiana, do not require SSN disclosure, McKay v. Thompson, 226 F.3d 752 (2000).

Mandatory disclosure requirements place Tennessee residents at substantial risk when SSNs are left vulnerable through inadequate and improper handling due to the increase of electronic records. In December 2007, the SSNs of more than 300,000 Davidson County, Tennessee registered voters were breached with the theft of two laptop computers from the Davidson County Election Commission. Additionally in Tennessee, students SSNs in Williamson County Schools were accidentally posted on the Internet in 2008 for a brief period of time. These data were revealed in S*afeguarding Social Security Numbers in Tennessee Government Records,* a study published in 2008 by the Tennessee Offices of Research and Education Accountability (OREA), which found state agencies in Tennessee lack comprehensive controls to secure personal information. Conclusions of the study were:

1. Tennessee government agencies have reduced SSN use, but further reduction may be possible.
2. Some agencies lack sufficient policies to protect SSNs.
3. Use of safeguards and management controls to protect SSNs in electronic and paper records varies.
4. Tennessee law does not clearly direct local government records custodians on the treatment of SSNs in agency records.
5. State information security policies meet best practices, but agency compliance is unclear.
6. State government provides limited oversight of local personal information protection practices.
7. State law does not designate an agency to receive security breach notifications.

Relationship of Awareness to Demographics

Survey results provided still more awareness data. There was no statistical difference in awareness in two of the survey variables: gender and education. Neither gender was more aware of SSN laws.

Educational achievement of respondents made no difference in SSN law awareness. An assumption that more educated persons as a group know more about privacy is false. Study results found persons with more formal education had no more knowledge of SSN laws than the less-educated.

The relationship of student status to age is an important one. As people grows older, they are more likely to have completed their formal education and more likely to engage in day-to-day activities where the SSN is requested, which may well explain why older respondents were significantly more aware of SSN laws. Survey variables in which there were statistical differences in awareness were age and student status. The majority of respondents in the student category were students in the on-campus class under the age of 25.

Concern

Analysis of individual concern of the use of the SSN for identification provided surprising results**.**

Research Question 2: What are the levels of concern pertaining to the disclosure of one's Social Security Number? **Answer**: Concern regarding use of SSN for identification is in the average to moderate range.

Study participants did not differ substantially by any demographic in their overall concern of the widespread use of the SSN. The finding of a low level of awareness of SSN law may explain the average to moderate level of concern. Possible reasons for the level of concern are many.

1) Perhaps individuals have a lower level of concern simply because they don't care who obtains their SSN.

2) Individuals may have a lower level of concern because there is a lack of awareness of the risks of identity theft and fraud associated with the use of the SSN.

3) Alternately, individuals could have a lower level of concern largely because of the protective actions taken to safeguard their SSN by limiting disclosure only to agencies and institutions that have a legal right to the SSN.

4) Finally, individuals may have a lower level of concern due to limiting activities that request an SSN either with or without legal authorization.

Why should individuals be concerned about the use of the SSN for identification? As one respondent stated, *The original Social Security card had "not to be used for identification" for a reason, but over time, more [and] more the SSN is required as proof of identification, almost a given in areas of credit [and] financial history. [It] bothers me that a number holds so much power*. This respondent appears to be especially aware of the deviation from the intended use of SSNs but an inference of survey results is that most respondents are not aware of the power of the SSN or how their personal information is used or can be used.

Why the SSN Fails as an Identifier

Although the public was assured when SSNs were first created that the use of the number would be strictly limited for the narrow purpose of social security benefits calculation, the promise was broken only seven years after enumeration of SSNs began in 1936. There was an unintended consequence of Executive Order 9397 signed by President Roosevelt in 1943 requiring federal agencies to use the SSN when creating new record-keeping systems. Undoubtedly, President Roosevelt never contemplated the advent of the Internet where SSNs can be accessed in public records and used from everything from applying for a driver license to applying for a school loan, effectively making the SSN a universal identifier.

A survey respondent noted that providing the SSN for something as *trivial* as obtaining a cell phone has nothing to do with the original purpose of the SSN. The Order is asserted as valid reason more than half a century later for applicants to disclose their SSN when applying for federal employment. In 1977, the Privacy Protection Study Commission recommended repeal of the Order because agencies had begun to state this law as authorization to collect SSNs. More than three decades later, the 1943 Order is still being used by the federal government to require disclosure from job-seekers, as shown in Figure 1. The rationale for demanding the SSN to uniquely identify applicants under a 1943 Executive Order ignores the online technology that exists today. In the rare occasion that the names of job applicants are absolutely identical, computer software can differentiate applicants not only by date and time of application, but by other identifiers in the application such as address, employers and telephone number.

USAJOBS
"WORKING FOR AMERICA"

Social Security Number - Your Social Security Number is requested under the authority of Executive Order 9397 to uniquely identify your records from those of other applicants who may have the same name. As allowed by law or Presidential directive, your Social Security Number is used to seek information about you from employers, schools, banks, and others who may know you. Failure to provide your Social Security Number on your application materials, will result in your application not being processed.

Figure 1: USAJOBS SSN Executive Order 9397 Disclosure Statement
Retrieved March 20, 2010 from http://www.usajobs.gov

The current practice of using SSNs for identification and authentication provide an efficient means of tracking individuals in computer databases but the practice is flawed. The SSN falls short of the criteria to be a considered a true universal identifier, as reported in Table 27. A true identifier must be a label, defined here as a description that includes the following characteristics:

1. No more than one person should have a given label;
2. No person should have more than one label;
3. The label must be unique to each person;
4. The label must be used throughout a person's lifetime and cannot be used after his death; and
5. The label must include an internal check feature to detect errors in transmission or communication.

(Hendricks, p. 61)

Table 27: Characteristics of a Universal Identifier

Universal Identifier Characteristics	True Universal Identifier	Social Security Number
Unique	Label must be unique to each individual	SSNs which are acquired fraudulently can be used by someone other than the person to whom it was issued
One number, one person	Only one label is issued to each individual	More than one SSN can be issued by the Social Security Administration to an individual
Lifetime use	The label cannot be used after the individual's death	SSNs of deceased persons are available in public and private databases
Internal check feature (ICF)	Verification feature included, i.e., CVV* code	No ICF or biometric feature

*Card Verification Value

The fact that the SSN is not secure is one of many reasons why it is a poor choice as an identifier. Records containing SSNs as the identifier place all records using the SSN in jeopardy. Not every institution that obtains an SSN for an authorized purpose should have access to all information that can be acquired with the use of that identifier (*Privacy: Preventing and responding to improper disclosures of personal information*, 2006, p. 4). Additionally, clerical mistakes from data entry errors or miscommunication of the SSN cause inaccuracies in records necessitating spending time and money to correct those errors.

There is an expectation of American citizens that personal information will be protected by government agencies and private businesses. This presumption is risky. Deliberate theft by current and former employees, accidental disclosure, federal and state disclosure law, and inadequate privacy policies preempt this expectation of privacy (*Privacy: Preventing and responding to improper disclosures of personal information*, 2006). The Social Security Administration's admonition printed on early social security cards against the use of the SSN for identification purposes is an indication that the use of the SSN as an identifier is ill-advised. The rise of identity theft and loss of privacy in the United States because of the illegal use of another's SSN is evidence of why the use of the SSN fails as an identifier. Equivalent to the SSN in the United States is the Social Insurance Number (SIN) in Canada Canadian government denies private organizations any legal right to request a customer's except for income reporting purposes (Saunders, J. & Graebrier, C., 2007, p. 96).

Information Seeking Behavior

Survey results indicate knowing where to search for SSN laws is a major step toward improving awareness.

Research Question 3: What sources are used to find information on laws pertaining to the disclosure of the Social Security Numbers? **Answer**: Of the five options offered in the survey, in order of preference, survey respondents are more likely to use: *Government offices (3.32); Search engines (3.03); Public libraries (2.39); Friends (2.37); and Blogs (1.78)* to search for privacy information.

Libraries are consulted on average only slightly more than friends on a five point scale. Of course, if the friend is also uninformed, any information gathered is likely erroneous. This finding of respondents using libraries less than search engines and government offices—but more than friends and blogs—may explain why the awareness level is so low.

Search engines are the second most used source of information. Web postings on privacy and SSN laws can be rife with inaccuracies. The most common source used is government offices and websites. Consulting these sources is a superior approach to obtaining accurate information on legal requirements of SSN laws. The Federal Trade Commission (FTC) is required to process complaints of identity theft. The Social Security Administration (SSA) issues new and replacement social security cards; its website provides links to publications pertaining to administration of the social security program. Additionally, Tennessee state laws are searchable online and in legal code and casebooks.

An overwhelming percentage of survey respondents indicated that they had not searched for privacy information on SSN laws (8.2%), government policies on SSN disclosure (7.1%) or privacy information in general (36.4%). Although the latter situation, privacy information in general is more than triple the other two categories, the incidence of privacy information seeking is still quite low.

Relationship of Information Seeking to Demographics

There were significant differences in information seeking across every demographic. Females are less likely to use blogs but more likely to use government sources; higher-educated individuals are more likely to use libraries. Interestingly, non-students (who tended to be older with more education) are more likely to use libraries and government sources than students but less likely to use blogs. The use of blogs by respondents who tended to be young, male and students are indicative of the method of communication used by this demographic. The researcher sees value in this finding. Not all blogs are sounding boards filled with opinions based on biased, personal beliefs. Blogs often contain current, factual information that is disseminated to interested individuals who may not be able to find useful information elsewhere. Information found on blogs may be in and of itself sufficient to satisfy an information need or may serve as a bridge to discover more authoritative sources.

When asked to list other sources for privacy information on requirements to disclose their SSN, respondents mentioned sources such as lawyer, parents, professor and police which suggests a desire for guidance from authority figures. Considering the sources of parents and professors were likely suggested by the student group, (statistics were not captured to confirm this conclusion) lawyer was the most-mentioned. It is not always feasible to consult with a lawyer for everyday activities because of expense and time constraints. Privacy agreements were also mentioned as sources of privacy information. Privacy notices are required of financial and other institutions by law but are largely notices, not bilateral agreements, of privacy practices. Third-party sharing of personal information is also explained in privacy notices. Customers in some circumstances have opt-out rights but usually have no input into the composition of these "agreements" which often change without the customer's knowledge. The option of ending the relationship with the institution is often the only recourse customers have if the privacy agreement is not to their liking.

Why a Privacy Discussion is Important

Privacy is essential for the whole of society by promoting the psychological well-being of individuals and allowing people to develop and fulfill themselves and the proper functioning of democracy (Strum, 1998, p. 7). Study findings show that some individuals clearly don't know about privacy laws; some don't care. Individuals who do not know about privacy laws or who are not concerned with disclosure of their SSN may be placing themselves at risk of exposure of the intimate details of their lives and identity theft unnecessarily. Citizens are not always consciously aware of how their private information is accumulated in public and private databases or how that information is being used.

Public records containing SSNs are often searchable in government databases. When the federal and state government enacts a law involving the use of the SSN, such as requiring disclosure of the SSN for voter registration, or a private medical office makes a rule requesting patient SSN disclosure, not under legal authority but to keep track of its clients, citizens don't always know what impact these laws and rules have on their personal privacy. Collecting SSNs to administratively process accounts is convenient and expedient for government agencies and private businesses but the widespread use of SSNs for identification exposes individuals to possible financial harm due to identity theft or fraud; loss of personal privacy because the SSN is tied to so many of a person's life records; or even loss of liberty due to mistaken identity by law enforcement.

The awareness levels of survey respondents were expected by the researcher to be low and these levels were low for both federal and state laws. With individuals living their personal and professional lives more at the state level, (e.g., marriage, divorce, voting, professional and driver licensing) the awareness levels were higher at the state level. However, the awareness levels for both federal and state laws was lower than the 50% threshold, which means respondents did not correctly answer most survey questions. Study results indicate the level of education achieved was not statistically significant. Awareness levels of SSN laws increase with life experience that comes with age which was statistically significant. Also statistically significant was the awareness level of non-students in the study. These non-students tended to be older presumably with more life experiences than students.

When individuals disclose their SSN to agencies and businesses which have no legal right to collect SSNs, an individual's action affects not only that individual but collectively determines what is considered the norm for the whole of society. As previously mentioned in this study, the SSN has become the de facto, universal identifier in the United States. This is so because the SSN is assigned by the United States, it is ubiquitous and it is unique to each individual. Contrary to its original purpose, the SSN is now legally required by many federal and state agencies. The many contextualized situations profiled in this study demonstrate that the routine gathering of SSNs by private organizations is not under the pressure of law. Instead, SSNs are regularly collected by private organizations not with legal authority (de jure), but without legal authority (de facto) as a matter of course. But, people don't know what they don't know. Individuals must become risk managers to better protect their personal information. Commercial businesses and medical facilities continue to require the SSN to establish and access accounts without legal authority partly because individuals disclose their SSN without knowing the legal disclosure requirements.

The power to control personal information circulating throughout society is essential to maintaining social relationships and personal freedom; however, when a person is deprived of that control, he becomes subservient to the institutions or people who are able to manipulate that information (Miller, 1971, p.25). The imbalance of power that exists with government agencies and commercial business use of the SSN necessitates individual awareness of pertinent laws. Often many individuals don't consider the possible consequences of disclosing their SSN when it is not legally required. This observation was shared in the comments by one respondent, "*Even with the knowledge of identity theft, people in the 18-40 age group don't seem to take it seriously. They … don't seem to care*." Another respondent acknowledged a sense of powerlessness, "*I don't trust most institutions to protect my SSN, but at the same time, I don't feel like there is much I can do about it. Hackers and similar people work much faster than any institutional policy.*" Another respondent stated, "*I hope to see a more informed and empowered public in the future regarding an individual's right when it concerns releasing their social security number to others.*" Finally, a respondent summed up the researcher's reasoning for pursuing this topic of research, *"I think a lot of people, myself included, have never really thought about examining laws pertaining to the disclosure of [their] SSN."*

Individuals are directly affected by the collection, use and dissemination of their personal information gathered by public agencies and private businesses. The use of information technology to collect and maintain personal information has increased the speed of communications, improved business efficiency and placed individuals in substantial risk of harm due to identity theft and fraud. Enforcement of privacy protections provided by the Privacy Act, FACTA, HIPAA, and other privacy laws are ineffective if individuals are unaware of the resources available to them or fail to exercise the power and control over their personal information that these laws provide. Most people simply provide their SSN when it is requested; equally unaware of the way SSNs have become the primary means of linking databases and of people's right in most circumstances to deny the number to nongovernmental entities (Strum, 1998). Rights to consent to collection of an individual's SSN lack meaning if people can be readily pressured, misled, or coerced into relinquishing their personal information (Solove, 2004, p. 97).

Although polls indicate that people care deeply about privacy, people routinely give out their personal information willingly reveal intimate details about their lives on the Internet (Solove, 2008, p.5). This research supports these statements from prior research. Individuals are willing to give out their personal information even when there is no law compelling disclosure. Some survey respondents, through their responses, suggested they had provided their SSNs to commercial businesses to obtain Internet, cell phone and utility services in addition to retail stores to obtain credit and even to libraries to obtain a library card when none of entities have legal authority to collect SSNs. Anecdotally, a student entered her SSN on the paper copy of the survey for question 2, which has the variable designation of *SSN*.

Information Professionals and Privacy Literacy

Alternately referred to as gatekeepers or watchdogs of information, librarians are charged with ensuring that people's information interests are met. The America Library Association defines an information literate individual as a person who is *able to recognize when information is needed and have the ability to locate, evaluate, and use effectively the needed information*. For other disciplines, privacy terms are regularly used by information professionals. For instance, the terms health literacy and financial literacy are fairly common. Health literacy is the ability to understand basic health information sufficiently enough to make appropriate health decisions. Financial literacy is the ability of individuals to make informed judgments and effective decisions about the use and management of their money. A review of the academic literature did not reveal a definition of the term *privacy literacy* which appears in blogs among those interested in privacy issues. This research suggests that the term should be defined in a formal scholarly way so that it may be incorporated in future published works in a consistent manner. The suggestion is for *privacy literacy* to be defined to mean *the ability to find and understand information about privacy in order to make informed decisions pertaining to one's personal information*.

Study results show that there is a need for a privacy literacy program and that is where information professionals can take a leading role in improving privacy literacy. The protection of personal information must be approached with a multi-pronged approach involving the input of information seekers, information providers and the federal and state legislatures. To increase individual awareness and improve privacy literacy, individuals must be informed of privacy laws through formal education and library user instruction.

Survey respondents agreed that people avoid looking for privacy information simply because they don't know where to look. Another consideration in privacy information seeking is the knowledge-behavior gap (Case, 2007). There is no guarantee that an individual will act on new information. Concern for privacy does not necessarily translate into actions that would restrict individuals from sharing their SSN. Although this study does not explore whether individuals limit their activities because of fear of identity theft, fraud, or invasion of privacy, future research can delve further into this area of study.

Conclusion

The major three significant findings in this study are:

1) Awareness of federal and state social security numbers is low among the sample of Tennessee residents and the general population of the United States;

2) Concern regarding the use of the SSN for identification purposes is in the average to moderate range; and

3) Most respondents indicated that they had not searched for privacy information.

Results from this research make a significant contribution to the privacy discussion by demonstrating that a lack of awareness of privacy laws exists. This study proposes that intervention by libraries can raise the level of awareness by offering workshops and user instruction to library users. Privacy literacy can be increased with access to authoritative sources of legal requirements to disclose one's SSN in particular and privacy information in general. Librarians and other information professionals are in a unique position to assist individuals in raising their awareness of privacy laws because libraries are an excellent place to disseminate information to help individuals learn more about privacy. Significant differences in awareness of age and student status suggests intervention could improve privacy literacy of students by offering or requiring courses in privacy starting in lower-division classes in formal education. The beginning of a school year at the university level comes with an inordinate amount of information for incoming students; however, academic librarians and library staff should be included during orientation to familiarize students with the layout of the library and the library's functioning. A cursory overview of the location of the library on campus or the circulation desk to check out books or rent a laptop may not be enough to acquaint students with the services offered by the library.

In American society, public libraries are a trusted institution not often used to full capacity. For individuals who are not engaged in formal education, public library outreach to the community would facilitate user instruction by offering access to credible sources from which to obtain privacy information pertinent to user needs. Other possibilities to increase awareness are workshops and seminars on preventing identity theft at public libraries in a *Privacy Day* format. Volunteer privacy professionals and attorneys along with librarians could conduct workshops on searching for privacy information from the library's website and from the patron's own computers. Links to authoritative, reliable websites through the public library's online public catalog system with optional printable pamphlets listing authoritative sources would assist patrons with their search.

Knowledge is power. Individuals must exert autonomy over their own personal information to manage their risk which is challenging because study findings seem to suggest that people feel compelled to provide this powerful number even in situations where there is no law compelling SSN disclosure.

Future Research

There are many possibilities for future research in information privacy noted throughout this thesis regarding the SSN. For instance, how does awareness of SSN laws influence behavior? Does concern determine actions? Do individuals limit their activities because of fear of identity theft, fraud, or invasion of privacy? Although SSN requirements for public health agencies were queried in the survey, those results were excluded from study results. As stated in Chapter 4, instances where SSNs may be legally required within public agencies may vary. Future research might explore the use of the SSN in public medical agencies and its impact on privacy. Because this study does not explore people's comprehension of privacy laws, only their awareness that such laws exist, future research can further seek to determine if there is an understanding of privacy laws in various situations. And finally, future research could explore whether an information literacy program increases protection of personal information.

REFERENCES

References

Agencies take steps to safeguard data. (2007). *Information Management Journal*, 41(5), 20.

Bielefield, A. & Cheeseman, L. (1994). *Maintaining the privacy of library records. A handbook and guide.* New York: Neal-Schuman.

Bertoni, D. (2007a). *Social security numbers. Federal actions could further decrease availability in public records, though other vulnerabilities remain. Report to the chairman, subcommittee on administrative oversight and the courts, committee on judiciary, U.S. Senate.* United States General Accounting Office. GAO-07-752. Retrieved January 23, 2009 from http://www.gao.gov/new.items/d07752.pdf

Bertoni, D. (2007b). Social security numbers. Use is widespread and protection could be improved. *Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives. United States General Accounting Office*. GAO-07-1023T. Retrieved January 23, 2009 from http://www.gao.gov/new.items/d071023t.pdf

Bovbjerg, B.D. (2005). *Social security numbers. Federal and state laws restrict use of SSNs, yet gaps remain. Testimony Before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, New York State Assembly.* General Accounting Office. GAO-05-1016T. Retrieved January 23, 2009 from http://www.gao.gov/new.items/d051016t.pdf

Bovbjerg, B.D. (2003). *Social security numbers*. *Ensuring the integrity of the SSN. Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives.* United States General Accounting Office. GAO-03-941T. Retrieved January 23, 2009 from http://www.gao.gov/new.items/d03941t.pdf

Bovbjerg, B.D. (2006). *Social security numbers. Stronger protections needed when contractors have access to SSNs. Report to Congressional Requesters.* General Accounting Office. GAO-05-1016T. Retrieved January 23, 2009 from http://www.gao.gov/new.items/d06238.pdf

Breckenridge, A.C. (1970). *The right to privacy.* Lincoln, Nebraska: University of Nebraska Press.

Case, D. (2007). *Looking for information: a survey of research on information seeking needs, and behavior.* New York: Academic Press.

Chen, C. & Hernon, P. (1982). *Information seeking: assessing and anticipating user needs.* New York: Neal-Schuman Publishers.

Cornelius, V. (Ed.) (2002). *Personal privacy*. Huntington, New York: Novinka Books, Nova Science Publishers.

Creswell, J.W. (2003). *Research Design. Qualitative, Quantitative, and Mixed Methods Approaches*, (*2nd ed.*). Thousand Oaks: Sage Publications, Inc.

Drivers Privacy Protection Act (DPPA) of 1994, 18 U.S.C. § 2721 et seq.

Fair and Accurate Credit Transactions Act (FACTA) of 2003, 15 U.S.C. 1601 note.

Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g.

Fagnoni, C.M. (2006). *Social security numbers. More could be done to protect SSNs. Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives.* United States General Accounting Office. GAO-06-586T. Retrieved January 23, 2009 from http://www.gao.gov/new.items/d06586t.pdf

Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1601 note (1970).

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g

Federal Trade Commission. (2007, November). *Federal Trade Commission – 2006 identity theft survey report.* McLean, Virginia: Synovate. Retrieved March 12, 2009, from http://www.synovate.com

Federal Trade Commission. (2008, December). *Security in numbers: SSNs and ID theft.* Retrieved March 11, 2009, from http://www.iapp.com

Gramm-Leach-Bliley Act (GLBA), 12 U.S.C. 1811 note (1999).

Hendricks, E., Hayden, T., & Novik, J. (1990). *Your right to privacy: a basic guide to legal rights in an information society* (2nd ed.). Carbondale: Southern Illinois University Press.

Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d -- 1320d-8.

Interest and Dividend Tax Compliance Act of 1983 (26 U.S.C. 1).

Klosek, J. (2007). *The war on privacy*. Westport, Conn.: Praeger Publishers.

Kniffel, L. Delusions of privacy. (2008). *American Libraries*, 39(8), 4.

Kuhlthau, C.C. (1993a). A principle of uncertainty for information seeking. *Journal of Documentation*, 49(4), 339-355.

Kuhlthau, C.C. (1993b). Seeking meaning: A process approach to library and information services. Norwood, New Jersey: Ablex Publishing Corporation.

Marx, G.T. (1999). *Privacy and technology*. Retrieved December 7, 2008 from http://web.mit.edu/gtmarx/www/privantt.html

McKay v. Thompson, 226 F.3d 752 (2000).

Miller, A.R. (1971). *The assault on privacy.* Ann Arbor: The University of Michigan Press.

Nicoll, C., Prins, J.E.J. & van Dellen, M. J. M. (Ed.) (2003). *Digital anonymity and the law: Tensions and dimensions*. The Hague, The Netherlands: T.M.C. Asser Press.

Offices of Research and Education Accountability (2008, October). *Safeguarding social security numbers in Tennessee government records.* Retrieved February 19, 2009, from http://www.comptroller1.state.tn.us/OREA/PublicationDetails.aspx?ReportKey=bae7ced e-f804-4a1b-bc2b-b120a52c6929

Oregon requires firms to protect data. (2008). Information *Management Journal*, 42(2), 12.

Privacy Act of 1974 U.S.C. 552a note

Privacy Protection Study Commission (1977). *Personal privacy in an information society*. Washington, D.C.: U.S. Government Printing Office

Privacy Protection Study Commission (1977). *Technology and privacy*. Washington, D.C.: U.S. Government Printing Office

Protecting the privacy of consumers' social security numbers. 108th Cong., 2nd Sess. 3 (2004) (testimony of Janice D. Schakowsky and E. Clay Shaw, Jr.).

Shattuck, J.H.F. (1977). *Rights of privacy.* Skokie, Illinois: National Textbook Company.

Sheehan, K.B. Antecedents and effects of privacy concern among on-line consumers. (May 1998) (unpublished Ph.D. dissertation, University of Tennessee) (on file with John C. Hodges Library, University of Tennessee).

Social Security Administration. (2009a). *Your social security number and card*. (Publication No. 05-10002, ICN 451384).

Social Security Administration. (2009b). *Social security numbers for children*. (Publication No. 05-10023, ICN 454925).

Social security numbers in commerce: reconciling beneficial uses with threats to privacy. 109th. Cong., 2nd Sess. (2006) (testimony of Joe Barton).

.Solove, D. J. (2004). *The digital person: technology and privacy in the information age*. New York: New York University Press.

Solove, D. J. (2008a). *Understanding privacy*. Cambridge, Mass.: Harvard University Press.

Solove, D. J. (2008b). The future of privacy, *American Libraries*, 39(8), 56-59.

Stambaugh, J. J. (2009, December 30). Felons found in voter records. *News Sentinel*, 1, A7.

Strum, P. (1998). *Privacy, the debate in the United States since 1945*. Fort Worth, Texas: Harcourt Brace College Publishers.

Sue, V.M. & Ritter, L.A. (2007). *Conducting online surveys.* Thousand Oaks, Calif.: Sage Publications.

Tenn. Code Ann. art. IV, § 2

Tenn. Code Ann. § 2-2-124 (Supp. 2008)

Tenn. Code Ann. § 2-2-127 (2003)

Tenn. Code Ann. § 4-4-125 (Supp. 2008)

Tenn. Code Ann. § 10-7-513 (Supp. 2008)

Tenn. Code Ann. § 10-7-515 (Supp. 2008)

Tenn. Code Ann. § 34-1-109 (2007)

Tenn. Code Ann. § 36-5-1301 (2005)

Tenn. Code Ann. § 36-5-1302 (2005)

Tenn. Code Ann. § 39-14-150 (2006)

Tenn. Code Ann. § 47-18-2110 (Supp. 2008)

Tenn. Code Ann. § 55-50-321 (Supp. 2008)

Tenn. Code Ann. § 68-3-401 (Supp. 2008)

Tenn. Code Ann. § 68-3-402 (2007)

Tenn. Code Ann. § 68-3-502 (Supp. 2008)

Teeter, D.L. & Loving, B. (2008). *Law of mass communications: Freedom and control of print and broadcast media*. New York: Thomson Reuters/Foundation Press.

U.S. Const. amend. I

U.S. Const. amend. III

U.S. Const. amend. IV

U.S. Const. amend. V

U.S. Const. amend. IX

U.S. Const. amend. XIV

Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism Act (Patriot Act) of 2001 (18 U.S.C. 1 note 2001).

APPENDICES

Appendix A: Original Design of Social Security Card

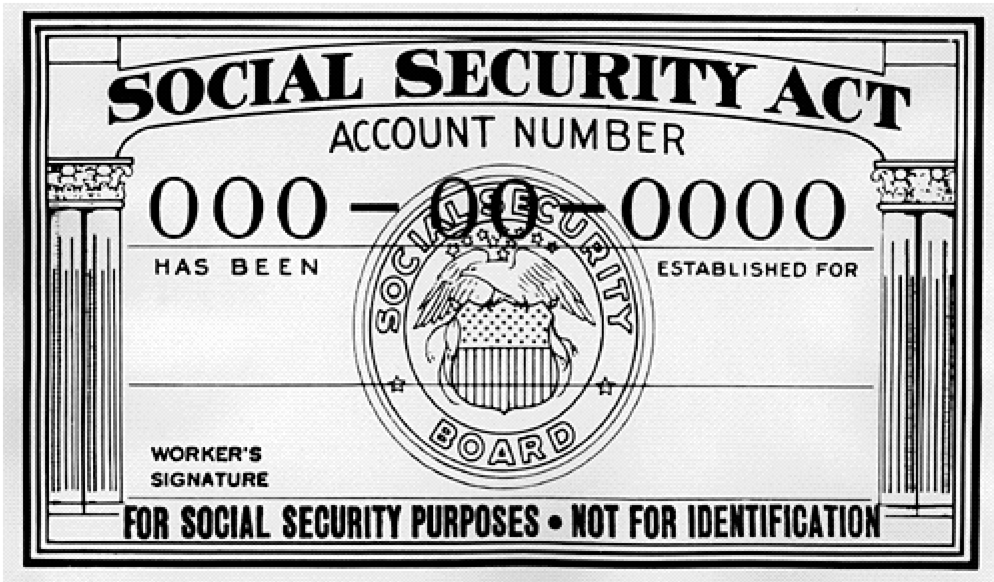

Figure 2: Original Design of Social Security Card
Retrieved October 7, 2009 from:
http://commons.wikimedia.org/wiki/Category:Social_Security_Administration

Appendix B: Selected Tennessee Social Security Number Laws

Tenn. Code Ann. § 2-2-116 (Supp. 2008). Title 2 Elections. Chapter 2, Voter registration Section 116, Registration form. Voter registration form must contain social security number, if any.

Tenn. Code Ann. § 2-2-124 (Supp. 2008) – Title 2 Elections--Chapter 2 Voter registration--Section 124--Registration card. Voter registration cards are not to contain SSNs.

Tenn. Code Ann. § 2-2-127 (2003) – Title 2 Elections--Chapter 2 Voter registration--Section 127--Permanent registration records open to inspection—Social security number redaction and use.--Registrar is to make reasonable efforts to redact social security number before the registration record is made public as voter registration cards are public records.

Tenn. Code Ann. § 4-4-125 (Supp. 2008) – Title 4 State Government--Chapter 4, Section 125--Dissemination of social security numbers**.** No state entity shall publicly disclose the social security number of any state citizen unless:

- Permission is given by such citizen;
- Distribution is authorized under state or federal law; or

Distribution is made:

- To a consumer reporting agency as defined by the federal Fair Credit Reporting Act,
- To a financial institution subject to the privacy provisions of the federal Gramm Leach Bliley Act; or

- To a financial institution subject to the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.

Tenn. Code Ann. § 10-7-513 (Supp. 2008) - Title 10, Public Libraries, Archives, and Records--Chapter 7, Public Records--Section 513, Request for removal of military discharge or redaction of social security number from military discharge. Veterans of United States armed forces may request in writing either the removal of military discharge record or redaction of social security number from discharge records.

Tenn. Code Ann. § 10-7-515 (Supp. 2008) – Title 10, Public Libraries, Archives, and Records--Chapter 7, Public Records--Section 515. Social security identification numbers on documents--Redaction. Social security identification numbers shall not be placed on any document filed or recorded in the office of the county register of deeds other than a power of attorney. A request for redaction of a social security number in the office of the county register of deeds must be made in writing. The request shall be made in electronic databases, as practicable.

Tenn. Code Ann. § 34-1-109 (2007) – Title 34 Guardianship--Chapter 1, Guardianships and Conservatorships Generally--Section 109--When fiduciary's appointment becomes effective – Evidence of appointment—Liability—Fiduciary oath. The social security number of respondent in matters pertaining to guardians for minors may be used in any other manner approved by the court. The court may release the social security number to a third party upon good cause shown and upon conditions that the court may deem appropriate.

Tenn. Code Ann. § 36-2-311 (2008) – Title 36 Domestic Relations—Chapter 2, Parentage—Section—Part 3—Paternity and Legitimation—Section 311, Order of parentage. Order of parentage shall include the social security numbers of mother, father and child.

Tenn. Code Ann. § 36-4-106 (2008) – Title 36 Domestic Relations—Chapter 4, Divorce and Annulment—Section 106, Contents of petition for divorce and legal separation. Social security numbers of husband and wife must be included on the complaint for divorce.

Tenn. Code Ann. § 36-1-126 (2008) – Title 36 Domestic Relations—Chapter 1 Adoption—Part 1—General Provisions, Section 126, Records kept under seal—Confidential records—Access to certain records. The sealed adoption record shall be registered by the department in such a manner as to record the names of the adopted person, the adopted person's birth name, the person's date of birth and social security number.

Tenn. Code Ann. § 36-5-1301 (2005) – Title 36 Domestic Relations--Chapter 5, Alimony and Child Support--Section 1301, Inclusion of social security numbers on certain licenses. All applications for professional licenses, driver licenses, occupational licenses, hunting and fishing licenses, recreational licenses, or marriage licenses issued by any agency or any political subdivision of the state of Tennessee shall contain the social security number of each applicant.

Tenn. Code Ann. § 36-5-1302 (2005) - Title 36 Domestic Relations--Chapter 5, Alimony and Child Support--Section 1302, Inclusion of social security numbers in certain records. The social security number of any individual who is subject to a divorce decree, order of support issued by any court, any order of paternity or legitimation, or any voluntary acknowledgment of paternity shall be placed in the records relating to such matter.

Tenn. Code Ann. § 39-14-150 (2006) – Title 39 Criminal Offenses--Chapter 14—Offenses Against Property--Part 1-Theft--Section 150--Identity Theft Victims Rights Act of 2004. The crime of identity theft is defined as occurring when a person knowingly obtains, possesses, buys or uses the personal identifying information of another.

Tenn. Code Ann. § 47-18-2110 (Supp. 2008) – Title 47 Commercial Instruments and Transactions.--Chapter 18 Consumer Protection--Part, 21—Identity Theft Deterrence, Section 2110, Protecting social security numbers from disclosure. Any person, nonprofit, or for profit business entity in this state … that has obtained a federal social security number for a legitimate business or governmental purpose shall make reasonable efforts to protect that social security number from disclosure to the public.

Tenn. Code Ann. § 55-50-321 (Supp. 2008) – Title 55 Motor and Other Vehicles--Chapter 50--Uniform Classified and Commercial Driver License Act--Part 3, Application, Examination, and Issuance--Section 321--Applications. Social security numbers must be included on application for license.

Tenn. Code Ann. § 68-3-401 (Supp. 2008) – Title 68 Health, Safety and Environmental Protection Health--Chapter 3 Vital Records--Part 4—Marriages, Annulments and Divorces.--Section 401--Marriage registration. Social security number must be included on certificate of marriage.

Tenn. Code Ann. § 68-3-402 (2007) –Title 68 Health, Safety and Environmental Protection Health. Chapter 3 Vital Records--Part 4—Marriages, Annulments and Divorces--Section 402--Divorce, dissolution of marriage, and annulment—Registration. For each divorce, dissolution of marriage, or annulment granted, the social security number shall be recorded on the certificate.

Tenn. Code Ann. § 68-3-502 (Supp. 2008) – Title 68 Health, Safety and Environmental Protection Health. Chapter 3 Vital Records--Part 5--Death registration. The form for a certificate of death shall contain the social security number of the deceased.

Appendix C: U.S. Government Accountability Office (GAO) Reports

1. Report by the comptroller general of the United States: Reissuing tamper-resistant cards will not eliminate misuse of social security numbers. HRD-81-20, 114062 (1980).
2. Report by the comptroller general of the United States: Eligibility verification and privacy in federal benefit programs: A delicate balance. GAO/HRD-85-22, 126333 (1985).
3. Social security: Government and commercial use of the social security number is widespread. GAO-HEHS-99-28 (1999).
4. Social security numbers: Subcommittee questions concerning the use of the number for purposes not related to social security. GAO/HEHS/AIMD-00-253R (2000).
5. Identity fraud: Prevalence and links to alien illegal activities. GAO-02-830T (2002).
6. Social security numbers: SSNs are widely used by government and could be better protected. GAO-02-691T (2002).
7. Social security numbers: Ensuring the integrity of the SSN. GAO-03-920 (2003).
8. Improved SSN verification and exchange of states' driver records would enhance identity verification. GAO-03-920 (2003).
9. Information security: Progress made, but weaknesses at the Internal Revenue Service continue to pose risks. GAO-03-44 (2003).
10. Social security numbers: Governments could do more to reduce display in public records and on identity cards. GAO-05-59 (2004).
11. Social security numbers: Private sector entities routinely obtain and use SSNs, and laws limit the disclosure of this information. GAO-04-11 (2004).

12. Social security numbers: Federal and state laws restrict use of SSNs, yet gaps remain. GAO-05-1016T (2005).
13. Information security: Despite reported progress, federal agencies need to address persistent weaknesses. GAO-07-837 (2007).
14. Information security: Protecting personally identifiable information. GAO-08-343 (2008).
15. Information security: Agencies make progress in implementation of requirements, but significant weaknesses persist. GAO-09-701T (2009).
16. Internal Revenue Service: Physical security over taxpayer receipts and data needs improvement. GAO/AIMD-99-15 (1998).
17. Personal information: Data breaches are frequent, but evidence of resulting identity theft is limited: however, the full extent is unknown. GAO-07-737 (2007).
18. Social security numbers: More could be done to protect SSNs. GAO-07-586T (2006).
19. Privacy: Lessons learned about data breach notification. GAO-07-657 (2007).
20. Identity fraud: Information on prevalence, cost, and internet impact is limited. GAO/GGD-98-100BR (1998).
21. Social security numbers: Use is widespread and protection could be improved. GAO-07-1023T (2007).
22. Social security numbers: Federal actions could further decrease availability in public records, though other vulnerabilities remain. GAO-07-752 (2007).
23. Social security numbers: Stronger protections needed when contractors have access to SSNs. GAO-06-238 (2006).

24. Social security numbers are widely available in bulk and online records, but changes to enhance security are occurring, GAO-08-1009R (2008).

25. Social security administration: Improved agency coordination needed for social security card enhancement effort, GAO-06-303 (2006).

26. Social security numbers: Internet resellers provide few full SSNs, but Congress should consider enacting standards for truncating SSNs. GAO-06-495 (2006).

27. Privacy: Preventing and responding to improper disclosures of personal information. GAO-06-833T (2006).

28. Cybercrime: Public and private entities face challenges in addressing cyber threats. GAO-07-705 (2007).

29. Employment verification: Challenges exist in implementing a mandatory electronic employment verification system. GAO-08-729T (2008).

30. Identity Theft: Prevalence and cost appear to be growing. GAO-02-363 (2002).

Appendix D: Google Social Security Number Search Results

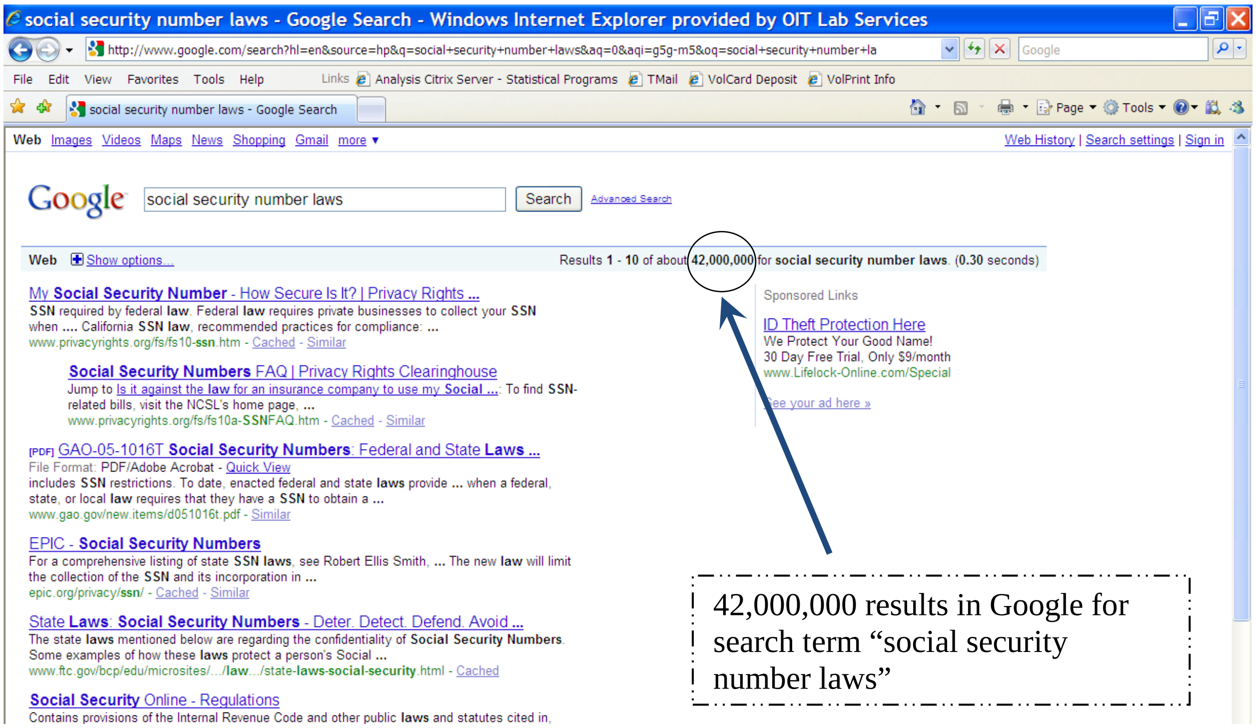

Figure 3: Google search for social security number laws
Accessed February 13, 2010

Appendix E: Dervin's 10 Dubious Assumptions about Information and Information Seeking

1. Only 'objective' information is valuable.	“For most tasks and decisions in life, people tend to settle for the first satisfactory solution to a problem, rather than the best solution.”
2. More information is always better.	“Typically there is not a problem getting enough information but rather with interpreting and understanding what information there is.”
3. Objective information can be transmitted out of context.	"But people tend to ignore isolated facts when they cannot form a complete picture of them.”
4. Information can only be acquired through formal sources.	“This assumption, often made by those in educational institutions, flies in the face of actual behavior.”
5. There is relevant information for every need.	“The truth is that mere information cannot satisfy many human needs.”
6 Every need situation has a solution.	“But sometimes the client is looking for something – a reassurance, and understanding – that does not come in the shape of a canned response.”
7. It is always possible to make information available or accessible.	“Formal information systems are limited in what they can accomplish, at least where the vague, ambiguous, and constantly changing needs of the public are concerned.”
8. Functional units of information, such as books or TV programs, always fit the needs of the individual.	“But the 'functional units' of the individual are not often these things; rather, they are responses, solutions, instructions, ideas, friendships, and so forth.”
9. Time and space – individual situations – can be ignored in addressing information seeking and use.	“Yet it is often the individual's definition of the situation that shapes his or her needs as much as the 'real' situation itself.”
10. People make easy, conflict-free connections between external information and their internal reality.	“We lack understanding about how people inform themselves, how they make connections over time, the sense they make of their world between significant events.”

Appendix F: Survey Instrument

Uses of the Social Security Number

This survey of 22 questions asks you about the use of the Social Security Number (SSN) for identification and authentication purposes in public and private agencies. The survey will take approximately 15 - 20 minutes to complete. Please indicate your responses by clicking on your chosen answer or entering text when indicated. You may choose not to answer a question or to discontinue the survey at any time. At the conclusion of the survey, you are invited to enter a drawing for an Amazon.com gift card in the amount of $50. Please take the survey only once.

CONSENT

Consent Form

Thank you for participating in this study of the uses of Social Security Numbers in public and private databases. Please read the following information before proceeding. This survey is part of a thesis research project in the School of Information Sciences at the University of Tennessee. The purpose of the research is to learn about your thoughts on the use of the Social Security Number for identification and authentication purposes in public and private agencies. The questions should take approximately 15 - 20 minutes to complete. There is minimal risk to you for participating, as your identity will remain unknown to the investigator. Your participation will help to further research by contributing to the field of knowledge of other researchers and practitioners. By consenting to participate, you acknowledge that findings may be published. Published findings will not identify you in any way since data is collected and analyzed in the aggregate. Responses to the survey are confidential and anonymous. After you submit your completed survey, you are invited to enter a drawing to win a $50 online gift card from Amazon.com. Entering the drawing is completely voluntary. You will be asked to provide your email address, which will not be stored with your survey responses. If you have any questions regarding this study, please contact the researcher at rclossum@utk.edu. Questions pertaining to study participation should be directed to the Institutional Review Board (IRB) Administrator at (865) 974-7697. Participation in this study is completely voluntary and may be discontinued at any time during the survey without loss of benefits to which you are otherwise entitled. All Participants must be 18 years of age or older. If you are less than age 18, you are not permitted to participate in this study.

O Yes, I am 18 years old or older and I wish to continue
O No, I do not wish to continue

STATE

1. In which state do you reside?

O Please select your state:
O Alabama
O Alaska
O Arizona
O Arkansas
O California
O Colorado
O Connecticut
O Delaware
O District of Columbia
O Florida
O Georgia
O Hawaii
O Idaho
O Illinois
O Indiana
O Iowa
O Kansas
O Kentucky
O Louisiana
O Maine
O Maryland
O Massachusetts
O Michigan
O Minnesota
O Mississippi
O Missouri
O Montana
O Nebraska
O Nevada
O New Hampshire
O New Jersey
O New Mexico
O New York
O North Carolina
O North Dakota
O Ohio
O Oklahoma
O Oregon
O Pennsylvania
O Rhode Island
O South Carolina
O South Dakota

O Tennessee
O Texas
O Utah
O Vermont
O Virginia
O Washington
O West Virginia
O Wisconsin
O Wyoming

SSN

2. Indicate how much you disagree or agree with each of these statements. Do you strongly disagree, disagree, agree, or strongly agree? Also, you may answer that you don't know.

	Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
If my Social Security Number (SSN) is used by another person without my consent, I can obtain another SSN.	O	O	O	O	O
Utility companies (electricity, sewer, water, gas, etc.) can charge a deposit fee if I refuse to provide my SSN	O	O	O	O	O
For consumer transactions, federal law requires consumer identity authentication (proof of identity) only in the financial sector (banks, credit unions, investment firms, etc.)	O	O	O	O	O
The USA PATRIOT Act requires that I provide my SSN to obtain internet service.	O	O	O	O	O

TN
2.A.The following questions focus on laws in Tennessee. Once again, indicate how much you disagree or agree with each of these statements.

	Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
According to Tennessee State law, an application for a commercial driver's license requires disclosure of the Social Security Number (SSN).	O	O	O	O	O
According to Tennessee State law, death certificates require the disclosure of the deceased's SSN.	O	O	O	O	O
Tennessee state law requires the disclosure of the SSN of a state scholarship recipient	O	O	O	O	O

RECORDS

2.B. For each of the items below, please indicate if Tennessee state law requires the Social Security Number (SSN).

	Yes	No	Don't Know
Divorce decree	O	O	O
Paternity record	O	O	O
Fishing license	O	O	O
Military discharge record	O	O	O
Marriage license	O	O	O

FEDERAL

3. The next set of questions asks about federal Social Security Number (SSN) laws. For each question, tell us if you think it is never true, sometimes true, always true or if you are not sure.

	Never	Yes, sometimes	Yes, always	Not sure
By federal law, yearly credit reports are available free of charge to everyone with a SSN.	O	O	O	O
Notification of privacy policy must be given in writing to all customers of financial institutions.	O	O	O	O
The USA PATRIOT Act requires that I provide my SSN to obtain lottery winnings.	O	O	O	O

Federal government agencies can legally refuse to grant services if I refuse to provide my SSN.	O	O	O	O
Retail businesses can legally refuse goods or services if I decline to provide my SSN.	O	O	O	O

CIRCUMST1

4. In each of these circumstances, are you required to disclose your SSN? For each question, please tell us if you think it is never true, sometimes true, always true or if you are not sure.

	Never	Yes, sometimes	Yes, always	Not sure
Applying for a library card	O	O	O	O
Establishing a bank account	O	O	O	O
Applying for credit	O	O	O	O
Receiving medical or dental services at a private office	O	O	O	O
Receiving medical or dental services at a public agency	O	O	O	O

INSURANCE

5. Federal law requires that I disclose my SSN to obtain the following types of insurance. For each question, please tell us if you think it is never true, sometimes true, always true or if you are not sure.

	Never	Yes, sometimes	Yes, always	Not sure
Medical Insurance	O	O	O	O
Life Insurance	O	O	O	O
Automobile Insurance	O	O	O	O
Home or Renter's Insurance	O	O	O	O
Business Insurance	O	O	O	O

IDENTITY

6. How likely are you to feel threatened by identity theft if you disclose your SSN in each of the following activities?

	Very unlikely	Unlikely	Likely	Very likely	Don’t know
Online transactions	O	O	O	O	O
Health care offices	O	O	O	O	O
Schools	O	O	O	O	O
Financial institutions (banks, credit unions, investment firms)	O	O	O	O	O
Government offices	O	O	O	O	O

PROTECT

7. For each of these types of organizations, how likely is each organization to protect your SSN?

	Very unlikely	Unlikely	Likely	Very likely	Don’t know
Retail stores	O	O	O	O	O
Utility companies (electricity, sewer, water, gas, etc.)	O	O	O	O	O
Cell phone companies	O	O	O	O	O
Financial institutions (banks, credit unions, investment firms, etc.)	O	O	O	O	O
Government agencies	O	O	O	O	O

CIRCUMST2

8. In each of the following circumstances, how likely would you be to provide your SSN if asked by the service provider?

	Very unlikely	Unlikely	Likely	Very likely	Don’t know
Applying for a library card	O	O	O	O	O
Establishing a bank account	O	O	O	O	O
Applying for credit	O	O	O	O	O
Receiving medical or dental services at a private office	O	O	O	O	O
Receiving medical or dental services at a public agency	O	O	O	O	O

FIND_INFO

9. Now, we'll ask a few questions about how you find information about privacy or privacy laws.

Have you ever searched for:

	Yes	No
Information about privacy in general	O	O
Government policies on the requirements to disclose your SSN	O	O
Federal or state laws on the requirements to provide your SSN	O	O

SOURCES

10. How likely are you to use each of these sources to find information on legal requirements to provide your SSN?

	Very unlikely	Unlikely	Likely	Very likely
Public library	O	O	O	O
Blog	O	O	O	O
Government office or website (such as Social Security Administration; Federal Trade Commission; or State Attorney General)	O	O	O	O
Search engine such as Google or Yahoo	O	O	O	O
Friend	O	O	O	O

OTHER_SOURCES

11. Please list any other sources you may use to find information on legal requirements to provide your SSN. (optional)

____

____

____

____

SEARCHING

12. There are many reasons why someone might avoid searching for information or laws about providing an SSN. Please indicate how strongly you disagree or agree that each of these reasons affects searching.

Someone may avoid looking for privacy information or privacy laws because:

	Strongly Disagree	Disagree	Agree	Strongly Agree	Don't Know
They don't know where to look	O	O	O	O	O
They trust the government agencies, businesses or people that are given their SSN	O	O	O	O	O
They feel a lack of control over who has access to their SSN	O	O	O	O	O
They may feel intimidated	O	O	O	O	O

ANY_CONCERN

13. Do you have any concerns about disclosing your SSN?

O Yes
O No

RANK_CONCERN

14. Which of the following concerns do you have about disclosing your SSN?

	Slight concern	Moderate concern	High concern
Threat of identity theft	O	O	O
Denial of services if I refuse to disclose my SSN	O	O	O
Violation of my right to privacy	O	O	O

OTHER_CONCERN

15. What other reasons do you have for not wanting to disclose your SSN? (optional)

____

____

____

____

CONCERN

16. Overall, how would you rate your concern over your disclosure of your SSN? Following each category of concern are examples that may or may not apply to you. Please choose the category that best describes your beliefs.

O **Extreme Concern** - Refrain from disclosing to government agencies, private agencies or online which sometimes limits my acquiring a new bank account, obtaining government benefits or making retail purchases

O **Moderate Concern** - Use last four-digits of SSN only for identification or verification; provide SSN on secure websites

O **Average Concern** - Do not carry SSN in wallet but provide SSN to retailers and online to apply for credit

O **Slight Concern** - Carry social security card in wallet but do not write SSN on checks

O **No Concern** - Carry SSN in wallet; write SSN on checks

GENDER

17. What is your gender?

O Male
O Female

AGE

18. What is your age?

EDUCATION

19. What is your highest level of education achieved?

O Some High School
O High School or GED
O Some College
O Two-year Certificate or Technical Degree
O Bachelor's Degree
O Master's Degree
O Doctorate or other Professional Degree

CAREER3

20. What is your field of employment?

O Arts and Entertainment
O Accounting
O Administrative & Clerical
O Architecture or Design
O Agriculture
O Banking & Finance
O Communication
O Education
O Engineering
O Government
O Health Care
O Hospitality
O Information Technology
O Legal
O Library & Information Services
O Manufacturing
O Sales & Marketing
O Science & Biotechnology
O Social Work
O Student
O Transportation
O Other: ______________________________

STUDY

21. What is your area of study?

____

____

____

____

COMMENTS

22. Is there anything else you would like to tell us? (optional)

____

____

____

____

Uses of the Social Security Number - Email

EMAIL

By completing the survey, you have been qualified to enter a drawing for a $50 gift card to Amazon.com If you wish to enter, please provide an email address: *Email addresses will only be used to contact the winner and will not be used in combination with data or for any other purposes.*

____

____

Appendix G: Research Variables

Table 28: Research Variables

Research Questions	Survey Variable Name	Survey Item Number
Awareness What are the levels of awareness of federal and state of Tennessee privacy laws pertaining to Social Security Numbers?	SSN, TN, RECORDS, FEDERAL, CIRCUMST1, INSURANCE	See Questions 2, 2.A, 2.B, 3, 4, and 5
Concern What are the levels of concern pertaining to the disclosure of one's Social Security Number?	IDENTITY, PROTECT, CIRCUMST2, CONCERN	See Questions 6, 7, 8, 13, 14, 15 and 16
Information Seeking What sources are used to find information on laws pertaining to the disclosure of the Social Security Numbers?	FIND_INFO, SOURCES, OTHER_SOURCES, SEARCHING	See Questions 9, 10, 11 and 12
Demographic Data This information is descriptive of the participants in the study.	STATE, GENDER, AGE, EDUCATION, CAREER3, STUDY	See Questions 1, 17, 18, 19, 20, 21
Comments Additional comments are solicited for further illumination and opinions regarding survey	COMMENTS	See Question 22

Appendix H: Definition of Terms

Awareness – being mindful or heedful; having knowledge of something (*Webster's ninth new collegiate dictionary*, 1984).

Concern – to be a care, trouble or distress to; worry, solicitude, or anxiety; matter that engages a person's attention, interest, or care, or that affects a person's welfare or happiness (*Webster's ninth new collegiate dictionary*, 1984).

Identity Theft – the crime of using personal information of another including name, date of birth and social security number for the purpose of making unauthorized financial transactions or obtaining other benefits by assuming another's identity (*Security in Numbers: SSNs and ID Theft*, 2008).

Information – cumulative data that has been organized and communicated. Information is needed to resolve an uncertainty and is necessary to make a decision (Case, 2007).

Information Privacy – the legal and political relationship between collection and dissemination of personal data (Hendricks, 1990).

Information Security – the protecting of information and information systems from unauthorized access, use, disclosure, modification or destruction. (44 U.S.C. § 3542(b)(1).

Privacy – the right to exercise control over information about oneself (Shattuck, 1977); the freedom to decide whether to share personal information (Hendricks, 1990).

Privacy Literacy – ability to find and understand information about privacy in order to make informed decisions pertaining to one's personal information.

VITA

Rhonda Marisa Clossum is completing coursework for a Master of Science in Information Sciences degree at the University of Tennessee. She is pursuing a career in information privacy.