2021-8

Personal Data Privacy and Protective Federal Legislation: An Exploration of Constituent Position on the Need for Legislation to Control Data Reliant Organizations Collecting and Monetizing Internet-Obtained Personal Data

Giovanni De Meo
University of San Diego

PERSONAL DATA PRIVACY AND PROTECTIVE FEDERAL LEGISLATION: AN EXPLORATION OF CONSTITUENT POSITIONS ON THE NEED FOR LEGISLATION TO CONTROL DATA RELIANT ORGANIZATIONS COLLECTING AND MONETIZING INTERNET-OBTAINED PERSONAL DATA

by

Giovanni Stephen De Meo

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

May 2021

Dissertation Committee

Fred Galloway, EdD

Robert Donmoyer, PhD

Marcus Lam, PhD

University of San Diego

University of San Diego

School of Leadership and Education Sciences

CANDIDATE'S NAME: Giovanni Stephen De Meo

TITLE OF DISSERTATION: PERSONAL DATA PRIVACY AND PROTECTIVE FEDERAL LEGISLATION: AN EXPLORATION OF CONSTITUENT POSITIONS ON THE NEED FOR LEGISLATION TO CONTROL DATA RELIANT ORGANIZATIONS COLLECTING AND MONETIZING INTERNET-OBTAINED PERSONAL DATA

APPROVAL:

_____, Chair

First Name Last Name, PhD

_____, Member

First Name Last Name, PhD

_____, Member

First Name Last Name, PhD

DATE:

ABSTRACT

In the past twenty years, the business of online personal data collection has grown at the same rapid pace as the internet itself, fostering a multibillion-dollar personal data collection and commercialization industry. Unlike many other large industries, there has been no major federal legislation enacted to monitor or control the activities of organizations dealing in this flourishing industry. The combination of these factors together with the lack of prior research encouraged this research designed to understand how much voters know about this topic and whether there is interest in seeing legislation enacted to protect individual personal data privacy.

To address the gap in research, and to gain deeper insight into constituent feelings on the topic, a 43-question closed-end survey instrument was created to gather demographic data from respondents and to assess individual sentiments in four construct areas: awareness, knowledge, concern, and desire. Based on a sample of 892 registered Democratic and Republican voters from California, Florida, New York, Texas, Ohio, and Georgia, descriptive statistics revealed high levels of awareness, concern, and desire among respondents, although low levels of knowledge, with 79% of participants demonstrating a poor to basic level of knowledge about existing data privacy legislation. When stepwise regression techniques were used to understand the extent to which demographic factors explained variation in the four constructs, age, race, education, location, and/or gender played some role in explaining variation in most of the constructs, although political affiliation was never a statistically significant factor. For example, higher levels of educational attainment were associated with increased levels of awareness, as was identifying as male and white; however, age was negatively associated with awareness. In another finding, identifying as white was associated with lower levels of concern, while age was positively correlated with higher levels of concern. Taken together, the construct regressions explained between 2% and 5% of the variation, suggesting the existence of other unexplored factors.

The opportunity to use this research extends to individuals, legislators and businesses operating in the data collection industry. Based on the results, it appears that individuals identify protection as important and further exploration could be highly valuable.

DEDICATION

I would like to dedicate this dissertation, and my success in all things, to my family. To my father, the greatest man I have ever known, who was my biggest supporter and allowed me to believe that I could accomplish anything that I wanted to in life. To my older sister who always made me feel successful regardless of my many failures. To my brother who has shown me that no matter how difficult life might be, you can always triumph and be a better person. To my younger sister who encouraged me to always be better. To my incredible wife and the love of my life, who has made me be a much better man. My wife, who is truly the kindest and most generous person I have ever had the privilege of knowing, has both encouraged and supported me in the most positive ways possible throughout this entire experience. And to my most precious daughter, for whom I want to be the best possible person I can be. My daughter, who has brought a depth of love into my heart that I could not have even conceived of before her birth, and who makes me want to be the best person I can be, I made sure that I completed this journey to set an example of possibilities, achievements, and love.

I wish I could say that I did this on my own, but if not for all of my supporters, and even my detractors, I would not have had the strength or resolve to see this through to the end. My greatest thanks and love to each and every one of you.

ACKNOWLEDGEMENTS

It may not be terribly original, but I would like to begin by expressing my deepest and sincerest appreciation to my dissertation chair, Professor Fred J. Galloway. Without his scholarship, support, encouragement, guidance, input, and most of all, friendship, I would not have been able to complete this incredible journey.

In addition, I would like to thank my two committee members, Professor Robert Donmoyer and Professor Marcus Lam, whose commitment to supporting me in this process was clearly demonstrated in their diligence in review, comment, and constructive criticisms of this paper. Their commitment to academic excellence and student success is noteworthy.

ORDER OF PAGES

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION AND BACKGROUND

The digital age has brought with it incredible change and access to knowledge unmatched in human history. Ironically, it has also brought with it great obfuscation in the areas of generating, collecting, and commercializing personally identifiable information (PII). As we enter a future that is virtually inseparable from technology, connectivity, mobility, and the internet-of-things, we are generating immense amounts of personal data that detail almost everything about us. As with most large scale and explosive societal phenomena, entire industries or business practices within industries have emerged to leverage these large-scale changes; one such industry centers around the collection and commercialization of individuals' personal data by data reliant organizations (DROs). These organizations generate some or all of their revenue from the commercialization of PII.

Most people in the U.S. have no idea the extent to which DROs are gathering personal data and building distinct profiles about almost every individual in the country (Federal Trade Commission, 2014; Kroft, 2014; Ramirez & Brill, 2014). Equally unknown are how accurate the profiles are that these DROs are generating, what they say about us, exactly what information is being collected and compiled, and how that highly personal data is ultimately being used.

Imagine a society in which everything you do, the places you go, who you speak to, what you watch on television, who you send emails to and what you write in each email, what you buy (and don't buy), how often you drink alcohol or eat high cholesterol foods, which websites you visit, what you have for lunch (yes, including that doughnut), and even how much you weigh, can be tracked by an unknown entity or entities. Then, without your knowledge or consent, all this personal data that you would never knowingly share publicly, is brought together, combined with other datasets of information about your personal activities and history, and is analyzed using advanced algorithms to produce a profile about

you. This profile not only groups you into clusters based on things like race, income, health issues, and sexual orientation (Boutin, 2016), but the algorithms also predict future actions, likes and dislikes, predilections and propensities, and even your thoughts.

This new personal profile about you is not accessible or available to you (even if, for some unlikely reason, you were aware of its existence); it is held secretly by one or more private companies, and any mistakes or inaccuracies about you and who you are as a person go unchecked and uncorrected. However, even in the presence of what might be severely inaccurate information about you, your profile is bought and sold repeatedly, many times being enhanced with new personal data that may or may not be accurate, before being resold or stored for some unknown future use. And to add the proverbial cherry on top, imagine that the United States (U.S.) federal government purchases these profiles and uses them to build their own database about you (Gellman & Dixon, 2013).

This scenario may sound like a dystopian society directly out of a George Orwell novel, but it is, in fact, occurring every single day in the U.S. However, this is not something to worry about, unless you are a part of the population that has a cell phone, uses the internet, shops at a supermarket, owns or rents a home or apartment, drives a car or takes public transportation, watches cable television, has a job, pays taxes, has a social security number, or was born in a public or private medical facility. If you fall into one or more of those groups, then you likely have a profile in one or more DRO databases (Federal Trade Commission, 2014).

Much like the consistency between large societal changes and the emergence of industries to profit from those changes, in U.S. history there has also been consistency between large scale societal changes and the enacting of federal legislation to protect citizens from abuses by possibly unscrupulous individuals or organizations. One of the more interesting facts about the internet explosion, however, is the almost total absence of recent and relevant federal legislation to monitor or control the activities of

organizations operating in the area of data commercialization. This is not to say that no federal legislation has even been enacted to protect personal data, but the legislation that has been enacted was either done decades ago, or it is only for a tiny subset/business sector when considering the immense amount of data being collected.

There have been four federal acts passed to protect personal data privacy. Unfortunately, all four could be classified as vintage legislation, given that they are each more than 20 years old. The three federal laws that are more widely known include legislation to monitor the credit reporting industry (Fair Credit Reporting Act, 2012) and the healthcare industry (*HIPAA History*, n.d.), as well as oversight of data collected from children under 13 years of age (*Children's Online Privacy Protection Rule (COPPA) | Federal Trade Commission*, 1998). These acts are 51, 25, and 23 years old, respectively. In fact, these three acts were all proposed and enacted before much of the business activities surrounding data commercialization were even possible.

The fourth and most recent federal law passed was the Gramm-Leach-Bliley Act. This act focuses exclusively on the financial industry and was passed 22 years ago in 1999 (Gramm-Leach-Bliley Act, 2010). Therefore, exclusive of those companies operating in health care, public finance, and credit reporting, or anyone collecting data from children under 13 years of age, there is no federal legislation in place to ensure that individual citizens' data is kept private, that individual profiles contain correct and accurate information, and that data is protected against abuses by individuals or DROs that collect and commercialize personal data.

In an effort to continue to limit federal oversight outside the current (less-than-adequately) regulated industries, a group of several of the world's largest companies with some of the highest market capitalization values on the planet (Apple, Google, Facebook, Amazon, Comcast, and AT&T) are actively lobbying the federal government to minimize legislative oversight of DRO's collection and

commercialization of personal data (Guynn, 2018). And although the noninvolvement position taken by the federal government thus far may seem contrary to what constituents would likely want, there is no independent data to determine true public opinion on this matter. It is this lack of knowledge about the public's opinion on the topic of the importance and/or need for federal legislation to monitor and control the collection and commercialization of PII that prompted the research that is represented here.

Before discussing the results of this research, however, I should acknowledge that the claim that there has been absolutely no federal actions taken relating to personal data privacy may be somewhat misleading. In April of 2017, Congress repealed the only federal regulation enacted in the past 20+ years to protect internet consumer privacy and data (Congressional Review Act, 2001; A Joint Resolution Providing for Congressional Disapproval, 2017). In what appeared to be direct opposition to protecting personal data privacy, Congress not only repealed the Federal Communications Commission's (FCC) most recent attempts to create regulations to protect individual consumers' data; it also enacted new legislation allowing internet service providers (ISPs) and telecommunications companies to sell user data without specific consent from individuals (A Joint Resolution Providing for Congressional Disapproval, 2017) .

Personal data is widely considered one of the fastest growing global asset classes (World Economic Forum, 2014) and has been touted as "the new oil of the internet and the new currency of the digital world" (Betz, 2011). And yet, even with the apparent value and importance of personal data, there is no U.S. federal legislation in place to control how personal information is collected and managed by DROs. In direct contrast to the nonexistent legislation pertaining to the monitoring and controlling of data being collected and commercialized by DROs, there has been significant legislation enacted to monitor and limit the data collected, stored, and used by government entities, agencies, and their affiliates (Federal Trade Commission, 2014).

Equally concerning, and in direct contrast to the legislation for how credit reports are controlled, there is no legal structure in place to ensure individuals have access to the profiles that are generated about them by data collectors and brokers, and no mandated process to allow individuals to review those profiles for accuracy or request changes to inaccuracies (Federal Trade Commission, 2014). For the purposes of this study, the term Data Broker was used to refer to any privately held or publicly traded company that collects personal information about adult individuals (from both online and offline sources) and then sells that information to others (individuals, companies, or governments). Data Brokers include those organizations whose primary business is collecting and selling data, as well as those organizations whose primary business is something other than personal data sales with the selling of personal data as an ancillary business. The term Data Collector was used to describe any privately held or publicly traded company that collects personal information about adult individuals (from both online and offline sources) and uses that information to sell ad space on their websites.

The collection and resale of personal data on its own is not inherently bad. The real question is whether, due to the incredibly private nature of what is being collected, there is a need for the federal government to step in and ensure that this sensitive data is not being inappropriately collected and/or used?

Statement of the Problem

The U.S. system of democracy is built upon a structure of representative government. This structure is the cornerstone of our political system because it allows for the election of individuals who are tasked with the responsibility of representing all constituents from the state or district where they are from. This is done through the drafting, supporting, and opposing of public policy that is deemed to be in the best interest of their constituents. To achieve this objective, the elected individuals should ideally first know what their constituents identify as most important and what position those constituents want

their representatives to take on the topic. One such topic is whether creating legislation to monitor and control the collection and monetization of individual citizens' personally identifiable information by DROs is important and necessary. Simply stated, the problem is that (as of the drafting of this document) there have been no known studies dedicated to discovering the opinions of constituents' around their desire for federal legislation to monitor and control the activities of DROs, and only one reliable study conducted that included two questions related to understanding the opinions and wishes of the public as they relate to the importance of enacting legislation in this area (Turow, 2010).[1] The lack of prior research in this area does not indicate that the subject is not important, or that a deeper knowledge in this area could be of value. It is more likely that necessity for the research and the significance of the activity have finally aligned to precipitate the activity of this research.

Embedded in this problem is the secondary issue: legislators do not have access to data that provides details on the level of importance that U.S. citizens place on increasing control over personal data commercialization. This means that legislators will find it difficult to take a position on the topic that is aligned with their constituency since no such data is available to inform legislators on the opinion of constituents. Presumably, this could be why very few representatives have taken a public position on this topic. As a result, constituents concerned about this issue would struggle to find out what position

[1] An exhaustive literature review was conducted between January 2015 and May 2020 looking at databases including, but not limited to: Academic Search Premier, EconLit, Business Source Premier, Communication & Mass Media Complete, Communication Source, Military & Government Collection, SocINDEX with Full Text, Sage Premier, Wiley InterScience, and Google Scholar. Some of the search terms used included, but are not limited to: (data collection or data collector or data broker) AND (privacy or confidentiality or security) AND personal data AND (perceptions or attitudes or opinion) AND (legislation or laws or regulation or policy), (information privacy or data collection or data broker) AND (mobile app or mobile device) AND (legislation or policy), Security or Privacy Americans Concerned of Fed Phone, Internet Surveillance, Personally Identifiable Information, Personal Privacy AND Legislation, Privacy AND Legislation.

legislators are taking on this topic and how involved legislators are in lobbying for or against legislation to oversee the activities of the data brokerage industry.

Purpose of the Study

In the United States, the collection and sale of personal data is an industry that is leading the way in internet company growth. However, the monitoring and control of that industry is still in its infancy and questions regarding who should be responsible for oversight of organizations trafficking in PII has yet to be resolved. Presently, efforts to prevent abuses by possibly unscrupulous DROs ultimately falls to one or more of the following three groups: the individual consumer whose data is being collected, DROs participating in the collection and commercialization of the data, and state and/or federal governments.

Considering the depth, detail, and pervasiveness of data collection, it is reasonable to say that individual consumers are not widely aware of how much information is being collected about them, what is being done with that information (Federal Trade Commission, 2014; Somerville, 2017), what mechanisms drive the financial operations of the internet (Popken, 2018), or how they are personally being impacted by these mechanisms. Data brokers, who are represented by some of the strongest lobbying entities in Washington (Guynn, 2018), are currently operating in an environment that has little to no oversight, allowing them the freedom to maximize company growth while minimizing investments in data security, portals that allow individuals access to their own profiles, customer service resources that would provide individuals the opportunity to contest and correct inaccuracies, and a variety of other high-cost resources that are imposed on other industries, such as credit, medical, and finance.

To compound the challenge of lack of oversight, the governing bodies that can and would have responsibility for ensuring individual privacy rights are still battling the internal struggles of self-education, the strength of lobbyists opposed to regulation, and the question of whether government regulation is something that individuals need and want (Federal Trade Commission, 2014).

It is the combination of these factors that creates the problem of limited understanding about what direction the U.S. government is moving, in terms of creating government regulations surrounding personal data transparency and control. This study's purpose is to gain greater insight into the position of voters regarding the topic of the passing of federal legislation to monitor and control the collection and commercialization of PII gathered from internet activity of adults. At this point, the future of personal data privacy regulation is unclear at best. And it is this lack of clarity that plainly identifies a need to gain a greater understanding of the current position of constituents, knowledge which will help guide legislators in determining the appropriate legislative direction.

In this study I specifically focused on data that is generated or collected from cell phones, personal computers, or tablets connected to the internet. These are not the only places that personal data can be collected from, but because they constitute the majority of individual online connectivity, they were chosen as the basis for this study (U.S. households with PC/computer at home, 2015; Demographics of Internet and Home Broadband Usage, 2018; Demographics of Mobile Device Ownership and Adoption, 2018; Ryan, 2018). Data generated or collected from these devices can occur while the device is *actively* engaged by a user or while the device is *dormant* and not engaged by any user. This means that a device has two states of existence: *active* or *dormant*. In addition, the connectivity to the internet can occur using one of two methods. The first method of connectivity occurs when it is *apparent* to the user that the device is connected to the internet because the device is actively being used, and in order for the device to achieve its objective it requires connectivity to the internet. The second method of connectivity is more *obscure* to users and occurs when the device is not being actively engaged by a user, and yet the device is still connected to the internet and sharing or collecting data. This results in devices having two forms of internet connectivity: *apparent* or *obscure*. Below are the three forms in which data generation and collection can occur.

Active-Apparent

The word *active* in this heading refers to the status of the device, meaning that the user is engaging with the device for some purpose. The word *apparent* refers to the reasonable assumption that the device user understands that in order to perform the current task, access to the internet is necessary. Examples of an *active-apparent* interaction with a device include internet browsing, online shopping, and the use entertainment portals. This definition makes no reference to whether the user is aware or unaware of whether data is being collected and simply identifies whether an awareness of connectivity to the internet exists.

Active-Obscure

The word *active* in this heading refers to the status of the device, meaning that the user is engaging with the device for some purpose. The word *obscure* refers to the user's potential lack of awareness that the device is connected to the internet and actively exchanging information with a third party. Examples of an *active-obscure* interaction with a device include playing games, actively using mobile apps, and streaming music.

Dormant-Obscure

The word *dormant* in this heading refers to the status of the device, meaning that the user is not engaging with the device and, from the user's perspective, the device is inactive. The word *obscure* refers to the user's potential lack of awareness that the device is connected to the internet and actively exchanging information with a third party. Examples of a *dormant-obscure* activity include tracked user movement through GPS and geolocation, apps collecting data in the background, operating system information sharing and software updates, and storing of images in the cloud.

A Fourth Permutation?

It could be argued that if we consider all possible permutations that there should be a fourth form that would be titled *dormant-apparent*. In this form the user would be aware that the device is not being actively used while also being aware that the device is connected to the internet and exchanging information with a third party. Examples of this form might be automated software updates or system backups. I have chosen not to accept this form since, according to the above definition, dormant means "the device is inactive." However, if a device were in the *dormant-apparent* state the user would need to be aware that the device would, on occasion, actively perform a function, thereby negating the *dormant* title.

Purpose Statement Context

Given that the purpose of the study was to gain greater insight into the position of constituents regarding the topic of the passing of federal legislation to monitor and control the collection and commercialization of PII gathered from internet activity of adults, I developed an instrument intended to determine constituents' positions. I used the instrument to survey a representative sample of Democrats and Republicans across the U.S. From the data generated by this survey, I was able to quantify constituent awareness surrounding the topic of PII collection and commercialization by DROs, and from those who were aware of the industry, the level of interest in legislation to monitor and control businesses operating in the industry.

Although measuring constituent awareness of the existence and activities surrounding the collection and commercialization of PII by DROs was not the primary purpose of this study, it was a necessary component in determining constituent interest in legislative oversight. Before asking respondents about their opinions relating to desire for legislation to control activities in the personal data industry, I needed to determine if the responding constituents believed data collection occurs while they are using

their personal devices to access the internet (or even when they are not actively engaged in using the internet). Then, constituents were separated into three groups. Group one included all survey respondents who demonstrated awareness of the fact that data is being collected about them while they are using internet connected devices. Group two included those respondents that believed that data may be collected about them, but their awareness was less certain than those in group one. Group three included those respondents who did not believe that any data was ever collected about them while they were online.

Because the purpose of this study was to gain greater insight into the position of constituents regarding the topic of the passing of federal legislation to monitor and control the collection and commercialization of PII gathered from internet activity of adults, those respondents who were completely unaware of the fact that data is being collected were not included in the survey results. However, in addition to the awareness results collected from group three, their demographic information was also collected for future research purposes. For both groups one and two, respondents were assessed on their knowledge, concern, and desire about legislation relating to the collection and commercialization of PII. To be clear, respondents only needed to possess a minimal level of awareness about data collection to be allowed to participate in the survey. Only those respondents who demonstrated a belief that data is definitively not collected from them while they are online were removed from the study, for the reasons stated above. Therefore, all respondents who met the minimum requirements of awareness were allowed to participate in the survey and provide their opinions relating to the need for legislation. The reason for using a survey instrument and, thereby, employing a purely quantitative research design, was because it allowed me to reach a large and representative sample-set of constituents. As the first attempt into measuring constituent sentiment, it seemed logical to understand the total landscape pertaining to constituent opinion before moving onto

more specific quantitative research (i.e., correlation), as well as qualitative research that would first require some general topic knowledge.

The specific research questions that were addressed by this survey included the following:

1. To what extent are constituents aware that personal data is being collected about them when their devices are connected to the internet?
2. For those respondents that are aware that such data is being collected, or believe data might be collected, are constituents knowledgeable about what state or federal legislation, if any, exists to monitor and control the collection and commercialization of individuals' PII; in the absence of state or federal legislation, to what extent do respondents feel concern for the lack of legislation; and, do respondents feel that there should be federal legislation in place to monitor and control what and how DROs are collecting and using their personal data?
3. Of the seven demographic factors identified in this survey; party affiliation, state of residence, sex, age, education, race/ethnicity, and community type; which have a significant impact on respondents' level of awareness, knowledge, concern, and desire?

In order to fully comprehend the situation, it is important to understand each of the following in greater detail: (a) the history of privacy in the U.S.; (b) existing consumer protection legislation in the U.S. and its oversight and enforcement, (c) what, if any, research has been done in this area; (d) the significance of the internet in the U.S.; and (e) the economic value of the internet. In Chapter Two, the Literature Review, I covered each of these topics fully, but before presenting this information, I want to provide definitions of the key terms used in this dissertation.

Definition of Terms

The term *Data Reliant Organization* (DRO) was created for the purpose of classifying organizations that participate in the collection and commercialization of personal data. More specifically, these are

public or private companies that can operate as for profit, not-for-profit, or non-profit organizations. They may or may not work with various governmental organizations or agencies, providing any form of products or services. These companies may generate revenue exclusively from the commercialization of personal data, or data commercialization may be just one of their revenue streams. The one limitation is that they cannot be an agency, department, or office of any local, state, or federal government, meaning that they operate independent of government oversight and without legislative control. This designation is important because governments have created their own sets of regulations pertaining to the collection of personal data, but these regulations do not apply outside of government offices or agencies.

Personally Identifiable Information (PII), *Personal Data*, or *Personal Information* can have different meanings depending on jurisdiction. It is common in the U.S. to see all three terms used in discussions about the importance of data privacy, with all of them frequently used interchangeably. Because all 50 states and the federal government have various forms of limited legislation that provide some sort of data privacy protection, and each state' legislation is independent of the legislation in other states, there is no consistency in the use of a terminology or its specific meaning.

Outside of the U.S. there have been decisions made to select and use just one phrase for legislation. Under the newly enacted General Data Protection Regulation (GDPR), European Union legislation created to protect consumer data and privacy, PII is not a term that is used at all. Instead, the GDPR prefers to use the term Personal Data (cite GDPR website https://eugdpr.org/), which carries a wider definition than that applied in the U.S. This variation can become confusing if users and reader are not fully aware of the similarities and differences in the definitions. However, regardless of the specific phrase, all definitions refer to the use of information on its own or in conjunction with other data that allows for the identification of an individual.

For the purposes of this research, PII and Personal Data were used interchangeably to mean information that is generated about and by the activity of an individual, and that can be uniquely associated with that individual, whether on its own or by combining it with other data. In the absence of widespread federal legislation pertaining to data privacy, and because the generally agreed upon definition means a variety of types of information that can be used independently or in combination with other data to identify an individual, there is not a single list of all types of data that would be included under the definition of PII. Some examples of data that are used in the creation of personal profiles include: names, addresses, phone numbers, income, biometric data, online activity, shopping history, location information, online identifiers, identification numbers (e.g., social security number, passport number, driver license number), parents names, family members, criminal records, place and date of birth, citizenship, ethnicity, financial information, medical information, employment information, marital information, military history, etc. This is not intended to be a complete list and is instead provided as an example of the depth and breadth of what can be included as part of PII.

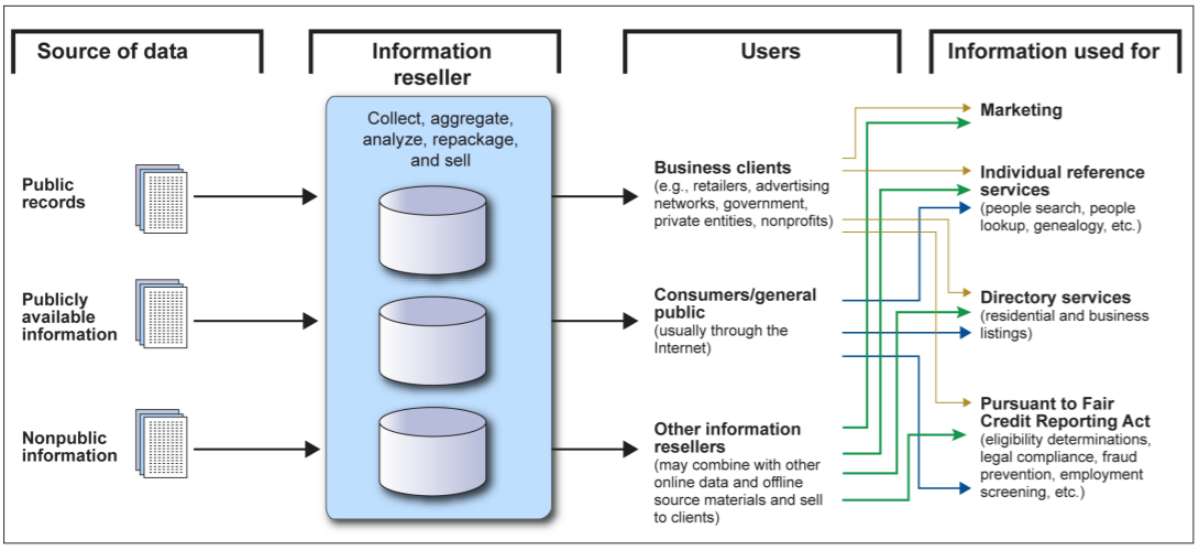
The word *commercialization*, as used here to refer to what DROs are doing with the data they collect, was chosen intentionally. In this case, commercialization refers to the creation of value for an organization for the direct or indirect sale of personal data. This distinction is important because not all DROs that participate in the commercialization of PII directly sell individuals data to other organizations.

Direct sales occur when DROs themselves sell PII to other individuals or organizations that are willing to pay for access to this highly valued information. These sellers are classified as data brokers. Data brokers can collect personal information from public and private sources, as well as using their own businesses (e.g., website, apps, store loyalty programs, etc.), building profiles on individuals, which they then sell on the open market, to their clients, or to other data aggregators. However, data brokers are not always exclusively in the business of brokering data. Some data brokers sell data as an ancillary business function. Retailers are an excellent example of this type of company. Retailers can fall into

either the direct or indirect group of DROs commercializing data, meaning that some retailers sell your personal data as an ancillary revenue source. To more clearly visualize the process, Figure 1 below, taken from the *INFORMATION RESELLERS* report created by the U.S. Government Accountability Office (2013), illustrates the flow of data throughout the sales process.

Figure 1

Typical Flow of Consumer Data Through Resellers to Third-Party Users



Note: Reprinted from the INFORMATION RESELLERS Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace (Puente Cackley, Alicia; Bromberg, Jason; Bowsky, Michelle; Chatlos, William R.; DeMarcus, Rachel; Siegel, Beth; Sinkfield, 2013)

Indirect sales of data occur when organization use data to sell their primary product. As an example, Google collects data about all of their users' online activity. This information is then used to generate highly targeted marketing opportunities for their advertising customers. Google does not give your personal information to their advertisers, but instead sells ad placements that are much more likely to

be seen by people who meet the profile of an ideal consumer for their customers' products. So, in this case Google is not directly selling your PII, but they are indirectly giving their customers access to you.

The term *Data Broker* was used to refer to any privately held or publicly traded company that collects personal information about adult individuals (from both online and offline sources) and then sells that information to others (individuals, companies, or governments). Data Brokers are those organizations whose primary business is collecting and selling data, but they can also be organizations whose primary business is something other than personal data sales (e.g., retailers with a loyalty program) and the selling of personal data is an ancillary business.

The term *Data Collector* was used to describe any privately held or publicly traded company that collects personal information about adult individuals (from both online and offline sources) and uses that information to sell ad space on their websites. A Data Collector could also be an organization that collects data and uses it to market products to its own customers (e.g., grocery stores), however, because this research was focused exclusively on data collected from online sources, the focus of the definition for Data Collectors was on those organizations that use the data for online ad sales.

CHAPTER TWO

LITERATURE REVIEW

The objective of this study was to better understand the position of constituents regarding the need to enact federal legislation to monitor and control the collection and commercialization of personally identifiable information (PII) by data reliant organizations (DROs). It is standard practice for a PhD dissertation to include a scholarly review of the academic literature available about the topic being studied. In this section I will make every attempt to adhere to this standard despite the fact that there is presently little to no scholarly literature published exploring public opinion regarding the need for federal legislation to protect PII collected and commercialized by DROs. After significant efforts were made to uncover research aligned with this topic, only two sources were found that briefly addressed this issue. The first piece of research was a study commissioned by a Washington, D.C. watchdog group, conducted as a telephone poll by a third-party researcher, which included a few questions about data privacy and respondents' interest in legislation to oversee data collection and commercialization. The second piece of research was a study commissioned by the Annenberg School of Communications on behalf of the Berkeley Center for Law and Technology, conducted by landline and wireless telephone interviews, which included two questions about respondents' interest in laws to protect personal privacy. Exclusive of these two examples, there is no additional research available.

In light of this limitation, this chapter will begin by reviewing the history of privacy in the U.S., followed by a review of existing U.S. protection and oversight related to personal data. Then I will provide a brief overview of the breadth and depth of the internet in U.S. society. Next I will review available literature to assess the economic value of the internet. Lastly, I will share a summary of the data captured as part of the research mentioned in the previous paragraph that was conducted by the D.C. watchdog organization and by the Berkeley Center for Law and Technology.

The History of Privacy in the U.S.

The notion of individual privacy, and more specifically, what is and is not protected as private, has been a topic of conversation and a basis for legislation (*Early Postal Legislation*, n.d.) since the formation of the U.S. To fully understand how we as a nation have arrived at our current stage of legislative development it is important to have a full grasp of the events that have delivered us to where we are today. As unlikely as it may sound, protection of PII generated through internet use has its foundations in the activities of regular citizens and legislators from the late 19th and early twentieth centuries, as well as the creation and interpretation of the Constitution and the Bill of Rights. In this section I will explore those individuals and events that have laid a foundation for the protection of PII today.

Early Efforts for Individual Privacy

As early as the late 19th century, citizens of the U.S. were calling for the formalization of federal law to address the concept of protection of personal privacy. In 1890, Samuel D. Warren & Louis D. Brandeis, two prominent Harvard Law School graduates, published an article in the Harvard Law Review about "The Right to Privacy" (Warren & Brandeis, 1890). This article is considered by some to represent the beginning of the privacy movement, or, as one article title stated the matter, "The Invention of the Right of Privacy" (Glancy, 1979). The purpose of the article by Warren and Brandeis focuses on two principles, the first being the importance and need for the laws addressing privacy "from time to time to define anew the exact nature and extent of such protection" going on to emphasis "political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society" (Warren & Brandeis, 1890, p. 194). Said differently, Warren and Brandeis felt that the law on privacy had to be elastic, changing with the times and flexible enough to change with the evolving social, economic and political landscapes. At the time of the drafting of Warren and Brandeis's article there were no statutory laws pertaining to personal privacy, meaning that

all rules about individual privacy were a result of common law and judiciary precedent (Rao, 2017). Warren and Brandeis recognized that the legal definition of personal privacy had changed many times during history, citing several examples of how defining privacy had grown throughout U.S. legal history, addressing the need for it again to be changed to keep up with shifts in society and business (Warren & Brandeis, 1890, p. 194).

Warren and Brandeis (1890) specifically address two drivers for the required change, technological developments and changing business practices. More specifically, the development of technology allowing for "Instantaneous photographs," rather than long exposure images that required people and things to remain still for extended periods of time, and the practice of newspapers printing more and more stories that were considered gossip rather than hard news in an effort to appeal to a wider audience (Warren & Brandeis, 1890, p. 195).

A secondary principle of the Warren and Brandeis article was that no one can be forced to share personal information, and if an individual does make the decision to share personal information, they still retain the right to determine how the information is disseminated (Warren & Brandeis, 1890, p. 199). In direct parallel to many of the concerns surrounding PII today, Warren and Brandeis talk about the importance of individuals having the right to determine "to what extent [their] thoughts, sentiments, and emotions shall be communicated to others" (Warren & Brandeis, 1890, p. 198). This sentiment is credited to Sir Joseph Yates, an 18th century English judge, who said:

> It is certain that every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his own friends…and no man can take it from him or make any use of it which he has not authorized, without being guilty of a violation of his property. ("Joseph Yates (judge) - Wikiquote," 2016, para. 4)

Several years after Judge Yates made this statement, on June 12, 1816, Thomas Jefferson wrote a letter to Samuel Kercheval (*Letter from Thomas Jefferson to Samuel Kercheval | Teaching American History*, n.d.). An excerpt from this letter appears on the southeast wall of the Jefferson memorial, which is one of only five quotes on the memorial (*Jefferson Memorial Features - Thomas Jefferson Memorial (U.S. National Park Service)*, 2017). Separate from Jefferson's ownership of slaves and possible fathering of children with one of them (History.com Editors, 2009), he was a political visionary who contributed significantly and positively to the creation of the democratic structure of the U.S. The inscription on the interior of the Jefferson Memorial, which also speaks to the importance of elasticity of law and the Constitution, reads:

> I am not an advocate for frequent changes in laws and constitutions, but laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with the change of circumstances, institutions must advance also to keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy as civilized society to remain ever under the regimen of their barbarous ancestors. (*Jefferson Memorial Features - Thomas Jefferson Memorial (U.S. National Park Service)*, 2017)

The Warren and Brandeis article is the first known attempt to establish a basis for what things are considered personal and private and should therefore be controlled by the individual and not by private business (Glancy, 1979; Rao, 2017). Ironically, Warren committed suicide on February 18, 1910 due to gossip about how he handled the executorship of his father's business and personal estates (Wikipedia contributors, 2018g), but not before he made a significant and lasting impact on the future of personal privacy.

The principle of caveat emptor in the U.S. has been on a steady decline since the late 19th century with the ushering in of the Progressive Era (*The Progressive Era (1890 - 1920)*, n.d.). Traceability, the capacity to track something through all stages of its creation lifecycle, as an element of consumer protection and government legislation is nothing new to post Progressive Era American society. Individual and consumer protectionism began its meteoric rise during this period due in large part to the efforts of people like Harvey Washington Wiley (Blum, 2018), journalists categorized as muckrakers (Weinburg, 1964), and the activist/novelist Upton Sinclair ("Upton Sinclair, Whose Muckraking Changed the Meat Industry - NYTimes.Com," 2016). These three sources are credited with contributing to the establishment of the first "federal consumer protection agency" (Commissioner, 2018), the Food and Drug Administration (FDA), an agency that was made possible with the passing of the Pure Food and Drugs Act in 1906 (Commissioner, 2018).

The U.S. Constitution and Privacy. The right to privacy in the U.S. is a long and passionately debated subject. I feel that I would be negligent in discussing the topic of privacy without addressing the elephant in the room --privacy granted as a constitutional right to all U.S. citizens. Although this research is focused on personal data privacy, and more specifically, data generated by using personal internet connected electronic devices, a discussion about any kind of privacy in the U.S. will almost inevitably circle around to the mentioning of constitutionally granted privacy rights. Therefore, I feel compelled to do a brief and narrow overview of constitutional privacy coverage.

The U.S. Constitution (the Constitution) did not come with a separate set of instructions; that fact can probably be agreed upon by virtually everyone. From that point of consensus there are an almost infinite number of interpretations of what is stated or intended by the words of this great document. The original Constitution, which was signed on September 17, 1787 (*The Constitution: How Was It Made? | National Archives*, n.d.), was written to specifically outline the powers granted to the federal government by the 13 states agreeing to form a new union. It is not a lengthy document when

considering its significance and purpose. It primarily serves to describe the three branches of the federal government; the powers assigned to each branch and the requirements for appointment; the powers assigned to the new federal government with a message that anything not assigned to the federal government falls to the states; and the rights granted to, and requirements of, individual states within the union (Wikipedia contributors, 2018h).

The Constitution itself did not outline specific rights given to the citizens of the new union, that task was achieved through the Bill of Rights and the subsequent 17 amendments. Although many of the signatories at the Constitutional Convention were not completely satisfied with the Constitution's contents, they agree to give their support in exchange for a promise of amendments to the document that would provide for specific individual rights (*The Constitution: How Was It Made? | National Archives*, n.d.). As agreed during the Constitutional Convention, on June 8, 1789 James Madison submitted 12 amendments to the first federal congress for approval (*The Bill of Rights: How Did It Happen? | National Archives*, n.d.). It took time, but eventually ten of the 12 amendments to the Constitution were ratified by the states on December 15, 1791 and were called the Bill of Rights (*Our Documents - Bill of Rights (1791)*, n.d.). It is these amendments, and a few others, that have been used to try and determine the existence of constitutionally granted rights to privacy. To be clear, when I reference the Constitution regarding the topic of privacy, I am explicitly focused on the amendments to the Constitution.

In support of the concept of there being no instruction manual for the Constitution, Supreme Court Justice Felix Frankfurter once "argued that the Constitution gives no guidance about how to weigh or measure divergent interests" (Finn, 2006). If you have ever read the U.S. Constitution, the one thing that can be said about the words that it contains, and that would likely not meet with significant argument, is that the vernacular and the lexicon of Americans has changed greatly over the past 231 years. Partially for this reason, partially for the reason that the world has profoundly changed well

beyond the possible imagination of the architects of the document, and partially because much of the content is non-specific -- a topic that is hotly debated as to whether that was intentional or mistaken (Steele, 2015) -- the U.S. Constitution is often interpreted differently by those who read and try to understand its meaning for the purposes of providing legal precedent and guidance.

Privacy Precedent Established by the Supreme Court. The word privacy is never used in the original Constitution or any of its amendments. However, according to some of the interpretations from the Supreme Court, the absence of the specific word does not mean that there was no intention for protection of privacy of individual citizens. It is that concept of penumbra rights that has been the driving force behind landmark cases like Roe v. Wade (Wikipedia contributors, 2018e) and Griswold v. Connecticut (Wikipedia contributors, 2018b). An exploration into the contents of the Constitution and its amendments reveals that legal efforts to determine what privacy rights are granted through the amendments has been occurring over the past 150+ years but did not begin in earnest and gain significant traction until the later part of the 20th century (*Privacy | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute*, n.d.).

Since the ratification of the Bill of Rights there have been several laws passed that set precedence for the existence and expectation of privacy in the U.S. Examples of these laws include the 1782 law prohibiting workers in the postal system from reading private letters (*Early Postal Legislation*, n.d.), and in 1919 when Congress made it illegal to release Census data about individuals (Solove, 2006). Arguably more important than the specific laws passed to protect individual privacy were the federal court decisions that both upheld a belief that the Constitution provided for the protection of individuals' privacy, and other rulings that expressed a belief that certain privacies were not intended to be protected.

The first example of the Supreme Courts belief that individual privacy was intended as a part of the implied protections of the constitution occurred in 1878 when the Supreme Court ruled that under the Fourth Amendment the U.S. government could not open mail without a warrant. The ruling specifically went on to say that there is a "constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be" (Ex Parte Jackson :: 96 U.S. 727 (1878) :: Justia US Supreme Court Center, 1878). A second example of judicial interpretation of privacy occurred in 1886 in the case of Boyd v. United States. In this case the government wanted Boyd to provide an invoice to prove the purchase of glass panes (Wikipedia contributors, 2018a). In the judgement, the Supreme Court ruled that based on implicit intent of the Fourth and Fifth Amendments, Boyd could not be forced to turn over the documents. Taking a quote from Daniel J. Solove's article titled A Brief History of Information Privacy Law, the Supreme Court said:

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right to personal security, personal liberty and private property. . . . [A]ny forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment. In this regard the Fourth and Fifth Amendment run almost into each other. (Solove, 2006, p. 1-9)

A strong belief in implied privacy within the Constitution by the Supreme Court has not always been present. In the landmark 1928 case of Olmstead v. United States the Supreme Court did not support the idea that wiretapping without a warrant was a violation of the Fourth and Fifth Amendments (Head, 2018). As a result of this ruling, then Justice Brandeis (the same Brandeis that co-authored "The Right to Privacy") published his dissent, which was aligned with his longstanding position on the importance of individual privacy, where he argued for a Constitutional Amendment to grant a right to privacy (Head,

2018). A strong part of his reasoning for his dissent was the development of new technologies that allowed for the government to gain access to individuals conversations, technology that did not exist in the past (Head, 2018). Brandeis's focus on the importance of technology and its contributions to a need for increased efforts to protect individual privacy were consistent with his article from almost 40 years earlier. In 1961, in a second landmark case supporting the belief that the Constitution does not contain implied rights to privacy, Poe v. Ullman (Wikipedia contributors, 2018d) upheld "a Connecticut law banning birth control on the grounds that the plaintiff was not threatened by the law and, subsequently, had no standing to sue" (Head, 2018, para. 6). In this case, Justice John Marshall Harlan II published his dissent, which would become law four years later (Head, 2018).

Shortly after the ruling on Poe v. Ullman in 1961, and the published dissent by Justice Harlan II, the landmark case of Griswold v. Connecticut was heard in 1965 by the U.S. Supreme Court. This case, which supported the implicit privacy rights in the Constitution, challenged the right to allow married adults to use contraception. This decision was important for two reasons. The first was that it identified a total of five amendments (the First, Third, Fourth, Fifth, and Ninth) having implicit privacy protection, or penumbra. This was significant because it was the first time that the Supreme Court took such a broad sweeping amendment approach to the privacy topic. The second reason for this case's importance was the court's decision that together these penumbras created a "zone of privacy" (*Privacy | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute*, n.d.), which are a group of rights granted to all citizens and implicit in the Bill of Rights. This zone of privacy would be used as the basis for landmark cases in the future. One such case, one of the most widely contested and debated Supreme Court privacy rulings of the 20th and 21st centuries, was Roe v. Wade in 1973.

Four years after Roe v. Wade, and relating more directly to data privacy, there was the case of Whalen v. Roe in 1977. Although this case did not support the plaintiffs' claim for privacy protection relating to drug prescriptions in New York State, it did result in the court's declaration that "the

constitutional right to privacy grounded in the Fourteenth Amendment respects not only individual autonomy in intimate matters, but also the individual's interest in avoiding divulgence of highly personal information" (Solove, Daniel J.: Schwartz, 2017, p. 564).

All of these rulings, and many others not mentioned her, have contributed to the public opinion of whether privacy is a right granted to all U.S. citizens or not. When individuals are questioned about their feelings regarding the right to protecting their PII these historic rulings will likely have an influence

Existing U.S. Protection and Oversight

Understanding the history of privacy in the U.S. provides valuable context into the development of the topic and its importance in our society. However, implicit in the concept of providing for privacy is protection for individuals' rights and safety. Just as understanding the history of privacy in the U.S. is critical to the ability to completely comprehend the factors contributing to protecting internet generated PII, so is possessing the knowledge of existing regulations and legislation pertaining to individual consumer protection and data privacy. When considering the factors associated with passing legislation, the motivations and processes that legislators use to make those decisions becomes incredibly relevant as well. For this reason, I will explore consumer protection agencies and the factors that contributed to their creation. In addition, I will examine existing legislation associated with PII, beginning with data breach laws, followed by data disposal laws, and then data protection laws. As a final element of privacy legislation, I will explore factors that contribute to legislators' decisions in support or opposition of proposed regulations.

State and Local Agencies to Protect Consumers. As part of this research, and where relevant, I have and will endeavored to provide a comparison and contrasting view of legislation within the individual U.S. states and the federal government. In the case of consumer protection oversight, all 50 states, the District of Columbia, and Puerto Rico each have a somewhat different approach to consumer rights

protection, albeit an identical sectoral breakdown of regulated industries. Each of them has mechanisms in place to address the creation of regulations, oversight of protected areas, acceptance and administration of consumer complaints, and enforcement of laws. The five sectors that are monitored for all states, the District of Columbia, and Puerto Rico include state-chartered banking activities, securities and investment dealings, insurance practices, and utilities services (*State Consumer Protection Offices | USAGov*, n.d.). Interestingly, this may be where the similarities end. The states have all created their own structures and systems for dealing with each of the sector businesses and complaints within each sector. Using information gathered from the State Consumer Protection Offices website, Table 1 below illustrates how several states have structured consumer protection:

Table 1

Sampling of State Agencies Responsible for Consumer Rights Protection

State	Number of offices with responsibility	Designated offices
Alabama	1	- Alabama Office of the Attorney General
Delaware	1	- Delaware Dept. of Justice
Alaska	2	- Dept. of Commerce, Community & Economic Development Anchorage - Alaska Office of the Attorney General, Anchorage
Mississippi	3	- Mississippi Dept. of Agriculture and Commerce - Mississippi Office of the Attorney General - Mississippi Office of the Attorney General – Biloxi

Florida	15	- Three State Consumer Protection Offices
		  ○ Florida Dept. of Agriculture and Consumer Services
		  ○ Florida Dept. of Financial Services
		  ○ Florida Office of the Attorney General
		- Six Regional Consumer Protection Offices
		- Six County Consumer Protection Offices

California	25	- Four State Consumer Protection Offices
		  ○ California Bureau of Automotive Repair
		  ○ CA Dept. of Consumer Affairs
		  ○ California Office of the Attorney General
		  ○ Contractors State License Board
		- 18 County Consumer Protection Offices
		- Three City Consumer Protection Offices

Note: Data to create this table was gathered from State Consumer Protection Offices website (*State Consumer Protection Offices | USAGov*, n.d.)

As you can see in Table 1, there are a variety of formats for how each state has chosen to deal with the issue of consumer protection against deceptive and predatory business practices. Although many states have given authority to state, county, region, and/or city attorneys general, there are some unusual offices of authority: Delaware's Department of Justice; Alaska's Department of Commerce, Community & Economic Development; and Mississippi's Department of Agriculture and Commerce.

Although the above are just a few examples of the states' approaches to managing consumer rights protection, they are representative of vast and varied differences from one state to another. This is one of the reasons that I have chosen not to go into detail about the establishment and the enforcement of state-run consumer rights protection, and yet I will provide more detail surrounding federally run agencies. The second reason is that several of the federal agencies that have consumer rights protection responsibilities are also currently participating in the creation of regulations, protection of consumers, and enforcement of laws specifically pertaining to PII.

Federal Agencies to Protect Consumers. The federal government has a long history for providing consumer protection. Beginning in 1906 with the formation of the FDA, and as recently as 2010 with the establishment of the Consumer Financial Protection Bureau, the federal government has formed a total of six consumer focused agencies, each having a mission to ensure fair business practices and consumer protection (including privacy protection) within their specific sectors of business. In the order in which they were established, these six agencies include:

- The Food and Drug Administration (FDA) – The FDA was establishment in 1906 with the passing of the Pure Food and Drugs Act (Commissioner, 2018). The agency is charged with the administration and enforcement of laws pertaining to the manufacturing and sale of food, medical supplies and drugs, tobacco, and cosmetics. In addition, the FDA has oversight for two other areas of public health and safety:

  - Providing critical oversight for "advancing the public health by helping to speed innovations that make medical products more effective, safer, and more affordable" and ensuring that the public has "accurate, science-based information they need to use medical products and foods to maintain and improve their health" (Commissioner, 2018).
  - Participating in counterterrorism efforts by "ensuring the security of the food supply and [the] development of medical products to respond to deliberate and naturally emerging public health threats (Commissioner, 2018).
- The Federal Trade Commission (FTC) – The FTC was created in 1914 when Woodrow Wilson signed the Federal Trade Commission Act. The mission of the FTC is "to protect consumers and promote competition" (Federal Trade Commission, 1970), with a focus in two areas:
  - Consumer Protection: "Stopping unfair, deceptive or fraudulent practices in the marketplace." The FTC will also "conduct investigations, sue companies and people that violate the law, develop rules to ensure a vibrant marketplace, and educate consumers and businesses about their rights and responsibilities" (*FTC What We Do | Federal Trade Commission*, n.d.).
  - Promoting Competition: The FTC monitors and reviews all mergers and business practices, challenging them when necessary to protect consumers from resulting "higher prices, lower quality, fewer choices, or reduced rates of innovation… to ensure that the market works according to consumer preferences, not illegal practices" (*FTC What We Do | Federal Trade Commission*, n.d.).
- The Securities and Exchange Commission (SEC) – The SEC was established with the signing of the Securities Exchange Act by Franklin D. Roosevelt in 1934. The SEC's mission is to enforce "the federal securities laws, proposing securities rules, and regulating the securities industry, the

nation's stock and options exchanges, and other activities and organizations, including the electronic securities markets in the United States" (*SEC.Gov | The Laws That Govern the Securities Industry*, 2013).

- National Highway Traffic Safety Administration (NHTSA) – The NHTSA was created in 1970 to enforce the regulations created by the Highway Safety Act of 1966 and the National Traffic and Motor Vehicle Safety Act of 1966. The mission is "to help Americans drive, ride, and walk safely…by promoting vehicle safety innovations, rooting out vehicle defects, setting safety standards for cars and trucks, and educating Americans to help them make safer choices when driving, riding, or walking" (*NHTSA History - Understanding the National Highway Traffic Safety Administration (NHTSA) | US Department of Transportation*, 2017).
- The Consumer Product Safety Commission (CPSC) – The CPSC was created through the signing of the Consumer Product Safety Act in 1972 (U.S. Consumer Product Safety Commission, n.d.). The mission is to protect "the public from unreasonable risks of injury or death associated with the use of the thousands of types of consumer products under the agency's jurisdiction." The agency does this through creating voluntary industry standards, "issuing and enforcing mandatory standards," (U.S. Consumer Product Safety Commission, n.d.) establishing product recalls and determining actions, conducting product research, and informing and educating consumers.
- The Consumer Financial Protection Bureau (CFPB) – The CFPB was created with the signing of the Dodd–Frank Wall Street Reform and Consumer Protection Act in 2010, which was in response to the Great Recession in the U.S. (*H.R.4173 - Dodd-Frank Wall Street Reform and Consumer Protection Act*, 2010). The CFPB's mission is to "protect consumers from unfair, deceptive, or abusive practices and take action against companies that break the law. We arm

people with the information, steps, and tools that they need to make smart financial decisions" (Consumer Financial Protection Bureau, n.d.).

Although possibly not obvious at first glance, each of these six agencies have two extremely important factors in common: the impetuses for their establishment and the overarching objectives of each of their missions. Although the six agencies were created over a period spanning more than 100 years, there was one consistent and ever-present reason for why legislators ultimately decided to pass the propositions that led to the formation of each group. According to research into the incentives surrounding the motivations of members of congress during each period, legislators were consistently motivated by "public outcry" (Cornish, 2009; *CPSC Outcry*, 2007; *FDA Outcry - The Pure Food and Drug Act | US House of Representatives: History, Art & Archives*, 1906; *FTC Outcry - Federal Trade Commission (FTC) - Encyclopedia - Business Terms | Inc.Com*, n.d.; McFarland, 2004; Peterson, 2016) in response to the unfair and deceptive practices of DROs operating in each of the respective industries. Stated differently, legislators were aware of what their constituents thought about these topics and acted accordingly.

The second commonality amongst these six organizations was that each was established to ensure that consumers had honest and consistent transparency into the operations of DROs. In each of their respective industries, and prior to the passage of each Act, there were no laws requiring private organizations to share details or specifics about business practices or manufacturing processes openly with consumers. Whether that openness consists of accurately listing all product ingredients on a food package or disclosing part failures and subsequent recalls of automobile parts, the objectives are consistent in their attempt to minimize misleading or false claims and ensuring consumer safety while allowing consumers visibility into the details of the consumer practices of the organizations with whom they are dealing.

State Data Breach Legislation. The subject of personal data is an incredibly hot topic in today's media. The trend of mainstream media is to focus on stories about data breaches, or cyber security breaches of well-known organizations (Confessore, 2018; O'Brien, 2017), which tend to result in viewer and readership spikes. As an example of the number of data breach stories versus PII stories, I did a Google search for PII and for data breaches and the results are surprisingly dissimilar. A search for the phrase "personally identifiable information" within quotes, to ensure that the results have all three words in them and in the exact order, returns about 6,500 results within the *News* tab. Doing a similar search for the phrase "data breach" returns about 2.7 million results within the *News* tab. This is obviously not a scholarly attempt at researching the differences in mainstream media's coverage of each topic, but it is intended to lightly demonstrate one example of the differences in what is covered by the media about each topic.

The first step into fully understanding what legislation exists around data privacy and protecting personal data was to conduct a thorough legislative review. At the state level this research revealed the existence of what I am calling a three-tiered, progressively more protective, system of regulations: (a) Data Breach Notification Laws – often loosely structured legislation containing requirements outlining necessary steps, with the occasional preventative regulation, designed to instruct DROs who own or hold personal data on how, and with whom, to communicate after the occurrence of a breach and how to correct any individual injuries, (b) Data Disposal Laws – slightly more restrictive, these laws have been designed to establish guidelines for how DROs should properly dispose of personal data after it is no longer needed, and (c) Data Security Laws – these laws were designed to provide guidelines, although often vague and interpretive, to ensure that those DROs holding or storing data take appropriate steps to protect personal data from unauthorized access. This state-by-state analysis was necessary in order to compare and contrast existing legislation, and to determine if overarching federal legislation was unnecessary, and/or repetitive, in the presence of existing state legislation. This research allowed me to

discover that there is a significant disparity between the actions that states have taken versus the actions that the federal government has taken relating to all three tiers of protective legislation, as well as specific oversight of DROs participating in the collection and commercialization of PII.

Data breaches, and the process of notifying those affected in the event of a breach, have received significant attention from state governments. A data breach is defined by Cambridge Dictionary as "an occasion when private information can be seen by people who should not be able to see it" (The Cambridge Business English Dictionary, n.d.). This definition, although simple, succinctly communicates the core idea of the term and is used in a similar form by many states when defining a breach (*Summary of U.S. State Data Breach Notification Statutes*, n.d.). Some definitions go on to speak of the damage that occurs in the event of a breach, when personal information is accessed. For example, the state of Arizona adds to their definition that a breach also "causes or is reasonably likely to cause substantial economic loss to a resident" (*Summary of U.S. State Data Breach Notification Statutes*, n.d.). This definition, although still somewhat vague, does provide greater information about the identity of what the state of Arizona considers to be a data breach. However, for sectors of the federal government this definition is still insufficient. In the federal government's definition for a breach, taken from the Health Insurance Portability and Accountability Act Omnibus Rule, a breach is further refined to say that a breach is "the impermissible acquisition, access, use, or disclosure of" protected health information (PHI), unless "a covered entity or business associate can demonstrate, through a documented risk assessment, that there is a low probability that the PHI has been compromised" (Williams, Rebecca L.; Greene, Adam H.; Barash, Louisa; Eckels, Jane; Rauzi, Edwin D.; Thurber, Kent B.; Blanchette, 2013). In a somewhat contrasting approach, in September of 2018 an amendment was passed for the Gramm-Leach-Bliley Act, which defines a breach much more interpretively by saying that a breach is "unauthorized access that is reasonably likely to result in identity theft, fraud, or economic loss"

(Luetkemeyer, 2018). As you can see, there are varying levels of complexity to the definition of data breach and there is no one accepted definition that is universally used.

Over the past 50 years the federal government has consistently chosen a sectoral approach to legislation regulating personal data protection. Specifically involving the area of data breach notification, there are only two pieces of sectoral legislation dealing with data breach notifications; healthcare and finance. In the presence of federal legislation applicable to only two business sectors, which leaves all other business unregulated, state governments have passed their own laws and regulations outlining the definition of a data breach, what data is covered and in what form, the actions to take in case of a breach, and penalties in the event of non-compliance. According to the National Conference of State Legislatures (NCSL), as of March 2018, all U.S. states, Washington D.C., Puerto Rico, Guam, and the U.S. Virgin Islands have enacted data breach notification legislation (National Conference of State Legislatures, 2018a, 2018b).

The overarching premise of the data breach notification legislation in all 50 states, Washington D.C., and the three U.S. territories requires organizations to inform individuals in the event of a breach that could impact personally identifiable information (*The Definitive Guide to U.S. State Data Breach Laws*, 2018) or cause financial harm as a result of the breach and information that was accessed (*Summary of U.S. State Data Breach Notification Statutes*, n.d.). When examining each law in detail, there are consistencies in the general content of each state's law and the existence of industry definitions for each law (but not in the definitions themselves), which are summarized well in *The Definitive Guide to U.S. State Data Breach Laws* (2018)*:*

> These laws typically define what is classified as personally identifiable information in each state, entities required to comply, what specifically constitutes a breach, the timing and method of notice required to individuals and regulatory agencies, and consumer credit

reporting agencies, and any exemptions that apply, such as exemptions for encrypted data.

Not surprisingly, there is little to no consistency across state boarders regarding legislation details. This includes, but is not limited to, variations in the definition of PII, the form in which data is maintained (i.e., digital and/or paper), what organizations are required to comply, exactly what data is protected, specific actions to take in the event of a breach (timing, content, method), exemptions for organizations or events, the requirements (or absence of requirements) for data security, penalties in the event of a failure to meet state laws, or even what constitutes a data breach (*Summary of U.S. State Data Breach Notification Statutes*, 2018; *The Definitive Guide to U.S. State Data Breach Laws*, 2018). Additionally, states are continually amending and updating their laws. In light of this information, it is not difficult to understand the challenges and frustrations that individuals experience when trying to understand their rights across state lines and the difficulty organizations face in attempting to navigate compliance when dealing with multi-state legislation. Consider the challenge for an organization that suffers a nationwide breach and the difficulty with satisfying the specific requirements of 55 individual state and territory data breach notification laws. As a point of clarity, the reason that there are 55 pieces of legislation when there are only 50 states, plus Washington D.C., and three U.S. territories (Puerto Rico, Guam, and the U.S. Virgin Islands) is because California has two pieces of legislation. The first piece of legislation is filed under the California Civil Code and applies to “A person or business [that] own or license computerized data” (CA Civil Code for Data Breaches, 2016). The second piece of legislation is filed under the California Health and Safety Code and specifically applies to businesses that operate as “A clinic, health facility, home health agency, or hospice” (CA Health and Safety Code for Data Breaches, 2014).

In contrast to the other 48 states, Washington D.C., Puerto Rico, Guam, and the U.S. Virgin Islands, there are two standouts who have taken further steps to try and prevent data breaches before they

occur. The state of Nevada has included as part of their revised data breach law a requirement for data encryption of any personal data that is stored on devices that are moved outside of the physical offices of the data holder, as well as encryption of any data that is transmitted wirelessly (excluding faxes) outside of the company (*Nevada Expands Personal Data Definition in Breach Notice, Data Encryption Law | Bloomberg Law*, 2015; Shiroff, 2015). Massachusetts, the state credited with having the most significant encryption regulations associated with their data breach law has taken an even stronger stance on the topic of data privacy protection (*Massachusetts Law Raises the Bar for Data Security | Jones Day*, 2010). According to a white paper published by Oracle in 2010, *Massachusetts Data Security Law Signals New Challenges in Personal Information Protection*, Massachusetts law 201 CMR 17.00 is enforcing higher standards of personal data protection that include "encryption, access control, authentication, risk assessment, security policies and procedures, security monitoring and training" (*Mass Law 201 CMR 17*, n.d.; *Massachusetts Data Security Law Signals New Challenges in Personal Information Protection*, 2010). Although the Massachusetts law is not specifically classified as a data breach law, it does include with the security requirements for any organization handling PII specific information about what to do in the event of a data breach, which is why the details are included here.

Interestingly, while Nevada created its law to minimize the opportunity for, and the effects of, a data breach, the law itself obviously only applies to personal data collected from, or held on, residents of the state. Massachusetts intentionally created their new law to provide greater protection for the "residents of the Commonwealth" (*Mass Law 201 CMR 17*, n.d.). This means that personal data in these two states, absent of the occurrence of a breach, is subject to more stringent security requirements than other states. These two examples are providing greater protection for the residents of their respective states, but together these two states represent only three percent of the total U.S. population, meaning that absent of any other data protection laws, 97% of the U.S. population has no preventative state breach protection in place (*US States - Ranked by Population 2018*, n.d.).

Although state legislation to notify individuals in the event of a breach is better than no protection at all, and it is a good line of initial defense in the event of a data disaster, the scope and value of these laws can be misleading and provide a false sense of security to individuals. As an example of how this misleading information is conveyed, the laws are very often referred to as “Data Breach Legislation” (National Conference of State Legislatures, 2018a) and “Data Breach Laws” (Lohrmann, 2018) by organizations that are perceived as, and take a position of, legislative experts. In fact, exclusive of Nevada and Massachusetts, the balance of these laws are considered “notification” laws by each state and are focused exclusively on ensuring that individuals are notified of a breach after the fact. These laws are not intended to prevent data breaches as the preceding titles could suggest. As protection, these regulations are tantamount to little more than legal guidelines for how to notify individuals in the event of a breach, sharing with those individuals their rights. They are limited to only requiring notification and maintain no requirements for DROs to uphold minimal levels of security; to disclose the type or amount of data that they collect, hold, or process; to ensure that individuals have access to data profiles or the ability review and correct inaccuracies in their data; to provide the opportunity for individuals to opt out of allowing the DROs to collect or use their data; or any of the other provisions that would provide individuals with greater transparency and control of their personal information. The 53 laws, again, exclusive of Nevada and Massachusetts, have clearly been designed to be a reaction in the event of a breach, and to provide awareness to an incident after it has occurred and after the potential damage is done. Once again, although the limited defense against personal data violations that is provided by the data breach notifications laws is better than no defense at all, data breaches are only a small portion of the larger personal data privacy concern. In addition, there are still fears regarding the sufficiency and productivity of a state-by-state approach for protecting both consumers and DROs.

In July of 2018 the U.S. Department of the Treasury released a report for regulating financial technology, titled *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation* (Mnuchin & Phillips, 2018). The report specifically discusses the Treasury's recommendation that "Congress enact a federal data security and breach notification law." This recommendation is in direct response to the two issues that are being raised by consumer and business advocates regarding the challenges associated with 55 independent pieces of legislation about the same issue: (a) confusion for consumers about their rights and how to pursue protective action (especially across state line), and (b) confusion for companies when having to address consumer reporting/notifications and dealing with penalties resulting from a breach. However, the Treasury's recommendation specifies that new legislation "Protect consumer financial data" (Mnuchin & Phillips, 2018) and would not apply to any other personal data that could be compromised in a data breach. Much like the state laws, enacting a federal data breach law as outlined by The Treasury Department would still leave opportunity for legislation to address wider reaching laws regarding data privacy protection and control.

Although state level legislation provides some protective benefit to individuals concerned with controlling the security of their personal data, these laws primarily focus on notification requirements after a breach has occurred and still leave the causality factor of proper data security prior to a breach unregulated and up to DRO self-regulation. Additionally, even if the data breach legislation were more comprehensive, it would still only address a small subset of the issues associated with data privacy protection and the control and the oversight of DROs collecting and commercializing PII. Therefore, although the expressed interest from The Treasury Department in federalizing data breach regulations would bring us closer to uniformity in our data breach messaging and protection (albeit exclusively in relation to financial data), it would still fall short of comprehensive data breach protection, which in and of itself is still a subset of the larger PII protection issues.

Federal Data Breach Legislation. Research into the topic of federal data breach notification laws revealed a significant weakness in the federal government's legislation to protect consumers in the event of a data breach. The federal government has adopted a sectoral strategy for personal data privacy protection (detailed in the following pages), but exclusive of two sectors, finance and healthcare, they have neglected the topic of data breach notification in any other form.

On August 21, 1996 the Health Insurance Portability and Accountability Act (HIPAA) was signed into law (*HIPAA History*, n.d.). According to the HHS.gov website, the Act was created to give individuals greater control over their ability to make informed healthcare decisions, to move more easily from one healthcare provider to another, and "for the first time [to] create national standards to protect individuals' medical records and other personal health information" (Office for Civil Rights, 2002a). The new HIPAA laws, which were aligned with the federal government's history of a sectoral strategy to data privacy, did not originally contain oversight for data breaches or guidelines for notification in the event of a data breach. It was not until February, 2009, as part of Title XIII of the American Recovery and Reinvestment Act of 2009 (The Recovery Act) (H.R.1 - 111th Congress (2009-2010): American Recovery and Reinvestment Act of 2009, 2009), which established the Health Information Technology for Economic and Clinical Health Act (HITECH Act), that the first federal data breach notification regulations were created. The HITECH Act provided for the digitization of medical records, and subsequently, a need for a change in the legislation to protect individual medical data privacy. Although the HITECH Act was a step in the right direction, some members of Congress felt that the definition of a breach and the ability to avoid notification was weak and that is was "too subjective, resulting in inconsistent interpretations" (Williams, Rebecca L.; Greene, Adam H.; Barash, Louisa; Eckels, Jane; Rauzi, Edwin D.; Thurber, Kent B.; Blanchette, 2013). This resulted in the passing of the Omnibus Rule in January, 2013 (Williams, Rebecca L.; et al., 2013), which is the current federal data breach notification legislation for HIPAA. The Omnibus Rule provided several improvements to the original HIPAA regulations, including

greater detail and specification regarding consumer protection, data portability, business associate responsibilities, a fines in the event of violations (Williams, Rebecca L.; et al., 2013). Specific to data breach protection, it more clearly defined what constitutes a breach, when organizations must take action, and what action is required.

The HIPAA regulations do not apply to all DROs involved in the collection and management of personal health data. According to HHS.gov, the organizations that are regulated by HIPAA include: health plans, health care clearinghouses, and health care providers (Office for Civil Rights, 2002b). However, at the time of the drafting of the Omnibus Rule, this definition left a group of DROs, described by The Recovery Act (2009) as "new types of web-based entities that collect consumers' health information" unregulated by the HIPAA rules. This gap in the protection of personal health information was recognized during the drafting of The Recovery Act and steps were taken to create a new set of regulations that would be overseen by the FTC (*Health Breach Notification Rule 16 CFR Part 318 | Federal Trade Commission*, 2010). This new set of regulations, passed in August of 2009 and regulated by the FTC, is called the Health Breach Notification Rule. To greatly simplify which organizations are covered by this set of regulations, it includes any organization involved in the collection of personal health information (PHI) that does not fall under the regulations of HIPAA. The requirements for data breach notification are aligned with those of HIPAA (*Health Breach Notification Rule 16 CFR Part 318 | Federal Trade Commission*, 2010) and are intended to offer full protection for individuals providing health information to DROs regardless of whether those DROs fall under the regulations of HIPAA or not.

The second industry that is controlled by federal regulations for data breach notification is the finance industry. The Gramm-Leach-Bliley Act (GLBA) of 1999, also known as the Financial Services Modernization Act, regulates "companies that offer consumers financial products or services like loans, financial or investment advice, or insurance" (Gramm-Leach-Bliley Act, 2010). As part of the GLBA, the data breach notification laws outlined the specific requirements for consumer notification in the event

of a breach. Unlike the Omnibus Rules, which were created in part to reduce DRO interpretation and provide more clear and definitive rules and actions (Williams, Rebecca L.; et al., 2013), the GLBA data breach notification rules were more subjective and allowed for independent understanding of the requirements by individual regulatory agencies governed by GLBA (Luetkemeyer, 2018). Another element of GLBA, unique from HIPAA, is that state legislation governing data breach notification requirements can supersede GLBA regulations. However, on September 13, 2018 the House Financial Services Committee approved H.R.6743, the Consumer Information Notification Requirement Act (Luetkemeyer, 2018), that would create federal data breach notification for the finance industry and supersede all state laws. As of the drafting of this document, H.R.6743 still must be assigned to a calendar, pass the full house vote, go to the Senate, be assigned to a senate committee, be approved by the committee, pass a full senate vote, and then be signed off on by the president. There is still a long way to go for this bill to become law, but as of now it has passed some of the initial hurdles.

State Data Disposal Laws. Data disposal laws pertaining to DROs, as a concept, are probably the easiest category to understand within the data privacy trio of legislation. Enacted in a total of 33 states and Puerto Rico (National Conference of State Legislatures, 2018c), these laws apply to people or businesses that hold or control data. The data disposal regulations provide the guidelines for the requirements of how data can be disposed of. Disposal requires that the data is altered or changed in some way, rendering the data unreadable or unusable by any unauthorized person. Destruction of the data can be done in one of several ways. For printed data, proper disposal can take the form of redacting, shredding, burning, or any other form that causes the data to be unreadable or indecipherable. Electronic data must be erased or destroyed in a way that results in the inability for anyone to reconstruct the information. The subject of if when data is destroyed is left up to the individual DROs. There is a 34th state that has passed data disposal regulations, Virginia, but those

regulations only apply to state government agencies and are not imposed on DROs. For a complete list of states that have passed data disposal laws see Image 1.

Federal Data Disposal Laws. Federal regulations regarding proper disposal of data, much like data breach notification laws, are sectoral in nature and tend to be part of, or amendments to existing legislation. Below is a list of all regulations that contain specific data disposal regulations:

- Fair and Accurate Credit Transactions Act (Credit Reporting Industry) – The broadest reaching of all of the federal data disposal laws, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) provides for "the proper disposal of information in consumer reports and records to protect against unauthorized access to or use of the information" (*FACTA Disposal Rule Goes into Effect June 1 | Federal Trade Commission*, 2005). The FTC sometimes brands the data disposal portion of FACTA as their own calling it the Disposal Rule (*FTC Seeks Comment on Disposal Rule | Federal Trade Commission*, 2016). FACTA is an amendment to FCRA and applies to any business that uses credit reports. Part of the FACTA is regulated and enforced by the FTC (Fair and Accurate Credit Transactions Act of 2003 | Federal Trade Commission, 2003).
- Gramm-Leach-Bliley Act (Finance Institutions) – The GLBA provides somewhat specific information about what type of personal data must be destroyed (i.e., paper and digital) and provides some information on how it can be destroyed (*Financial Institutions and Customer Information: Complying with the Safeguards Rule | Federal Trade Commission*, 2006). However, there is no specification about when, if ever, data must be destroyed. Because it is possible for a financial institution to have credit report information on individuals, the FTC directs that financial institutions should follow the disposal rules of Gramm-Leach-Bliley instead of FACTA. Like FACTA, the GLBA is regulated and enforced by the FTC (Gramm-Leach-Bliley Act, 2010).

- The Health Insurance Portability and Accountability Act (Healthcare Industry) – In this example of federal disposal regulations, HIPAA does not specify exactly how data should be disposed of. The recommendation is to ensure "that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of [protected health information] PHI" (Office for Civil Rights, 2009b). Although the Act is absent of specifics on process for disposing of data, the Department of Health & Human Services provides some recommendations and additional details (Office for Civil Rights, 2009a). Enforcement of HIPAA Privacy and Security Rules is overseen by Health and Human Services' Office for Civil Rights (Office for Civil Rights, 2017).
- Child Online Privacy Protection Act (Online Data Collection of Children Under 13 Years of Age) – To an even less specific degree than with HIPAA, Child Online Privacy Protection Act (COPPA) provides no information surrounding the process for data destruction beyond copy that reads "using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion" (*ECFR — Code of Federal Regulations*, n.d.). What the Act does make clear is that data can be kept "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." The requirements for when to delete are also the most stringent of all regulations and include deletion upon parental request. In addition, and even in the absence of a request, deletion of all contact data is required is there is a lapse in subscription renewal or a subscription is cancelled, unless the data is needed for billing purposes. Like FACTA and GLBA, COPPA is regulated and enforced by the FTC (*Children's Online Privacy Protection Rule (COPPA) | Federal Trade Commission*, 1998).
- Video Privacy Protection Act (Protecting Video Rental, Sale, or Streaming Information) – Enacted during the height of the video rental era, the Video Privacy Protection Act (VPPA) was intended to protect the viewing history of individuals. The disposal of PII was prescribed to be done "as

soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected" (18 USC 2710: Wrongful Disclosure of Video Tape Rental or Sale Records, 1988). However, details surrounding the process for data destruction are not provided as part of this Act. Violation of these rules are considered a civil action and can be taken in the United States district court.

State Personal Data Security Legislation. In contrast to the approach seen by all 50 states specific to enacting data breach notification laws, where the states have collectively taken the lead in providing some form of coverage for all citizens, data security legislation to regulate DROs who handle highly personalized data has not seen the same level of participation.

When discussing data security legislation, the term refers to laws that are created to protect PII from being accessed by unauthorized users. These laws incorporate both administrative regulations (employee training, security documentation, and security change notification) and technological hardware recommendations. Although similar in purpose and objective – to protect individuals' PII and to ensure that consumers have visibility into what is happening to their data – data security legislation is uniquely different from data breach notification laws, and somewhat more obviously, data disposal laws. As discussed earlier, with the noted exceptions, data breach notification regulations are specific to ensuring that predetermined steps are taken, after a breach has occurred, to notify all relevant parties. Data disposal laws were designed to ensure that personal data is not kept beyond its period of use and regulates the disposal processes of PII. It can be said that data breach notification laws and data disposal laws are both process laws. Data security laws, on the other hand, are technology laws. This means that unlike data breach notification laws and data disposal laws, where the states direct DROs on procedural requirements, data security laws identify the use of technology as the requirement to ensure compliance. Figure 2 below provides a summary of all 50 states, illustrating those states that have data breach notification laws, data disposal laws, and data security laws.

Figure 2

A State-by-State Comparison

States with Data Privacy Regulations Applicable to DROs

States	Data Disposal Law	Data Security Law	Both Disposal & Data Security Laws	No Disposal & No Data Security Laws
Alabama	-	-	-	◇
Alaska	✓	-	-	-
Arizona*	✓	-	-	-
Arkansas	✓	✓	◆	-
California	✓	✓	◆	-
Colorado	✓	✓	◆	-
Connecticut††	✓	✓	◆	-
Delaware	✓	-	-	-
Florida	✓	✓	◆	-
Georgia	✓	-	-	-
Hawaii	✓	-	-	-
Idaho	-	-	-	◇
Illinois	✓	-	-	-
Indiana	✓	✓	◆	-
Iowa	-	-	-	◇
Kansas	✓	✓	◆	-
Kentucky	✓	-	-	-
Louisiana	✓	✓	◆	-
Maine	-	-	-	◇
Maryland	✓	✓	◆	-
Massachusetts	✓	✓	◆	-
Michigan	✓	-	-	-
Minnesota	-	✓	-	-
Mississippi	-	-	-	◇
Missouri	-	-	-	◇
Montana	✓	-	-	-
Nebraska	-	✓	-	-
Nevada	✓	✓	◆	-
New Hampshire	-	-	-	◇
New Jersey	✓	-	-	-
New Mexico	✓	✓	◆	-
New York	✓	-	-	-
North Carolina	✓	-	-	-
North Dakota	-	-	-	◇
Ohio	-	✓	-	-
Oklahoma	-		-	◇
Oregon	✓	✓	◆	-
Pennsylvania	-	-	-	◇
Rhode Island	✓	✓	◆	-
South Carolina††	✓	✓	◆	-
South Dakota	-	-	-	◇
Tennessee	✓	-	-	-
Texas††	✓	✓	◆	-
Utah	✓	✓	◆	-
Vermont	✓	✓	◆	-
Virginia†	-	-	-	◇
Washington	✓	-	-	-
West Virginia	-	-	-	◇
Wisconsin	✓	-	-	-
Wyoming	-	-	-	◇
Totals	33	21 (18)	18 (15)	14

* Regulations apply only to personal data printed on paper

† Data disposal regulations exist, but are only applicable to government agencies

†† States whose Data Security legislation is limited to a single business industry and is not applicable to all businesses

( ) Number in parentheses identifies states with Data Security legislation that applies to all businesses

Data Sources: ncsl.org, Blancco.com

With a focus on state laws regulating PII data security, and based on a legislative review of all state and federal legislation that has been passed as of the date of this research, it appears that fewer than

half of all states have enacted legislation to provide guidelines for DRO data security requirements. There are 21 states that have enacted legislation focused on enforcing varying levels of requirements for protecting PII held by DROs in digital form (see Figure 2). There is one additional state, Arizona, which has data security legislation that only applies to PII in paper form. Three of the 21 states, Connecticut, South Carolina, and Texas have enacted sector specific laws in health insurance, insurance, and sports & athletics, respectively. The remaining 18 states have data security legislation that applies to all people and DROs that use or hold digital PII. Two of these states, Vermont and California, took a big step forward in 2018 to provide greater oversight and control of DROs participating in the commercialization of PII. Both Vermont and California have taken steps beyond data security requirements and have ventured into requiring disclosure by DROs. Upon analyzing the legislation for both states I found that Vermont has taken a narrower, sectoral approach to monitor and control DRO activity in a specific industry and has combined data security requirements with modest disclosure mandates as well. A closer look at California legislation revealed that California began limited disclosure requirements in 2003, and in 2018 passed broad sweeping legislation that will could have impact across wider sectors of businesses. The Vermont approach is more closely aligned with the method that the federal government has consistently taken since its first legislative action to protect consumer privacy with the passage of the Fair Credit Reporting Act in 1970. In addition, while

To be clear, state governments have passed varying forms and strengths of legislation in their pursuit to provide protection for individuals and their PII. In fact, prior to the changes that occurred in Vermont and California in 2018, all 21 states with data security legislation provided little specificity when outlining the guidelines for security. Although the exact wording varies somewhat from state to state, it is consistently vague and non-specific. An example of this type of wording, taken directly from the California's existing civil code, requires companies that hold PII to "maintain reasonable security procedures and practices" (California Data Security, 2015), which is the entirety of the detail that is

provided regarding security requirements for all companies. One exception to this vague and somewhat self-guiding wording comes from the state of Vermont, which directs DROs to be "consistent with the safeguards for protection of personal information set forth in the federal regulations" (General Law - Part I, Title XV, Chapter 93H, Section 2, n.d.). Although, as demonstrated by Vermont and California, the existing vague and self-regulating approach for data security regulations is no longer sufficient and a more aggressive and specific set of laws to protect personal data privacy are necessary.

In May of 2018, the state of Vermont passed a new, and first of its kind law to regulate the activities of data brokers. Data brokers are private companies that are in the business of monetizing data. There are a variety of business models that are used by data brokers, which can include companies that handle data in the following ways before selling it: companies that compile data from public and private sources (both free and paid), companies that only generate their own primary data, companies that compile data from offline-only sources, companies that compile data from online-only sources, companies that only analyze data and generate profiles and groupings or clusters, companies that only host data, and companies that only buy and sell data. Although there are examples of data brokers that do only one of the preceding functions, many data brokers do a combination of these activities, expanding their scope of services. Data brokers come in all sizes, from tiny, sole proprietorships running their own company, to multi-billion-dollar global firms. Regardless of the size, the objective of all data brokers is to build databases of information that are sold to other individuals, organizations, or groups, including other data brokers and the federal government. Most data brokers do not have direct relationships with consumers. Because of this, most consumers are unaware of the data broker activity or even their existence. The data, in the form of either individual personal profiles or clustered target group profiles, is used primarily in one of three way: marketing, people searches, and fraud prevention (Ramirez & Brill, 2014). It is the Vermont governing body's position that they believe it is their "duty to exercise its

traditional Police Powers" to protect the rights and safety of consumers (*H.764 Vermont Data Broker Legislation*, 2018).

The new Vermont legislation, although 37 pages in length, is somewhat limited in its detail of specific data broker requirements. A summary of the regulations, taken directly from the document itself (*H.764 Vermont Data Broker Legislation*, 2018), outlines the following protections:

- Requires all data brokers operating in the state to register annually as data brokers.
    - According to the state of Vermont, data brokers are "those businesses that aggregate and sell the personal information of consumers with whom they do not have a direct relationship" (*H.764 Vermont Data Broker Legislation*, 2018).
- Implements requirements for security measures that provide "appropriate administrative, technical, and physical safeguards to protect sensitive personal information" (*H.764 Vermont Data Broker Legislation*, 2018). This further outlines details that include:
    - Assigning management of the security protocols to employees,
    - Training of current and new employees on policies, with controls to prevent former employees for obtaining unauthorized access,
    - Working with and requiring similar security from third party vendors,
    - Ongoing assessment and improvement, when necessary, to the security protocols,
    - Building or implementing systems for detecting and preventing failures,
        - This includes data breach requirements similar to those already enforced in Vermont, and
        - Prohibits the acquisition or use of PII for fraudulent purposes.
- Mandates that data brokers provide "the name and primary physical, e-mail, and Internet addresses of the data broker" (*H.764 Vermont Data Broker Legislation*, 2018).

- Directs data brokers to share if they allow for "consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data" (*H.764 Vermont Data Broker Legislation*, 2018).
    - When opting out is available, the data broker must provide details about how to opt out, what consumers can opt out of (and what they cannot opt out of), and if they allow for third party authorization to request opting out for consumers.
- Eliminates credit agencies authority to charge consumers $10 and $5, respectively, to implement a security freeze and unfreeze on their credit reports.
- States that data brokers must share whether they have a "credentialing process" (*H.764 Vermont Data Broker Legislation*, 2018) for screening data purchasers.
- Conditions data brokers to reveal all data breaches that have occurred during the previous year and how many individuals were affected.
- Requires data brokers to share if they collect data on minors, and if so, to create separate documentation about their practices for collecting data on minors that mirrors all of the above requirements.

It is important to note several relevant factors about this new legislation. Although only applicable to the data brokerage business sector, Vermont is requiring all data brokerage companies operating in the stat to disclose data collection activities of adults for the first time. Data brokers are required to provide contact information to the state when they register annually. In addition, they must share if they have an opt out option for consumers, which allows consumers to choose to not allow brokers to use their personal information. Lastly, data brokers must share with consumers, upon request, the process for how to opt out of data sharing. This last disclosure may seem unnecessary to mention, but in the past data brokers could tout that they allowed for opting out, but they were not required to share with consumers how to actually opt out. Also worth mentioning is that contrary to the way in which the

new legislation is being presented in mainstream media, the law does not require data brokers to provide the option of opting out of data collection, profiling, or sale of individuals PII. The law simply states that if data brokers have this option available, they must share that information with the state when they register. Interestingly, if a data broker currently has an opt-out option available, they can change that option prior to registering on January 1, 2019 before the law takes effect.

This sectoral approach, focusing on the data brokerage industry, is the first of its kind by a state. Adopting this method of consumer protection is more closely aligned with the way the federal government has chosen to address data privacy protection than it is to the way that other states have chosen to apply blanket style legislation.

California is the other state that has taken unprecedented action to protect consumer privacy. A leader in privacy protection for its residents, California has led the way in many areas of privacy protection. Although California was the first state to pass a wide sweeping data privacy bill this year, it was also the first for other privacy legislation. California was the first to pass a state data breach notification law in 2002 (CA Civil Code for Data Breaches, 2016), the first to pass an online privacy protection law in 2004 (Internet Privacy Requirements, 2002), and the first to pass anti-phishing legislation in 2005 (*Anti-Phishing Act of 2005*, 2005), just to name a few. Not only is California a leader in state privacy legislation, it has also been incredibly prolific with privacy legislation. According to the California Department of Justice website (*Privacy Laws | State of California - Department of Justice - Office of the Attorney General*, n.d.), the California "Constitution gives each citizen an inalienable right to pursue and obtain privacy," there are 70 "General Privacy laws" enacted in the state, 10 "Health Information Privacy" laws, 18 "Identity Theft" laws, 15 "Online Privacy" laws, and five "Unsolicited Commercial Communications" laws. It is important to remember that in addition to these 119 state laws to protect individual privacy, there are also numerous federal laws that provide similar or related protections.

Unlike any other state prior to Vermont's 2018 legislation, California addressed the topic of disclosure of personal data business practices, specific to personal data monetization, back in 2003. The Shine the Light law was officially enacted on January 1, 2005 and outline the requirements of a limited sector of for-profit companies sharing consumer data with third parties (*California Shine the Light Law*, 2003). The law required that business operating in the state of California, who collected personal information on their customers, to create measures for sharing details on the company's data sharing procedures. In summary, if a company shares personal customer data with a third party for some type of compensation, the company must share with their customer(s) the details of who the information was shared with and exactly what information was shared (*California Shine the Light Law*, 2003). The exclusions to this requirement are lengthy and include the following exemptions. The law only applies to third parties that use the data to directly market products or services to customers. This means that the sale of personal information to many data brokers would not fall within the requirements of this law because most data brokers do not directly market products or services customers. Exclusive of data brokers selling online searches of individuals, data brokers mostly sell their profile information to companies that will use the data in one of three forms: to sell to others, to marketing products to customers, or to do background searches. Another exemption is if the company selling the personal data has fewer than 20 employees. In those cases, they are not required to share their business practices with the consumers whose data they collect or sell. As a third example, the law only applies to companies that have a direct customer relationship and are conducting business with individuals for "personal, family, or household purposes" ("California Shine the Light Law," 2003, e.1.5). So although there are many exemptions from this law, it was the first of its kind in the U.S.

On June 28, 2018 California passed a first of its kind privacy protection bill called the California Consumer Privacy Act of 2018. Although passed in June of 2018, the law is not scheduled to go into effect until January 1, 2020. During this time the state legislature has the right to make changes to the

law (*California Consumer Privacy Act of 2018*, 2018, sec. 1798.185). The new law is much more restrictive on companies and provides much greater protection to individuals than its predecessor, California Shine the Light law. As the law is currently written, it applies to any company that falls within the following limitations:

- For profit companies doing business in California or collecting personal data on California residents.
- Although the new California Act does apply to data collected electronically (internet, mobile, etc.) and non-electronic data collection (Section 1798.175 "The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers."), it only applies to organizations that directly sell the data they collect. It clearly does not apply to companies that collect (or presumably acquire) data to be used for non-direct sales purposes (meaning google does not "sell" their data but sells the value created from the data they hold).

Federal Data Privacy/Security Legislation. Unlike the federal government's conspicuous lack of action in enacting data breach notification legislation, beyond its two sectoral efforts in healthcare and finance, the federal government does have a somewhat long history of being more widely involved in protecting consumers' private data from abusive business practices.

Although the federal government has been active in protecting consumer data using a sectoral approach, that approach has left many sectors unregulated. In addition, and as stated by the Government Accountability Office, federal laws have not kept up with changing technologies and data collection processes (Staff of Chairman Rockefeller, 2013, p. 4). The federal laws that exist today may not cover all instances of personal data collection by DROs, but at least there is some legislation in place to protect consumers. However, it is important to note that exclusive of COPPA laws to protect children

under the age of 13, and activities in health care, public finance, or credit reporting, there is no federal legislation specifically targeting the activities of Data Brokers or Data Collectors. Below is a review of all existing federal legislation that addresses the topic of online data privacy and security applicable to DROs. The list does not include legislation enacted to control the activity of federal agencies or offices. The list is organized in order of passage of the legislation, beginning with the oldest.

- The Federal Trade Commission Act of 1914 – The FTC was created in 1914 with a mission "to protect consumers and promote competition" (Federal Trade Commission, 1970). The agency is tasked with both enforcing existing legislation associated with data privacy and security as well as creating regulations that support existing legislation.
- The Fair Credit Reporting Act of 1970 – This Act was "designed to promote accuracy, fairness, and privacy of information in the files of every consumer reporting agency" (*A Summary of Your Rights Under the Fair Credit Reporting Act*, 2003). Each of the three designated targets of this act (accuracy, fairness and privacy) are key to the relevance of this act as it relates to protection of PII. However, this Act only applies to consumer reporting agencies and does not extend beyond that sector.
- The Family Educational Rights and Privacy Act of 1974 – This Act restricts disclosure of information about students and their educational records without the consent of students or parents. This Act only applies to institutions or agencies that receive federal funding. (*Family Educational Rights and Privacy Act (FERPA)*, 2018).
- The Fair Debt Collection Practices Act of 1977 – The Act was created to "to eliminate abusive debt collection practices by debt collectors, to insure that those debt collectors who refrain from using abusive debt collection practices are not competitively disadvantaged, and to promote consistent State action to protect consumers against debt collection abuses" (*Fair Debt Collection Practices Act | Federal Trade Commission*, n.d.).

- The Computer Fraud and Abuse Act of 1984 – This Act makes it a crime to access or damage protected computers or to traffic passwords. In addition, the Act has been amended to include activities associated with the distribution malicious codes and computer viruses (Wikipedia contributors, 2019b).
- The Electronic Communications Privacy Act of 1986 – The Act "protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically" (*Electronic Communications Privacy Act of 1986*, n.d.).
- The Video Protection Act of 1988 – This Act was passed to prevent the disclosure of individuals viewing history of digital or electronic media. The bill was originally passed to address video tape rental history but it does include "similar audio visual materials" and includes streaming video and game history (Wikipedia contributors, 2018f).
- The Driver's Privacy Protection Act of 1994 – This Act establishes limitations on what information can be shared by state departments of motor vehicles and with whom. This does not mean that your information is not shared, but it puts limitation on the reasons the information is shared and prevents the use of that information from being used for marketing purposes (*Driver's Privacy Protection Act | ASPE*, 2014).
- The Health Information Portability and Accountability Act of 1996 – The Act was created to give individuals greater control over their ability to make informed healthcare decisions, to move more easily from one healthcare provider to another, and "for the first time [to] create national standards to protect individuals' medical records and other personal health information" (Office for Civil Rights, 2002a).
- The Children's Online Privacy Protection Act of 1998 – This Act was created to allow parents to manage and control what information is collected online about their children who are

under the age of 13. This Act applies to both websites and mobile app operators who target children as well as those who knowingly collect information for children under age 13 (*Children's Online Privacy Protection Rule (COPPA) | Federal Trade Commission*, 1998).

- The Financial Services Modernization Act/Gramm-Leach-Bliley Act of 1999 – The Act was created to allow for the consolidation of financial services companies but also includes requirements for institutions to share their data sharing practices and allow individuals to opt-out of allowing some of their information to be shared (Gramm-Leach-Bliley Act, 2010).

Beyond the federal sectoral laws enacted to protect consumers' PII generated through online activity, many DROs endorse the concept of self-regulation rather than supporting the enactment of additional or new legislation. In an effort to provide some direction and to participate in the oversight of industries self-regulation, in 2007 the FTC developed a set of self-regulatory guidelines called the Behavioral Advertising Principles. The decision to follow these principles is voluntary for all companies but considered as best practices by many.

Existing Research

A Watchdog Voter Poll. Campaign for Accountability is a Washington, D.C. based watchdog who focuses on "federal accountability, state oversight, corporate responsibility, and consumer protection" (*About Us | Campaign for Accountability*, n.d.). Beginning on June 11 and continuing through June 19, 2018, Campaign for Accountability engaged Greenberg Quinlan Rosner, a polling and opinion research firm, to conduct a study on voter sentiment about internet companies, monopolies, security of data, and interest in legislative oversight of large internet and technology companies. This poll was the only example available of research whose purpose was to identify individual or constituent interest in legislation to oversee DROs dealing in the commercialization of PII.

The poll was conducted via telephone contacting 1,001 registered voters. Beyond the total number of voters contacted, no additional sampling data is provided. The results of the poll present some interesting data regarding voter sentiment surrounding internet companies, data privacy, and an interest in greater government regulations. This data includes the following:

- 43% of voters support increased regulations of internet and technology companies
- 59% of voters believe they have little to no control over information collected about them online
- 77% of voters believe internet and technology companies have a negative effect on privacy
- 50% of voters believe internet and technology companies have a negative effect on personal safety
- 46% of voters believe internet and technology companies have a negative effect on society
- 58% of voters support the idea that online political advertising should be controlled in the same way that television and radio political advertising is controlled (Greenberg Quinlan Rosner, 2018)

Although this data is interesting and seems to take the first step into exploring the sentiments of voters' feelings about legislation to oversee personal data commercialization, there are two major concerns: data reliability and validity.

In its simplest form, data reliability is the extent to which a test or tool produces similar results under consistent conditions (Phelan, Colin; Wren, 2006). However, the conditions do not have to be identical and allow for variations in administrator, i.e., inter-rater reliability, or changes in when the test is administered or the order of the questions, i.e., test-retest reliability (Roberts, Paula; Priest, Helena; Traynor, 2006). For the above study data to be reliable the instrument would need to produce the same

results if different people were to administer the same survey, and potentially if the questions were reordered.

Data validity is the proverbial other side of the coin in the measurement of the quality and usefulness of a survey instrument. In summary, validity is the determination of how well a test measures the research question(s) and how well it represents the assumptions it makes. For the above study results to be valid it would need to demonstrate both external and internal validity (Eby, 1993; Punch, 1998), meaning that the respondents would need to be a representative sample of all voters, the questions would need to be clear and understandable by the respondents, and the answers would need to have no bias in administrator interpretation.

I address reliability and validity because I question both in this study. In the administration of the survey, the respondents are twice asked if they feel "there should be more regulation on internet and technology companies" (*Legislation Survey; What Americans Think About Tech Companies | Campaign for Accountability*, 2018, p. 17). The first-time respondents are asked this question and the administrator logs their answers. Then the administrator provides some additional information about the topic before asking the question a second time (the details of the additional information are not provided). When asked the same question the second time, respondents feelings changed significantly. Prior to hearing the additional information, 43% of participants felt there should be more regulations. After hearing the additional information, 73% of participants felt there should be more regulations. This represents an increase of 30 points, or a 70% increase from pre to post additional information(*Legislation Survey; What Americans Think About Tech Companies | Campaign for Accountability*, 2018, p. 17). Additionally, the administers propose questions that are leading, with inaccurate details, and chose to phrase the questions as statements of fact with the expected response being how strongly the respondent agrees (*Legislation Survey; What Americans Think About Tech*

Companies | Campaign for Accountability, 2018). As an example, see the question below (Greenberg Qunilan Rosner Research, 2018, p. 16):

> (DATA IS PROFIT) Facebook and Google only offer their services for free to consumers because they sell our personal data on the backend. Facebook and Google makes millions by selling personal data to advertisers who target ads based on our search history, gender, age, and income. There need to be regulations on what personal information companies like Facebook and Google are allowed to sell.

To begin, the survey chooses a title that is potentially negative and could sway the opinion of the respondent. Then, in the first sentence, the statement inaccurately states that Facebook and Google are "selling personal data" to advertisers. This is not true as neither Facebook nor Google ever sell data. They sell ad space and use their respective data to ensure that the advertisers' ads are delivered to users who meet the advertisers chosen profiles, but the data is never shared. Lastly, instead of asking if the respondents believe that these situations warrant legislation, they survey states that "There need to be regulations…" and then expect the respondents to rate how strongly they agree with the statement. These inaccuracies and leading methods called into question the reliability and validity of the survey and the results reported.

In an effort to better understand the process and facts associated with the data collection, I contacted Daniel Stevens, Executive Director of Campaign for Accountability. I requested more detail about the method for administering the questions, specifically the order of the questions and what information was provided to respondents in what the Campaign for Accountability called the "Initial Ask" and the "Re-ask Post Messages" (*Legislation Survey; What Americans Think About Tech Companies | Campaign for Accountability*, 2018). In addition, I offered to have a phone call or to answer any questions Mr. Daniels might have. Mr. Daniels did respond to my request, informing me that all of the

information that the Campaign for Accountability was willing to provide was available on their website. Unfortunately, there are no details about the process or method of administering the survey or the additional information provided. It is for this reason that, even in light of the fact that this is the only known data available on the topic of how constituents feel about the need for legislation to oversee the commercialization of PII by DROs, I do not feel that this data can be considered in the administration or assessment of research into understanding constituent sentiments on this topic.

Comparing Privacy Attitudes Among Adults. The University of Pennsylvania's Annenberg School of Communications, in conjunction with the University of California's Berkeley Center for Law and Technology, conducted a telephonic survey in 2009. Led by the Annenberg School of Communications, and engaging with market research and polling company Princeton Survey Research Associates International, a national survey of adults in the U.S. was conducted. Completed between June 18 to July 2, 2009, a survey was conducted to understand "attitudes towards and knowledge of the rules and practices surrounding the collection and use of personal information" (Turow, 2010).

The survey was conducted via landline and wireless telephone contacting 1,000 adults. Although the purpose of the survey was to measure the similarities or differences in the sentiments of U.S. adults about collecting and sharing personal information, there were two specific questions pertaining to their interest in laws to provide protection of privacy, with a third question referencing permission before sharing personal information. The three questions were:

- "Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?" (Turow, 2010).
- "Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, or do you feel such a law is not necessary?" (Turow, 2010).

- "Generally speaking, anyone who uploads a photo or video of me to the internet where I am clearly recognizable should first get my permission." (Turow, 2010).

The survey was conducted and published with a clear analysis of the data's validity and reliability. And although the two questions about respondents' interest in laws to regulate certain activities were thought-provoking, the data was not ideally aligned with the purpose of my study. The purpose of the survey was to compare sentiments and knowledge across age groups and not to understand to any extent the strength, depth, or urgency of the respondents' opinions or the application of any such laws across businesses or industries. This purpose could explain why the responses to the questions about laws were limited to only yes or no answers.

The first question asks about respondents' opinions regarding a law to "know everything that a website knows about them" (Turow, 2010). This question, although likely appropriate for allowing for the comparison of opinions across age groups, only asks about websites and makes no reference to any other data gathering or commercializing groups. For the purposes of having extendable value for research into constituent opinions regarding legislation over DROs, the responses from this literature do not hold enough detail or context.

In a similar style, the second question asks if respondents think there should be a law that "requires websites and advertising companies to delete all stored information about an individual" (Turow, 2010). However, without the context of why and when this would happen, it is difficult to know what respondents meant and when they believe the data should be deleted. Some respondents could have meant that data should be deleted immediately and never used. Other respondents could mean that the data should be deleted upon request from the individual. The possible interpretations of this question weaken its value and limit its applicability to the purpose of my study.

The third question, although not specifically about respondents' interests in laws to protect privacy, does imply the concept of some type of enforceable regulation or rule. For that reason, it is included in the assessment of potential literature relating to my study. However, the data being referenced in the question is limited to pictures or videos and there is no clarity on to whom the potential rule or regulation would be enforced upon; individuals, DROs, etc. For these reasons, this question provides the least amount of potential value for my study.

The assessment of this study is not intended to diminish its overall value or objective to achieve it purpose. It seems as though, based on the outlined purpose of the study, the data collected provided the insight that the authors were pursuing. Unfortunately, although this is a peer reviewed piece of empirical research, it provides little to no additional insight into constituent opinions pertaining to the need for federal legislation to monitor and control the activities of DROs.

The Omnipresent Internet

It is unlikely that anyone reading this study needs to be convinced of the magnitude of the internet or its global impact. However, it may be helpful to be provided with some context in order to fully embrace the pervasiveness of its presence in our lives.

Since the introduction of the first commercial internet service provider (ISP) in 1989 (Leiner et al., 1999), and the launch of the World Wide Web in 1993 (Leiner et al., 1999), life in the United States (U.S.) has been profoundly impacted by this thing we call the internet. Simply do a search on Google Scholar for "impact of the internet" and you will receive almost four million results in less than two-tenths of a second, with article topics ranging from the internet's contributions toward eventually curing cancer to the perils of sexual addition via online pornography and social-sexual websites. Do the same search on Google and the number of results increases to 547 million in .51 seconds, with similarly varying and diverse opinions of the internet's impact. Whether the impact is measured as positive, negative, or a

combination of both is up to the individual, but the significance of the impact of the internet itself is nonetheless real.

In the U.S. the internet is directly leveraged and accessed by all forms of government, both large and small-scale businesses (McLeod, 2018), and almost all individuals (Ryan, 2018) to enhance operational performance, to create greater access, to communicate, to educate, and to entertain. So regardless of how we are directly or indirectly touched by its existence, every individual (yes, everyone) in the U.S. is being affected in some way by the proliferation of the internet. Whether it is the homeless family who receives meal-assistance from the networked soup kitchen whose supplies arrive on-time and in the proper quantities due to improved logistical efficiencies and ordering systems managed through web based Software as a Service (SaaS) fulfillment networks (Food Bank for New York City, 2013), to the multi-cultural global fans of the most widely watched video of all time, Despacito, which has been viewed more than 5.5 billion times (Wikipedia contributors, 2019).

I think it is safe to say that there is a vast amount of value to be gained from the internet, and at little to no out-of-pocket cost to the individual. Search the World Wide Web for the greatest inventions of all time and you will consistently be presented with the internet as one of those inventions. And although most people in the U.S. choose to purchase their own hardware devices and obtain private access to the internet through commercial ISPs (U.S. households with PC/computer at home, 2015; Demographics of Internet and Home Broadband Usage, 2018; Demographics of Mobile Device Ownership and Adoption, 2018; Ryan, 2018), 98% of all public libraries have networked computers available as well as Wi-Fi (Bertot, John; Palmer, n.d.), both of which are free to anyone who goes to a public library, including the homeless. So, even though the majority of Americans choose to incur some cost to gain access to the internet, there is no direct cost to use the internet itself or to access much of the content and services available through its various protocols (e.g., HTTP for the web, IMAP and POP for email, FTP for file transfers, etc.). And although we live in a world dominated by the concept of

commercialization and profit, the internet itself has somehow remained a free entity for virtually anyone in the U.S. who wants to use it. All of this information considered, isn't it strange that two of the world's top five most valuable companies ("Top Companies - The top 10 US companies by market capitalization," n.d.) are internet content providers that do not charge users to use their service? But as the saying goes, "There is no such thing as free unless the thing in question is without value" (Penn, 2009).

This last point is important because it is the basis for the fact that in return for providing access to the content and services that are available on the internet, and with no direct out-of-pocket expense to the user, the DROs generating the content and delivering the services are receiving something of great value in return - access to personally identifiable information about every user. But as hard it may be to believe after learning about how pervasive the internet is, and having experienced the transformation that the internet has had on all of us over the past 25+ years, the impact of the internet so far may pale in comparison to the impact that the next generation of internet technology will have on our lives and our society; specifically I am referring to the IoT and AI.

The Economic Value of the Internet

When exploring federal legislation that will affect an industry it is important to understand the economic impact of that industry on the economy. The age of the internet is arguably one of the most impactful ages in modern history; one par with the development of commercial electricity and the industrial revolution. Therefore, as I explore the factors that are influencing decisions about the need for federal legislation to monitor and control data collection and commercialization, I would be negligent if I did not also provide some cursory research into the valuation of the internet economy.

Estimating the value of the internet is no small task. People like Hal Varian, Chief Economist at Google attempted to do this in 2013 by estimating the annual value to individuals via time savings,

coming up with an estimated value of $500/year/individual (Varian, 2013). That equates to approximately $165 billion per year. Unfortunately, this hypothesis was not based on any verifiable research, making it difficult to assess its true value.

In a similar attempt to value the internet globally, in October 2011 McKinsey Global Institute released a report evaluating the global economic value that the internet provides. This study ascertained that 21% of the GDP growth in mature countries during the previous five years came from the internet (Manyika & Roxburgh, 2011). From the same report the authors put forth information stating that "an average of 3.4% of GDP across large economies" (Manyika & Roxburgh, 2011, p. 3) comes from the internet, economies constituting "70% of global GDP" (Manyika & Roxburgh, 2011, p. 3). Although an interesting study, the details specific to the U.S. economy were not available, which significantly limited its usefulness for this research.

Another attempt at valuation was brought forward by the Internet Associating in 2015. In this report, the author identified important factors like employment growth in 2012 reaching 2.87 million new jobs and sector contribution to GDP reaching $896 billion (Siwek, 2015). Although a robust report, the author did not include secondary contributors to the economy, like jobs that were created to support employees of internet related jobs and GDP contribution from companies that directly support internet related organizations.

A much more recent study forecasts the value of machine-2-machine (M2M) communication to the economy. In this study, conducted by Frontier Economics and presented at the *International Conference on Competition Law and Big Data* in Valencia, Spain, the study results estimated that "over the next 15 years, a 10% increase in M2M connections would increase GDP in…[the U.S. by] $2.26 trillion" (Caldano, 2018) annually. Once again, although a valuable insight, it is predictive in nature, limited only to the impact of the internet of things, only assess the direct economic impact without considering the indirect

effects, and does not broadly assess the value of the total internet today. For these reasons I do not feel that this study's value is relevant to my research.

The most comprehensive and complete report comes from a study conducted by the Harvard University School of Business and was sponsored by the Interactive Advertising Bureau (IAB). The Interactive Advertising Bureau is an organization made up by 650+ of the top "media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns" (*About IAB*, n.d.), while educating and promoting the importance and value of online digital marketing. For this reason, the content of the study could be considered biased because the sponsoring organization benefits from the size, growth, and existence of the internet. However, according to a statement by the authors addressing this concern, "The Interactive Advertising Bureau (IAB) did not control or direct the research or its findings" (Deighton, John; Kornfeld, Leora; Gerra, 2017, p. 2). The study has been conducted every four years since 2008.

Because the 2008 study was the first in the series, the initial results had no data for comparison and analysis to measure change. The 2012 and 2018 reports not only reassessed the same metrics from the 2008 report, but also used previous year(s) data to compare changes as well as forecasting future events in the industry. The studies are entitled *Economic Value of the Advertising-Supported Internet Ecosystem* (Deighton, John; Kornfeld, Leora; Gerra, 2017; Deighton, 2012; Hamilton Consultants; Deighton, John; Quelch, 2009) and provide insight not provided in any other studies found during the literature review. The results of this study can be summarized into two distinct categories: Internet Employment and Growth and Dollar Contribution to U.S. GDP by the Internet.

Internet Employment and Growth. One of the more valuable and enlightening contributions made by this study is the deconstruction of job categories and the assessment and calculation of incremental jobs created as a result of the internet and internet related industries. In each of the three studies, the

authors used a two-tiered system for calculating incremental job creation: “Direct Employment” (Deighton, John; Kornfeld, Leora; Gerra, 2017, p. 6), which refers to jobs that are a direct result of the functioning of the internet, and “Derived Employment” (Deighton, John; Kornfeld, Leora; Gerra, 2017, p. 6), which refers to jobs created in an effort to support the needs of direct employees (e.g., transportation, retail, food services, etc.). As shown in Figure 3, the authors of this study divided employment into 4-5 categories. During the first two studies in 2008 and 2012 the authors chose to use four category types of employment. However, due to significant changes in the structure and services of the internet, the authors felt it necessary to add a fifth category beginning in 2016. The addition of this fifth category did not provide incremental positions not accounted for during the first two studies, but instead provided greater delineation of job details and category specific employment.

Figure 3

Direct U.S. Employment Summary from 2008, 2012, and 2016

Layer	2008 U.S. Employment	2012 U.S. Employment	2016 U.S. Employment
Infrastructure/Hard Infrastructure	140,000	420,000	304,393
Infrastructure Support/Soft Infrastructure	165,000	254,000	662,691
Consumer Services Support	190,000	435,000	1,068,364
Consumer Services	520,000	885,000	1,619,335
Integrated Firms			442,218
Total	**1,015,000**	**1,999,000**	**4,097,001**
Growth in Employment (% per annum compound)		18.5%	19.6%

Note. Reprinted from Economic Value of the Advertising-Supported Internet Ecosystem (Deighton, John; Kornfeld, Leora; Gerra, 2017)

From Figure 3 it is easy to see that direct employment grew by 97% from 2008 to 2012, and from 2012 to 2016 the employment growth rate more than doubled again achieving a rate of 105% increase

over the previous study. This growth is also illustrated through the "Growth in Employment" numbers below the totals. The annualized compound growth from 2008 to 2012 and from 2012 to 2016 was 18.5% and 19.6% per year, respectively.

Additional value from the data generated by these studies is presented in the form of what they authors call derived employment. As explained above, this refers to jobs created in support of the direct employment positions. Interestingly, although not surprisingly, the derived employment numbers are even greater in total number than the direct employment jobs. As shown in Figure 4, derived jobs grow as direct jobs increase with derived jobs representing 67%, 61%, and 61% of total jobs created for 2008, 2012, and 2016, respectively.

Figure 4

All Internet Created U.S. Employment from 2008, 2012, and 2016

	2008 Report	2012 Report	2016 Report
Direct employment due to internet	1,015,000	1,999,000	4,097,000
Derived (indirect) employment	2,035,000	3,101,000	6,286,000
Total employment	3,050,000	5,100,000	10,383,000

Note. Reprinted from Economic Value of the Advertising-Supported Internet Ecosystem (Deighton, John; Kornfeld, Leora; Gerra, 2017)

As an additional point of interest, we can look at the total internet employment as a percent of the entire U.S. employed population. According to the Department of Labor and Statistics, in May 2016 there were 151 million full-time employed people in the U.S. (Bureau of Labor Statistics, 2016b). This means that in 2016 the internet, with total employment of 10.38 million people, represented approximately 6.9% of the U.S. workforce. When compared to other industry sector employment from 2016, the internet is ranked among the top employment sectors in the U.S., eclipsing major sectors like

construction (6.7 million), education (8.3 million), and even agriculture (1.5 million) (Bureau of Labor Statistics, 2016a).

Dollar Contribution to U.S. GDP by the Internet. The second highly valuable content from the *Economic Value of the Advertising-Supported Internet Ecosystem* (2008, 2012, 2016) study is the estimation of the industry's contribution to U.S. GDP in the form of "national income, corporate gross profits, and interest" (Deighton, John; Kornfeld, Leora; Gerra, 2017). Although the total dollar contribution is significant and noteworthy on its own, two other factors worth detailing are the growth rate of the total contribution during the eight-year span of the three studies and the percentage that the contribution represents as a portion of the total GDP.

As shown in Figure 5 below, the growth in contribution by the internet during the periods of study illustrate how rapidly the industry is growing. Between 2008 and 2012 the internet contribution grew at a compounded rate of 15.5%. During the following four years that number increased to a compounded annual growth rate of 20% (Deighton, John; Kornfeld, Leora; Gerra, 2017; Deighton, 2012; Hamilton Consultants; Deighton, John; Quelch, 2009). Each of these growth rates are far greater than the U.S. industry average of 7% (Green, 2017).

Figure 5

Economic Value of the Internet Industry and Its Share of U.S. GDP from 2008, 2012, and 2016

	2008 Report	2012 Report	2016 Report
Contribution of internet to GDP	$300 billion	$530 billion	$1,121 billion
Growth in GDP (% per annum compound)		15.5%	20.0%
Share of Total US GDP	2.1%	3.7%	6.0%

Note. Reprinted from Economic Value of the Advertising-Supported Internet Ecosystem (Deighton, John; Kornfeld, Leora; Gerra, 2017)

It may be surprising if you are looking at this data for the first time, but the internet, as defined by the authors of this report, has been one of the largest contributors to the U.S. GDP over the past decade. As illustrated in Table, ten years ago the internet contributed 2.1% to the U.S. GDP, growing rapidly during the following four years to reach 3.7% of GDP, a growth of slightly more than 76%. Then between 2012 and 2016 the industry saw another four years of incredible growth, reaching 6% of total U.S. GDP, replacing retail as the number three largest industry sector contributor and trailing the construction sector in the number two position by less than a six percent difference in total contribution (Deutsch, 2018). Leading in the number one position is the healthcare spending, which represented 17.9% of U.S. GDP in 2016 (Deutsch, 2018).

Throughout the report the authors discuss the future of the industry and the likelihood for continued growth at similar rates to what has been seen in the previous three reports. However, there are two technologies that are not considered in the reports thus far but that will likely have as much of an impact on the internet industry as the internet has had on the world over the past 20 years. These two technologies are the Internet of Things (IoT) and Artificial Intelligence (AI). The authors acknowledge that their data does not include information about these two technologies, stating that the technologies are “not yet large sites of value or employment” (Deighton, 2012). In the two and a half years since this study was conducted, and the almost two years since it was published, IoT and AI have become much more widespread and pervasive. As an example of the changes during this period, I chose to look at what was being featured and highlighted at the annual technology show in Las Vegas, CES. CES is a technology conference, held annually since 1967, where leading technology companies and experts display, discuss, and explore near-term trends in technology and consumer electronics (*CES Consumer Electronics Show Las Vegas 2019*, n.d.). Each year, the event tends to choose a few areas of technological focus based on the most current or forthcoming trends. In 2016 the event focus was e-commerce and how online shopping was going to change the world (*New at CES 2016: ECommerce*

Marketplace, n.d.), and as we have seen, e-commerce has and does continue to have a huge impact. In 2017 CES focused on continued improvements toward self-driving cars (meaning technology that is assisting drivers, not the concept of fully autonomous cars) and voice assistants/smart home devices (*CES 2017: What to Expect at the Consumer Electronics Show, the Year's Biggest Tech Showcase in Las Vegas - CBS News*, n.d.). 2018 was a year for focusing on wearable technology (all types of wearables, not just smart watches), augmented and virtual reality devices, and drone technology (*CES 2018: Everything You Need to Know about the World's Biggest Tech Show | TechRadar*, n.d.). At the CES show in January 2019, the focus is on two technologies, IoT and AI (*CES 2018: Everything You Need to Know about the World's Biggest Tech Show | TechRadar*, n.d.). And as we have seen with previous CES shows, the event themes or focuses are typically on trends with emerging or relevant technologies that are either already generating significant revenue or are beginning to do so. Therefore, it is not unreasonable to assume that by the time the next report is completed in 2020 the IoT and AI will contribute to another strong upward trend in industry growth, employment opportunities, and GDP input.

Summary

To date, academic research exploring the topic of individual constituent feelings regarding the importance and need for federal legislation to monitor and control the collection and commercialization of PII collected from internet connected personal devices by DROs has seen virtually no activity. However, the topic of individual privacy rights in the U.S. has been an ongoing issue of debate with limited and narrow legislation since revolutionary times. In the absence of traditional academic research, and to ensure that the topic is fully reviewed, I segmented the research into five categories: The History of Privacy in the U.S., Existing U.S. Protection and Oversight, Existing Research, The Omnipresent Internet, and The Economic Value of the Internet.

The review of the history of privacy in the U.S. revealed that concerns about individual privacy dates back to the drafting of the Constitution and were part of the reason for certain delegates demanding that a Bill of Rights be created to amend to the Constitution (*The Bill of Rights: How Did It Happen? | National Archives*, n.d.). Continuing throughout American history, prominent figures like Thomas Jefferson acknowledged the importance of flexible legislation to accommodate changing needs (*Letter from Thomas Jefferson to Samuel Kercheval | Teaching American History*, n.d.), while respected legal experts and future Federal Justices wrote about the importance of federal legislation to protect privacy (Warren & Brandeis, 1890) and ultimately influenced Progressive Era changes, and lastly how landmark civil rights cases provided for significant changes in individuals' privacy throughout the twentieth century (Wikipedia contributors, 2018b, 2018c, 2018a, 2018d, 2018e).

The historical review was followed by an in-depth analysis of all state and federal personal privacy legislation, which revealed that the federal government has taken a limited and sectoral approach to protecting personal data while state legislation varies widely based on the type of protection. While all states have laws to enforce data breach notification, only one state, California, has passed legislation that will go into effect in 2020 and will provide wide reaching protection (*California Consumer Privacy Act of 2018*, 2018).

Only two pieces of research were discovered that addressed the topic of constituent sentiments surrounding the importance of federal legislation to protect individual data privacy. One piece of research covered various topics, including one question about constituent sentiment around the need for legislation, which suggested that constituents were interested in federal legislation to protect privacy (Greenberg Qunilan Rosner Research, 2018). However, when I attempted to discover additional details about the methods used to achieve the results the organization refused to provide greater detail. The second piece of research include two questions pertaining to PII legislation: one asking about interest in

laws to require access to personal data profiles, and another about laws to allow individuals to request deletion of PII.

As a supplementary point of reference, and to provide additional context, I researched the pervasiveness of the internet in the U.S. There is a general consensus that the internet is one of the most significant and influential changes in human history and that it touches virtually everyone and everything, rich or poor, homeless or economically privileged, private companies and state and federal governments (McLeod, 2018; Ryan, 2018). Not surprisingly, in the U.S. we are reaching nearly 100% availability and accessibility of the internet (Bertot, John; Palmer, n.d.). However, because the internet is essentially free, the companies providing the content require something in return, and that is almost inevitably your personal data.

To ensure that everyone understands the magnitude of the internet and its impact on our society, I have provided an assessment of the economic value of the internet, including an estimate of the impact on the job market and the dollar contribution to the GDP. Incredibly, in 2016 the internet employed 6.9% of all people working in the U.S. and represented 6% of the total GDP in the same year (Deighton, John; Kornfeld, Leora; Gerra, 2017).

CHAPTER THREE

METHODOLOGY

This chapter will detail the methodology used to explore the study's research questions, which were focused on gaining insight into voter sentiment about whether federal legislation is necessary for the oversight and control of data reliant organizations (DROs) participating in the collection and commercialization of personally identifiable information (PII) gathered from online activity using personal devices connected to the internet. The chapter contains three sections: (a) a review of the purpose of the study and associated research questions; (b) an explanation of the research design chosen and why that choice was appropriate for this study; and (c) a discussion of the procedures employed to select respondents and to collect and analyze data, along with rationales for using these procedures.

Purpose of the Study/Research Questions

In the United States, the collection and sale of personal data is an industry that is driving the growth and success of many internet companies. However, legislation to monitor and control the industry is still in its infancy, and questions regarding who should be responsible for oversight of organizations trafficking in PII have yet to be resolved.

Considering the depth, detail, and pervasiveness of data collection, it is reasonable to say that individual consumers may not be widely aware of how much information is being collected about them or what is being done with that information (Federal Trade Commission, 2014; Somerville, 2017). Data brokers, who are represented by some of the strongest lobbying entities in Washington (Guynn, 2018), are currently operating in an environment that has little to no oversight due to an almost total lack of legislative oversight. And the governing bodies that can and would have responsibility for ensuring

individual privacy rights are still battling the internal struggles of self-education, the strength of lobbyists opposed to regulation, and the question of whether government regulation is something that individuals need and want. It is the combination of these factors that creates the problem of limited understanding about what direction the U.S. government is moving in terms of creating government regulations surrounding personal data transparency and control. At this point, the future of personal data privacy regulation is unclear at best. And it is this lack of clarity that plainly identifies a need to gain a greater understanding of the current position of constituents, knowledge which will help guide legislators in determining the appropriate legislative direction. This information provides the structure for the purpose of this study, which was to analyze the attitudes and level of interest that constituents had in seeing legislation enacted to monitor and control the collection and commercialization of PII and to protect individual privacy rights.

The following research questions were used to guide the study:

1. To what extent are constituents aware that personal data is being collected about them when their devices are connected to the internet?
2. For those respondents that are aware that such data is being collected, or believe data might be collected, are constituents knowledgeable about what state or federal legislation, if any, exists to monitor and control the collection and commercialization of individuals' PII; in the absence of state or federal legislation, to what extent do respondents feel concern for the lack of legislation; and, do respondents feel that there should be federal legislation in place to monitor and control what and how DROs are collecting and using their personal data?
3. Of the seven demographic factors identified in this survey; party affiliation, state of residence, sex, age, education, race/ethnicity, and community type; which have a significant impact on respondents' level of awareness, knowledge, concern, and desire?

Research Design

This study did groundbreaking research into understanding the sentiments of individual U.S. constituents stand on the topic of the need for federal legislation to monitor and control the collection and commercialization of PII collected from internet connected personal devices. To provide a concise representation for how each of these constituents felt about the topic of federal legislation surrounding PII collection and use, the quantitative research method that was employed represents a combination of exploratory and descriptive research (Pratap, 2018) and utilizes a cross-sectional approach. By providing an overview in three areas—i.e., (a) an analysis of how personal data is monetized by different types of companies, (b) a complete literature review to learn about existing legislation to protect individuals' privacy and a discovery of how privacy rights have developed in the U.S., and (c) an examination into the history and valuation of the internet—a solid foundation was created for the development of a survey instrument containing critical context and literature- and context-informed questions. After the survey instrument was developed, the next phase in this study was to gather responses from survey respondents and provide a description of participant responses to the four identified constructs: awareness of what data is collected about them, knowledge of what legislation exists to protect PII, concern about the lack of legislation, and desire to see legislation enacted. The final step was to use regression analyses to determine what demographic variables contributed most significantly to the measures of each of the four constructs.

Survey Instrument

To gather data relevant to the purpose of this study, I developed a survey instrument that was used to gather information from a sample of the U.S. population of registered voters. The instrument was administered using the online survey tool/service, Qualtrics, and consisted of only quantitative, closed ended questions. The use of an online method of data collection allowed for efficient data collection

and a more rapid data analysis. The list of possible respondents was taken from a market research company's available database. Each respondent was asked to answer a series of qualifying questions to ensure that they met the requirements of living in one of the geographic areas selected for the survey, being a registered voter, and being an active online user.

My intent was to measure four constructs: Awareness, Knowledge, Concern, and Desire. The first two constructs assess knowledge gap areas, while the second two constructs assess interest in current activity. Below are the full construct descriptions and the information that each construct was expected to reveal.

1. Awareness: Awareness, by individual, of the collection of PII by DROs, which is obtained as a result of DROs monitoring individual online activities. Within awareness, an attempt was made to understand constituent familiarity from three perspectives:
    a. What - The What perspective determined to what extent respondents are aware of the fact that data is being collected about them when they are using their personal devices, or even when they are not actively using their devices (Recall the Dormant-Obscure discussion above).
    b. Who - The Who perspective assessed the respondents awareness about the different organizations collecting their data.
    c. Where - The Where perspective evaluated the respondents' awareness of the various places from where their data is collected.
2. Knowledge: Knowledge of what legislation already exists to monitor and control the activities of DROs participating in the collection and commercialization of PII obtained from individual online activity.
3. Concern: Concern about the lack of either state or federal legislation to monitor and control DROs participating in this industry.

4. Desire: Desire for legislation that will provide oversight and control of companies participating in the collection and commercialization of PII obtained from online activities.

All respondents were first prescreened to ensure that they met the minimum requirements for participation. These minimum requirements included being a registered voter in their state of residence with either the Republican or Democratic parties, and, that they consistently access the internet (at least once per month for each of the previous twelve months). After meeting those requirements, and immediately following the screening questions, all remaining respondents received as series of questions to determine general awareness of online personal data collection activities. How respondents answered those awareness questions determined which of three groups they were put into and which logic paths they followed for the balance of the survey.

Group one contained respondents whose answers indicated that they are aware of, or believe that, some data is collected about them during their online activity or while their devices are connected to the internet. Those respondents selected to be in group one were moved on to answer questions in the knowledge construct, the concern construct, the desire construct, and then finished with demographic questions.

Group two contained respondents whose answers indicated that they somewhat believe, or question, whether data is or is not collected about them during their online activity or while their devices are connected to the internet. Those respondents selected to be in group two also moved on to answer questions in the knowledge construct, the concern construct, the desire construct, and then finished with demographic questions. The only difference between the paths of group one and group two was terminology used in the questions they were given.

Group three consisted of respondents whose answers in the awareness construct indicated that they did not believe that any data is collected about them or their online activities. To be selected for

inclusion in group three meant that after completing all questions in the awareness construct, participants received a single qualifying question to confirm that they definitively did not believe that any data is collected about them while using their internet connected personal devices. If respondents confirmed that they did not believe any data is collected about them, they were sent to the demographics questions and then exited from the survey. The decision to only collect demographic data from this group of respondents and then exit them from the survey was based on their belief that online data collection does not take place. It would have been unproductive to collect responses relating to knowledge, concerns and desires from individuals who made it clear that they do not believe data collection practices exist. For those respondents who answered the single qualifying question differently, suggesting that they were not sure whether or not data was being collected about them, the survey redirected to join respondents in group two.

The overall path that groups one and two followed were virtually identical paths. Both groups received the same questions, but the terminology of the questions for each group were modified slightly to ensure that the content of the questions did not call into question the beliefs of either group.

Using survey logic, group one received questions that explored their general knowledge of data collection practices and existing personal data privacy legislation, their concerns about the activities of data brokers and data collectors and individuals' limited access to the profiles created about them, and whether there is a desire for additional legislation to protect individual privacy. Because respondents in group one self-identified as believing that data is collected about them, respondents had their beliefs confirmed and they were introduced to the existence of data brokers and data collectors, as well as definitions for both and how the data is used and stored. Unique from group two, group one received questions specific to the activities of data brokers and data collectors and how data is collected and commercialized. Throughout their survey experience, group one respondents were presented with questions that acknowledge data collection practices and inquired about their depth of knowledge,

concern, and wishes regarding the collection and commercialization of their personal data. The questions and statements in the survey exposed each respondent, for the first time during the survey, to facts that may increase their understanding of the data collection and commercialization industries.

Using logic like that applied to group one, group two received questions based on their responses to questions from the awareness construct. Group two respondents were also queried about their knowledge, concerns, and desires pertaining to data collection, but with two distinct differences: respondents in group two were not told of the existence of data brokers and data collectors, and they were not asked about the activities of these two industry operators. The questions they received questioned whether laws exist to oversee the activities of companies that collect data or protect individual rights. However, unlike group one, group two respondents were not informed that entire industries exist to collect and monetize data. Questions pertaining to the collection of PII were designed to allow respondents to continue to hold their beliefs questioning if or how much data is being collected. The questions did, however, inform them of whether legislation currently exists to protect individual privacy and they were asked about their knowledge on the topic.

The objective of the questions given to groups one and two were to assess the sentiments of constituents' feelings about protection of personal privacy rights, even in the absence of factual knowledge about from where and how much personal data is being collected. To review all questions in detail, see Appendix A.

Format

The survey was designed to consist exclusively of closed-ended questions using response formats that will include rating scale questions (e.g., Likert scale, ranking systems, etc.), dichotomous questions, and multi-option/multi-response questions. As mentioned above, the survey began with two screening questions. The first screener question determined if the respondent is a regular internet user. The

second screener question was used to determine if the respondent was a registered voter in their state of residence during the previous two years. Once respondents had been qualified to participate, meaning they were identified as registered voters who are also consistent users of the internet, the next priority was to find respondent representation from both republican and democratic parties. The final priority was to obtain respondents representation from as many of the categories within each of the demographic factors as possible (i.e., sex, age, education, race/ethnicity, and community type). This approach provided for both an expedient completion rate for the surveys as well as a representative sampling of constituents. As Appendix A indicates, there were a total of 43 survey questions for Groups One and Two. As outlined above, not all respondents answered all 43 questions and the total number of questions for each respondent was dictated by the answers they provide for certain logic-action questions. All respondents in Groups One and Two answered between 37 and 43 questions. Respondents who were part of Group Three, and who were redirected back into Group Two after answering the qualifying question, answered a total of between 38 and 44 questions. Included in the total number of possible questions were six demographic questions. See Appendix B for a list of all six questions.

Answering the Research Questions

1. To what extent are constituents aware that personal data is being collected about them when their devices are connected to the internet?

To answer this question, the ten survey questions that make up the Awareness construct were used to generate a score for each respondent. The answers to each of the ten questions were assigned a value between zero and one. Respondents who chose an answer that demonstrated no awareness of the type of data collection being addressed in a question were given a score of zero for that question. Respondent who chose an answer(s) that demonstrated a partial, but not complete knowledge of the

topic, were given a score with a value greater than zero but less than one for that question. And for respondents who chose the most factual and accurate answer, demonstrating full awareness, they were given a score of one for that question. The minimum score that any respondent could receive for a question was zero, and the maximum score was one. Two of the ten questions were conditional questions. Conditional questions are used to gain more detail about the respondents' depth of knowledge about a topic. However, if a respondent demonstrated in the question preceding a condition question that they have no awareness of the topic, a conditional question would provide no value as they had already demonstrated a zero level of awareness. For this reason, when conditional questions were not presented to respondents, it meant that respondent was assigned a value of zero for the conditional question and that zero was added to their cumulative Awareness construct score. When analyzing all answers from the Awareness construct, each respondent's score was calculated by adding up the individual scores from each of all ten questions. The minimum possible score for the Awareness construct was zero and the maximum score was ten. A score of zero for the Awareness construct would indicate that a respondent has a complete lack of awareness about data collection or that the respondent does not believe data is being collected about them from the options presented. A score of ten would indicate that a respondent has a complete awareness about data collection and is familiar with the practices of data collection that are addressed in each of the ten Awareness construct questions.

2. Are constituents knowledgeable about what legislation, if any, exists to monitor and control the collection and commercialization of individuals' PII? Are constituents concerned about the lack of legislation to oversee DROs and to protect their privacy? Are respondents desirous to see legislation enacted to monitor the activities of DROs and to protect the PII of individuals?

The three sub-questions within this second question were answered in much the same way as with the first research question, beginning with the score assignment process. Each of the three sub-

questions represented here are respectively associated the remaining three constructs: Knowledge, Concern, and Desire.

For the Knowledge construct there were eight possible questions, resulting in a possible score for each respondent of between zero and eight. No conditional questions were present in the Knowledge construct questioning.

For the Concern construct, there were a maximum of seven possible questions, with one question being conditionally delivered to respondents. This meant that there was a minimum possible score of zero and a maximum possible score of seven.

The final sub-question assessed the desire of each respondent and included a total of seven possible questions, four of which were conditional. This resulted in a score for the Desire construct of a minimum of zero and a maximum of seven.

3. Of the seven demographic factors identified in this survey; party affiliation, state of residence, sex, age, education, race/ethnicity, and community type; which have a significant impact on respondents' level of awareness, knowledge, concern, and desire?

To address this question, stepwise regression analysis was used to explain constituent variation in the four constructs (Awareness, Knowledge, Concern, and Desire) using the identified demographic measures of party affiliation, state of residence, sex, age, education, race/ethnicity, and community type. While the constructs served as the dependent variables in a series of four multiple regression models, the independent variables were a mix of continuous (e.g., age) and discreet variables (e.g., party affiliation and sex). Taken together, these models allowed for the identification of variables significantly correlated (at the $p \leq .05$ level) with the individual constructs, the calculation of an effect size associated with each of the significant variables, and finally, providing an overall estimate of the amount of variation in the constructs explained by the models.

Survey Respondent Selection

There are numerous approaches to addressing the question of how individuals feel about the topic of legislation to protect PII. However, in an attempt to ensure that this research was targeted and defensible, I chose to narrow this first survey to a representative sample of voters, discussing only the topic of federal legislation, and exclusively focusing on PII collected from individual online activity gathered while individuals are using personal digital devices. Future research can approach the topic from a myriad of other perspectives.

Respondent Selection Summary

The objective was to obtain as many complete survey responses as possible from the list of possible respondents in the database used for this research. The criteria for the sampling of respondents was created without consideration of the database limitations, and instead focused on attempting to find a representative sample. The geographic distribution of the surveys was from six U.S. states. The six states included, in descending order based on population: California, Texas, Florida, New York, Ohio, Georgia.

Explanation of Selection Criteria

Total Weight of Influence. All six states fall within the top ten most populous U.S. states (*US States - Ranked by Population 2018*, n.d.), meaning that these states would heavily influence the passing or vetoing of federal legislation if a bill were proposed in congress to monitor and control the collection and commercialization of PII by DROs. All of the information used to assess each of the six states was determined during the data collection period, which was at the end of 2019 and prior to the 2020 presidential elections.

California and New York: Feeling Blue. In the past four presidential elections, California and New York have both cast their electoral votes for the democratic candidate (*Historical Presidential Election Information by State*, 2019), meaning they are considered Blue States (Wikipedia contributors, 2019a). These states also have a majority of House representatives (*Directory of Representatives | House.Gov*, 2019), and both Senate seats (*U.S. Senate: Our States*, 2019), that are affiliated with the Democratic party and would likely lean toward the positions and sentiments of democratic voters and the democratic party

Texas and Georgia: In the Red. In the past four presidential elections, Texas and Georgia have both cast their electoral votes for the republican candidate (*Historical Presidential Election Information by State*, 2019), meaning they are considered Red States (Wikipedia contributors, 2019a). These states also have a majority of House representatives (*Directory of Representatives | House.Gov*, 2019), and both Senate seats (*U.S. Senate: Our States*, 2019), that are affiliated with the Republican party and would likely lean toward the positions and sentiments of republican voters and the republican party

Florida and Ohio: Straddling the Line. Florida and Ohio have been somewhat party agnostic in the past four presidential elections (*Historical Presidential Election Information by State*, 2019). Both states gave their electoral votes to the democratic candidate in two of the past four elections and to the republican candidate in the other two elections. Iowa is the only other state to fall into this category. In addition:

- Florida registered voters are almost equally distributed, with 37.3% registered as Democrats and 35.3% registered as Republicans (*Registered Voters by State*, 2018). And although the state's federal representation has a majority of its current House of Representatives aligning with the Republican Party (16 Republicans and 11 Democrats), its senate seats are split with one Republican senator and one Democratic senator (*U.S. Senate: Our States*, 2019).

- Ohio registered voters are also almost equally distributed, with 40% registered as Democrats and 42% registered as Republicans (*Registered Voters by State*, 2018). And although the state's federal representation has a majority of its current House of Representatives aligning with the Republican Party (12 Republicans and 4 Democrats), its senate seats are split with one Republican senator and one Democratic senator (*U.S. Senate: Our States*, 2019).

State Positioning. Leveraging a 2018 study ranking all 50 states on a scale of 0-100, with zero being no state legislation in place to protect consumer online data privacy and 100 being legislation in place across 20 categories of online data privacy, Comparitech (Bischoff, 2018) found five out the six states selected for the survey sampling received very similar scores ranging from 30-40. California ranked significantly higher than the other five with a score of 75, due in large part to the passing of the Consumer Data Privacy Act (*California Consumer Privacy Act of 2018*, 2018) in June of 2018.

The belief was that in allowing for factors including Representative presence in Congress, geographic location, and state history of party affiliation (or lack thereof), in combination with a demographic sampling of the population, I have been able to obtain a fair representation of the sentiments of the total population.

Sampling Rationale

In an effort to ensure that the results of this study were representative of the population parameter, I attempted to employ a proportionate stratified random sampling method (Ross, 1978) with strata representing party affiliation, state location of voter registration, sex, age, education, race/ethnicity, and community type (rural, suburban, and city). An argument could be made to use a non-probability, convenience sample of the population to simplify the process of this initial study. However, in my opinion, the reliability limitations of a convenience sample approach, as well as arguments of possible bias, would be so great as to render the data analysis open to far too many challenges and objections.

The final sample was ultimately dictated by the available responses from the databased used to gain survey responses. Ultimately, respondents from each of the classes within the seven strata were included in the sampling, but a proportionate stratified sample was not possible for this survey.

Survey Demographics & Distribution

Within each of the six states, every effort was be made to obtain a proportionate representative sampling of respondents. Proportionate stratified random sampling is designed to ensure that the observations used in the sample reflect the actual proportions that exist in the population (Ross, 1978). For this sample, data gathered from the U.S. Census on each of the six states was be used to determine the parameters of the stratified sample of respondents. The five demographic factors, not including party affiliation or state of residence, are: Sex (male/female), Age (ranges up to 65+, beginning with 18), Education (from “did not attend or finish high school” to “doctoral degree”), Race/Ethnicity, and Community Type (urban, suburban, rural). When executing the survey, I was aware that it was unlikely that with a target sample size of 1,200 total responses distributed across six states, that all five demographic factors would be represented in proportions similar to those reported in the most recent Census, but every attempt was be made to find respondents from each category within the chosen demographic factors.

Regardless of the political leaning of the individual states, each state followed the same format for respondent selection. As mentioned above, although the goal was a proportionate stratified random sample, the was ultimately unattainable. Instead, I took as many respondents as I was able to obtain for each of the six states.

Significance of the Study

Arguably, exploratory research is the prologue to, and a required component of, any study and could therefore be considered unnecessary to mention under typical circumstances. However, I believe that in this study exploratory research was more uniquely critical than the typical and is therefore worthy of discussion. My reasoning for this sentiment is due in large part to the significant role that privacy plays in the history of the formation of the U.S. As defined by Kotler and Armstrong exploratory research has the objective of "gather[ing] preliminary information that will help define problems and suggest hypotheses" (Kotler & Armstrong, 2006, p. 122). In the case of this study, the exploratory component provides valuable insight into understanding why privacy was virtually an expected right of citizens in the U.S. As far back as the drafting of the Constitution, or more specifically, the Bill of Rights, the concept of the right to privacy has been an important concern and hotly debated topic for citizens of this country (Finn, 2006). This has been followed by more than 200 years of continuous challenge and question regarding what privacy rights are inalienable, which are grantable, and which are not available. If not for the historical context that was discovered through the exploratory research phase, the resulting framework, constructs, hypotheses, survey instrument, and even the problem statement itself would have been materially different from what has been produced. It is for these reasons that I believe honorable mention should be given to the critical phase of exploratory research.

This survey was intended to explore the level of awareness of constituents about this topic, gaining insight into constituents knowledge of how their collected data is being used, whether they know of the existence of state or federal legislation to monitor and/or control the industry, exploration into the existence and level of concerns about PII data collection and the absence of protective legislation, and how they rate its importance in their personal lives. Distinct from these questions will be an assessment of whether constituents believe that Washington should be focusing on this issue at all or whether they believe it is something that wastes the limited resources of their tax dollars.

Based on the nascency of this topic, it is difficult to specifically identify who the greatest beneficiaries of the research will be. However, it is certain that several different groups will each be able to obtain some level of value from this research. These groups include: legislators, the general public, other researchers, and even the DROs participating in the commercialization of PII.

The expectation is that this study will be the first in a series of studies on personal data privacy protection. With a continued focus on legislation, future research will explore the positions of federal and state legislators about controlling data collection and commercialization and whether legislators are aligned with constituents on the importance of these topics. Also of interest will be research to better understand the depth to which individuals are aware of how much, and from where data is being collected about them and their personal activity. Future research opportunities will address how constituents feel about the following topics: the collection and use of biometric data, the generation and use of data from smart home devices (not just Amazon Echo and Google Home, but smart appliances, thermostats, and vacuum cleaners that are creating 3-D models of your home, and other Internet of Things devices), the generation and use of data from transportation (personal cars, public transportation, air/train/bus travel), the collection and use of data from smart clothing (a rapidly growing sector), and whether enough is being done to ensure data security and to prevent breaches of databases storing PII. One other piece of research that can be generated without collecting additional data is an assessment of respondents based on zip codes. In an effort to verify respondents' geographic location, respondents were required to provide their zip codes. This information will allow for future research to include overlaying known data about populations within zip codes to provide further insight into leanings by geographic location.

Although all of the ideas for future research are interesting, without first developing a foundation of understanding of how individuals feel, the future research would have limited value. For this reason,

this first study to better understand how individuals feel about the topic of legislation to protect PII is critical to being able to build upon it in future research efforts.

CHAPTER FOUR

RESULTS

This chapter contains the results of the quantitative research that was conducted to discover the answers to the following proposed research questions:

1. To what extent are constituents aware that personal data is being collected about them when their devices are connected to the internet?
2. For those respondents that are aware that such data is being collected, or believe data might be collected, are constituents knowledgeable about what state or federal legislation, if any, exists to monitor and control the collection and commercialization of individuals' Personally Identifiable Information (PII); in the absence of state or federal legislation, to what extent do respondents feel concern for the lack of legislation; and, do respondents feel that there should be federal legislation in place to monitor and control what and how data reliant organizations (DROs) are collecting and using their personal data?
3. Of the seven demographic factors identified in this survey; party affiliation, state of residence, sex, age, education, race/ethnicity, and community type; which have a significant impact on respondents' level of awareness, knowledge, concern, and desire?

To present a clear and comprehensive overview of the results of this study, this chapter will follow a format that begins with outlining the procedures used to gather data from the sample population. This will be followed by a descriptive analysis of the results for each of the assessed demographic factors, a summary of each construct's reliability, and an answer to each of the three research questions. The chapter will end with an explanation of the results of the regression analysis that was used to identify statistically significant demographic factors correlated with each of the four constructs.

In this chapter I will also demonstrate how a combination of exploratory and descriptive research (Pratap, 2018) has been employed utilizing a cross-sectional approach, for the purpose of analyzing the attitudes and level of interest that constituents have in seeing legislation enacted to monitor and control the collection and commercialization of PII and to protect individual privacy rights. It further examines attitudes within four constructs; Awareness, Knowledge, Concern, and Desire, to identify how demographic factors affect individual attitudes.

Participants and Procedures

The database of possible respondents used for this research came from a mystery shopping company's database of all mystery shoppers in the U.S. From the existing database of mystery shoppers, all known shoppers registered as living in the six states selected for the survey were exported into a new distribution database. There were no other criteria to filter who was included in the database, as the qualifier and demographic questions would provide all additional details necessary to ensure that respondents fit the participant requirements.

An email was sent out in early February 2020 to the new distribution database of approximately 10,000 people. The email contained an explanation of the request to participate in the survey and a link to the survey instrument. The objective was to obtain as many responses as possible from the chosen database, based on the limitations set forth in the sampling criteria: must live in California, Texas, Florida, New York, Ohio, or Georgia; must have been a registered voter with either the Democratic or Republican party in 2018 or 2019; and must have accessed and used the internet at least one a month during the 12 months prior to taking the survey. The only other requirement was that for a respondent's answers to be included in the analysis, the respondent was required to complete the entire survey. The survey sent out to a database of approximately 10,000 individuals and remained

open for email recipients to complete for two weeks. Based on these criteria, there were a total of 892 surveys completed and analyzed for this study.

Sample Demographics

For the purposes of both efficiency and single-source referencing, Figure 6 displays the frequencies and percentages associated with the seven demographic factors assessed in the survey: Political Affiliation, State of Residence, Sex, Age, Education, Ethnicity, and Community Type. Each cell is divided diagonally, with the number in the upper left representing the frequency and the number in the lower right representing the percentage of the total. The sections following Figure 6 discuss in detail each of the seven factors separately.

Figure 6

Descriptive Summary of All Sampling Results

Summary of Survey Respondents Political Affiliation and Five Demographic Factors							
	All States	California	Texas	Florida	New York	Ohio	Georgia
RESPONDENTS							
Totals	892 / 100%	254 / 30%	209 / 23%	140 / 16%	91 / 10%	118 / 13%	80 / 9%
PARTY							
Democrat	497 / 56%	161 / 63%	86 / 41%	82 / 59%	57 / 63%	60 / 51%	51 / 64%
Republican	395 / 44%	93 / 37%	123 / 59%	58 / 41%	34 / 37%	58 / 49%	29 / 36%
SEX							
Female	689 / 78%	190 / 75%	163 / 78%	109 / 78%	65 / 71%	95 / 81%	67 / 84%
Male	203 / 23%	64 / 25%	46 / 22%	31 / 22%	26 / 29%	23 / 19%	13 / 16%
AGE							
18 - 24	17 / 2%	3 / 0.1%	5 / 2%	1 / 0.7%	2 / 2%	5 / 4%	1 / 1%
25 - 38	253 / 28%	64 / 25%	64 / 31%	32 / 23%	29 / 32%	35 / 30%	29 / 36%
39 - 54	294 / 33%	99 / 39%	63 / 30%	38 / 27%	28 / 31%	40 / 34%	26 / 33%
55 - 65	213 / 24%	57 / 22%	47 / 23%	41 / 29%	22 / 24%	26 / 22%	20 / 25%
Over 65	115 / 13%	31 / 12%	30 / 14%	28 / 20%	10 / 11%	12 / 10%	4 / 5%
EDUCATION							
Attended/graduated high school	66 / 7%	20 / 8%	17 / 8%	7 / 5%	10 / 11%	9 / 8%	3 / 4%
Some college credit, no degree	199 / 22%	53 / 21%	45 / 22%	30 / 21%	21 / 23%	34 / 29%	16 / 20%
Trade/technical/vocational training	54 / 6%	19 / 8%	14 / 7%	6 / 4%	3 / 3%	4 / 3%	8 / 10%
Associate's degree	110 / 12%	32 / 13%	26 / 12%	17 / 12%	13 / 14%	14 / 12%	8 / 10%
Bachelor's degree	294 / 33%	86 / 34%	63 / 30%	51 / 36%	33 / 36%	36 / 31%	25 / 31%
Master's degree	136 / 15%	30 / 12%	39 / 19%	20 / 14%	10 / 11%	19 / 16%	18 / 23%
Doctorate or Professional degree	33 / 4%	14 / 6%	5 / 2%	9 / 6%	1 / 1%	2 / 2%	2 / 0.3%
ETHNICITY							
White	610 / 68%	151 / 60%	147 / 70%	106 / 76%	64 / 70%	103 / 87%	39 / 49%
Hispanic or Latino	80 / 9%	44 / 17%	19 / 9%	9 / 6%	6 / 7%	1 / 0.8%	1 / 1%
Black or African American	127 / 14%	21 / 8%	28 / 13%	21 / 15%	16 / 18%	7 / 6%	34 / 43%
Native American or American Indian	5 / 0.6%	2 / 0.8%	1 / 0.5%	0 / 0%	1 / 1%	0 / 30%	1 / 1%
Asian / Pacific Islander	37 / 4%	22 / 9%	8 / 4%	1 / 0.7%	2 / 2%	2 / 30%	2 / 3%
Other	33 / 4%	14 / 6%	6 / 3%	3 / 2%	2 / 2%	5 / 30%	3 / 4%
COMMUNITY							
City/Urban	360 / 40%	121 / 48%	76 / 36%	57 / 41%	37 / 41%	44 / 30%	25 / 31%
Suburban	411 / 46%	107 / 42%	98 / 47%	72 / 51%	37 / 41%	49 / 30%	48 / 60%
Rural/Farm	121 / 14%	26 / 10%	35 / 17%	11 / 8%	17 / 19%	25 / 30%	7 / 9%

Political Affiliation

The initial thought was that an equal representation of Democrats and Republicans would have provided a good mix for this study. However, the final distribution from the total sample turned out to be more interesting. Of the 892 completed surveys included in this study, 497 were completed by registered Democrats and 395 were completed by registered Republicans. This represents a percentage distribution of 56% Democrat and 44% Republican. Interestingly, this distribution aligns very closely with the national distribution of registered Democrats and Republicans. According to the Pew Research Center (*The 2020 Electorate by Party, Race, Age, Education, Religion: Key Things to Know | Pew Research Center*, n.d.), from the national pool of registered voters who identify as either Democrat or Republican, 54% identify as Democrat and 46% identify as Republican. Therefore, the distribution of Democrats and Republicans in this sample suggests that the representation is appropriate when compared to the total population of registered voters.

When examining the party affiliation by state, there were a couple of surprises, but nothing concerning. As expected, California and New York respondents leaned more heavily toward Democrat vs. Republican, with a distribution of 63% Democrats responding and 37% Republicans responding from both states. In addition, as expected, Texas leaned more right with 41% of respondents being registered Democrats and 59% registered Republicans. Ohio, selected as one of two middle-of-the-road states, resulted in 51% Democrat responses versus 49% Republican. The other middle-of-the-road state selected was Florida, which produced a larger than expected Democrat representation at 59% versus 41% Republican. The difference is not concerning and simply warranted mention as it was identified as one of the two middle-of-the-road states. The final state, Georgia, produced the greatest surprise. Georgia, along with Texas, was identified as a red state based on its history of voting and congressional representation. However, the distribution of respondents was weighted heavier for Democrats with

64% of respondents identifying as registered Democrats and 34% as registered Republicans. Much like the Florida difference, there is no concern about representation for either party.

State of Residence

In addition to the summary information presented in Figure 6, I have created Table 2, which directly compares each state's sample representation in the survey to each state's total representation in the U.S. population. As seen in Table 2, 30% of all survey respondents came from California. According to the U.S. Census Bureau's 2019 population estimates (*US States - Ranked by Population 2021*, n.d.), California represented 30% of the total U.S. population. Similar results can be seen for Texas (Survey: 23%, Population: 22%), Florida (Survey: 16%, Population: 16%), and Georgia (Survey: 9%, Population: 8%). The two states that are not as well aligned with the U.S. population percentages are New York (Survey: 10%, Population: 15%) and Ohio (Survey: 13%, Population: 9%). However, the number of respondents from New York and Ohio were not so low as to be concerning, coming in at 91 and 118, respectively.

Sex

The mix of female to male respondents, although heavily weighted toward female, does not come as a surprise when considering the database from which the potential respondents were mined. According to Zippia (*Mystery Shopper Demographics and Statistics - Zippia*, n.d.), a careers website, the average distribution of female to male mystery shoppers in the U.S. is 70% and 27%, respectively (3% were identified as unknown). Therefore, when analyzing this survey, the results of 77% of respondents being female and 23% being male was not an unexpected outcome albeit a potential limitation to the study.

At the state level, four of the six individual states saw very similar results, except for Ohio and Georgia. Both of these states saw slightly higher female respondent percentages, coming in at 81% and

84%, respectively. Although not an ideal mix, especially for the 16% male respondent rate in Georgia, it is a known and acknowledged limitation.

Age

Age groupings were selected based on commonly accepted age ranges for Gen Z (only those over 18), Millennials, Gen X, Baby Boomers, and everyone over 65 years of age (*Where Millennials End and Generation Z Begins | Pew Research Center*, n.d.). Excluding the youngest group, each of the other age ranges had a fair representation of respondents: 25-38 years old having the second highest respondent rate with 253, 39-54 years old having the highest respondent rate with 294, 55-65 coming in third with 213 respondents, and Over 65 delivering 115 respondents. The age group 18-24 only produced a total of 17 responses. Although disappointing, this number was not a surprise. According to Zippia (*Mystery Shopper Demographics and Statistics - Zippia*, n.d.), mystery shoppers in the age range of 20-30 years old only make up 10% of the mystery shopper population, with the number of shoppers increasing as the age range increases. Therefore, the fact that this survey resulted in 2% of all responses coming from people between the ages of 18 and 24 does not come as a surprise. Once again, this is a known and acknowledge limitation in the response dataset.

Education

The distribution across all education levels was of particular interest for this study. With the known limitations of the database used, and the six education level groups ranging from high school through doctorate, there was concern that one or more groups might not have enough respondents to warrant inclusion in the study. Fortunately, all groups had numbers sufficient to include, with doctorate/professional respondents producing the fewest surveys at 33 (4% of the total) and Trade/technical/vocational school and Attended or graduated high school coming in second and third

from last at 54 (6% of the total) and 66 (7% of the total) respondents each, respectively. The remaining four education groups had strong showings with more than 100 respondents each.

Ethnicity

For this study, six response options were provided to respondents for the question asking about ethnicity. However, one of the six options was "Other," which allowed respondents who did not identify with any of the five ethnicities to have an option. For the purposes of this study, and because I have no detail on how each respondent defined "Other," the Other category was not included when assessing the impact of ethnicity on the study questions. For the remaining five ethnic groups, only one had response numbers that were too low to include in the analysis. Native American or American Indian produced only five responses, or 0.6% of the total responses. Lastly, a known and acknowledged limitation of the database of respondents used for this study is that it is a database of mystery shoppers. According to Zippia (*Mystery Shopper Demographics and Statistics - Zippia*, n.d.), the distribution of ethnicities within the mystery shopper community is predominantly white, with representation consisting of 74.7% White, 7.8% Hispanic or Latino, 6.1% Black or African American, 0.5% American Indian or Alaska Native, 8.7% Asian, and 2.2% Unknown. Therefore, it is not a surprise that the results of this survey produced responses that were somewhat consistent with Zippia's data, showing results of 68% White, 9% Hispanic or Latino, 14% Black or African American, 0.6% Native American or American Indian, 4% Asian / Pacific Islander, and 4% Other.

Based on the responses received, White, Hispanic or Latino, Black or African American, and Asian / Pacific Islander were included in the final analysis. As mentioned above, both Native American or American Indian and Other were excluded.

Community Type

The results from the community types were straightforward. Forty percent of all responses came from respondents living in a City/Urban community, 46% came from Suburban dwellers, and 14% from Rural/Farm communities.

Table 2

Comparison of Survey Respondents to U.S. Population as a Percentage

Variables	All States	California	Texas	Florida	New York	Ohio	Georgia
State % representation within survey sample							
n=892	100%	30%	23%	16%	10%	13%	9%
State % representation of actual U.S. population							
N=328mm	100%	30%	22%	16%	15%	9%	8%

Construct Data Reliability

One of the objectives of this study was to generate data that can be used to assess individual constituent interest in seeing federal legislation enacted to monitor and control the activities of DROs while also providing protection for individual PII. In order to accurately assess that level of desire in each respondent, it was first important to understand each respondents' level of awareness of what data is being collected, their knowledge of what legislation already exists, and what level of concern each respondent has when they are told about what legislation does (or does not) exist. It is these three assess areas, in conjunction with the assessment of desire, that make up the four constructs measured in this study.

To achieve the measurement objective, and to provide a solid foundation for future research, it was necessary for the data generated by the survey instrument to be considered reliable. For that reason, each construct was assessed using Cronbach's alpha measure of reliability; this ensured that the

grouping of questions used to form each construct produced the greatest reliability score. Although minimum threshold scores of reliability tend to vary by individual and discipline, some research promotes that a Chronbach alpha score of between 0.6-0.7 is considered good and reliable for the social sciences (Ursachi et al., 2015) (Ghazali, 2008). For that reason, I assessed the reliability of each of the four constructs with a minimum threshold α score of 0.6.

As a reminder, question one of this study looked to understand the level of awareness for all respondents. Similarly, question two asked about respondents' level of knowledge, concern and desire. Therefore, in an effort to provide a logical flow to the data analysis and results, I will answer the first of the three study questions after providing the reliability results for the Awareness construct. Then, after sharing the reliability results for the Knowledge, Concern, and Desire constructs, I will answer question two of the study. The third question is unique from questions one and two, and I will therefore answer question three after sharing the regression analysis results.

Awareness Construct

The first construct measured by this instrument assessed individuals' awareness by identifying their level of understanding about what type, who, and from where PII is being gathered during online activity. Each respondent answered between eight and ten questions to produce an awareness score. The resulting Cronbach's alpha reliability score that was generated by the ten possible questions was 0.73. This score exceeds the minimum alpha coefficient threshold of 0.06 and meets this study's requirements for internal consistency reliability.

Answering Research Question 1

The first of the three research questions in this study sought to identify how aware respondents are that data is being collected about them while they are online. As outlined in chapter three, each survey question within each construct is assigned a possible score between zero and one, assessing the

respondent's level of understanding or interest for that construct. When respondents have finished all of the questions within a construct, their total score is calculated. Because there are a total of ten questions in the Awareness construct, each respondent has the opportunity to receive a score of between zero and ten. Although there is no standard scale for what is considered low to high scores, for the purposes of this research, I have assigned the scale in Table 3 for Awareness construct scores. The rationale for the scoring is an attempt to show that respondents who received a score equivalent to less than 60% (+/- 5%) of the maximum available score were considered at the bottom of the group. Those respondents that received a score equivalent to >60%, but less than <75% (+/- 5%), were at a basic level. Those respondents that received a score equivalent to >75%, but less than <90% (+/- 5%) were at an adequate or intermediate level. And those respondents that received a score equivalent to >90% (+/- 5%) were at a high or superior level. This system of scoring was applied to Tables 4, 5, and 6 as well. Table 3 also shows the percentage of respondents who achieved each of the possible score groups.

A total of 10.1% of all respondents scored below 6.0 points, corresponding to a Poor/Low Awareness. An additional 18.9% of respondents scored between 6.0 and 7.25 points, corresponding to a Basic Awareness of data collection. The third level of awareness of online data collection is considered Adequate, representing a total of 38.8% of all respondents. As the final score on the Awareness Scale, 32.2% of all respondents achieved a level of Superior Awareness. In total, 71% of all respondents had either an adequate or superior level of awareness about from where and the type of data being collected about them while they are using an online connected personal device. The remaining 29% of the sample population demonstrated a less than adequate level of awareness.

Table 3

Awareness Scale and Respondent Percentages

Rating	Range	Respondent %
Poor/Low Awareness	0.0 – 5.75 points	10.1%
Basic Awareness	6.0 – 7.25 points	18.9%
Adequate Awareness	7.5 – 8.75 points	38.8%
Superior Awareness	9.0 – 10.0 points	32.2%

Note. N = 892.

Knowledge Construct

The second construct measured by this instrument assessed individuals' knowledge of whether legislation exists to monitor and control the activities of DROs collecting and commercializing PII and the rights of individuals to know what information is collected. Each respondent answered eight questions to produce a knowledge score. The resulting Cronbach's alpha reliability score that was generated by the eight possible questions was 0.76. This score exceeds the minimum alpha coefficient threshold of 0.06 and meets this study's requirements for internal consistency reliability.

Concern Construct

The third construct measured by this instrument assessed individuals' concern about the lack of any legislation to monitor the business practices of DROs. Each respondent answered seven questions to produce a concern score. The resulting Cronbach's alpha reliability score that was generated by the seven possible questions was 0.90. This score exceeds the minimum alpha coefficient threshold of 0.06 and meets this study's requirements for internal consistency reliability.

Desire Construct

The fourth construct measured by this instrument assessed individuals' desire to see legislation enacted to monitor and control the activities of DROs collecting and commercializing PII and to provide rights for individuals to have some control of what data is collected and how it is used. Each respondent answered seven questions to produce a desire score. The resulting Cronbach's alpha reliability score that was generated by the seven possible questions was 0.61. This score exceeds the minimum alpha coefficient threshold of 0.06 and meets this study's requirements for internal consistency reliability.

Answering Research Question 2

As addressed earlier in this chapter, question two has three sub-questions within it that require answering separately. Each of these three sub-questions relates to each of the remaining three constructs. Below are the answers to each of the three sub-questions.

Sub-question A. The first of the three sub-questions in this study sought to identify how much knowledge each respondent had about what legislation already exists to monitor and control the activities of DROs participating in the collection and commercialization of PII obtained from individual online activity. Possible scores for respondents had a range between zero and eight. Just as with the awareness measure, although there is no standard scale for what is considered low to high scores, for the purposes of this research, I have assigned the scale in Table 4 for Knowledge construct scores. Table 4 also shows the percentage of respondents who achieved each of the possible score groups.

A total of 57.3% of all respondents scored below 5.0 points, corresponding to a Poor/Low Knowledge. An additional 20.1% of respondents scored between 5.0 and 5.50 points, corresponding to a Basic Knowledge of data collection. The third level of knowledge of existing legislation is considered Adequate, representing 13.2% of all respondents. As the final score on the Knowledge Scale, 9.4% of all respondents achieved a level of Superior Knowledge. In total, 22.6% of all respondents had either an

adequate or a superior level of knowledge about what legislation does or does not exist to protect individual data privacy. The remaining 77.4% of the sample demonstrated a less than adequate level of knowledge.

Table 4

Knowledge Scale

Rating	Range	Respondent %
Poor/Low Awareness	0.0 – 4.75 points	57.3%
Basic Awareness	5.0 – 5.50 points	20.1%
Adequate Awareness	6.0 – 6.5 points	13.2%
Superior Awareness	7.0 – 8.0 points	9.4%

Note. N = 889.

Sub-question B. The second of the three sub-questions in this study sought to identify the level of concern that each respondent had to the fact there is no state or federal legislation that exists to monitor and control DROs participating in the collection and commercialization of PII or to protect individual privacy within the industry. Possible scores for respondents had a range between zero and seven. Just as with the awareness and knowledge measures, although there is no standard scale for what is considered low to high scores, for the purposes of this research, I have assigned the scale in Table 5 for Concern construct scores. Table 5 also shows the percentage of respondents who achieved each of the possible score groups.

A total of 6.6% of all respondents scored below 4.0 points, corresponding to Little/No Concern. An additional 7.1% of respondents scored between 4.0 and 4.75 points, corresponding to some concern about the lack of legislation. The third level of concern about the lack of legislation is considered Intermediate, representing 19.2% of all respondents. As the final score on the Concern Scale, 66.7% of

all respondents expressed a level of High Concern. In total, 85.9% of all respondents had either an intermediate or a high level of concern about the lack of legislation to protect individual data privacy. The remaining 14.1% of the sample demonstrated little and some levels of concern.

Table 5

Concern Scale

Rating	Range	Respondent %
Little/No Concern	0.0 – 3.75 points	6.6%
Some Concern	4.0 – 4.75 points	7.1%
Intermediate Concern	5.0 – 5.75 points	19.2%
High Concern	6.0 – 7.0 points	66.7%

Note. N = 889.

Sub-question C. The third and final of the three sub-questions in this study sought to identify the level of desire that each respondent had to see legislation enacted that will provide oversight and control of companies participating in the collection and commercialization of PII obtained from online activities. Possible scores for respondents had a range between zero and seven. Just as with the awareness, knowledge, and concern measures, although there is no standard scale for what is considered low to high scores, for the purposes of this research, I have assigned the scale in Table 6 for Desire construct scores. Table 6 also shows the percentage of respondents who achieved each of the possible score groups.

A total of 0.1% of all respondents scored below 4.0 points, corresponding to Little/No Desire. An additional 1.2% of respondents scored between 4.0 and 4.75 points, corresponding to some desire to see legislation enacted. The third level of desire to see legislation enacted is considered Intermediate, representing 9.3% of all respondents. As the final score on the Desire Scale, 89.4% of all respondents

expressed a level of High Desire. In total, 98.7% of all respondents had either an intermediate or a high level of desire to see legislation enacted to protect individual data privacy. The remaining 1.3% of the sample demonstrated little and some levels of desire.

Table 6

Desire Scale

Rating	Range	Respondent %
Little/No Desire	0.0 – 3.75 points	0.1%
Some Desire	4.0 – 4.75 points	1.2%
Intermediate Desire	5.0 – 5.75 points	9.3%
High Desire	6.0 – 7.0 points	89.4%

Note. N = 889.

Answering Research Question 3

Regression Analysis. One of the objectives of this study, as represented by the third of the three identified research questions, was to generate data that can be used to understand which demographic factors most significantly influenced the results of the score for each construct. To achieve this objective, the decision was made to leverage stepwise analysis as the approach that would effectively identify which factors most significantly affects overall awareness, knowledge, concern, and desire. This approach, chosen because of its ability to measure iterate each independent variable in a model and remove those that are not significant, helped explain constituent variation in each of the four individual constructs using the identified demographic measures of party affiliation, state of residence, sex, age, education, race/ethnicity, and community type. Each of the constructs served as the dependent variable in a series of four multiple regression models, with the independent variables being a mix of continuous (e.g., age) and discreet variables (e.g., party affiliation and sex). Taken together, these

models allowed for the identification of variables most significantly correlated (at the $p \leq .05$ level) with the individual constructs. Through the review of the results from each construct, the third and final research question has been answered: Of the seven demographic factors identified in this survey; party affiliation, state of residence, sex, age, education, race/ethnicity, and community type; which have a significant impact on respondents' level of awareness, knowledge, concern, and desire?

Awareness Stepwise Regression. In explaining variation in the Awareness construct, there were a total of nine factors that contributed significantly to an individual's awareness of who was collecting data and from what sources. As illustrated in Table 7, some factors were positively associated with awareness while others were negatively associated.

Table 7

Stepwise Regression Analysis for the Awareness Construct

	Unstandardized Coefficients			
Variables	B	Std. Error	t	Sig.
(Constant)	.78	.01	71.83	.00
EDUC_BACH	.03	.01	2.67	.00
EDUC_MAST	.04	.01	2.54	.01
EDUC_DOC	.05	.03	1.87	.06
SEX	.03	.01	2.40	.02
OVER65	-.04	.02	2.86	.00
RACE_WHITE	.03	.01	2.99	.00
AGE55_65	-.03	.01	-2.11	.04
OH_RES	-.04	.02	-2.46	.01
TX_RES	-.03	.01	-2.13	.03

Education correlated strongly with awareness, with greater education correlating positively with greater awareness. Those respondents who have a bachelor's degree were 3% more aware than

respondents with less than a bachelor's degree. Respondents with a master's degree were 1% more aware than respondents with a bachelor's degree, or 4% more aware than anyone with less than a bachelor's degree. Additionally, respondents with a doctorate were 1% more aware than those with a master's degree, or 5% more aware than respondents with less than a bachelor's degree. Of the nine variables that were significantly correlated with respondent awareness, one third were related to education.

The other two variables that were positively correlated with awareness were sex and race. According to the results, men were 3% more aware than women about the type and from where personal data is being collected. Race also showed a positive correlation, with whites demonstrating a 3% greater awareness than all other races.

The negatively correlated factors were found in both age and state of residence. Based on the results, respondents who are between 55-64 were 3% less aware than respondents younger than 55 years of age. Similarly, respondents who are over 65 years old were 1% less aware than respondents between 55-64 years old, or 4% less aware than respondents under 55 years old. State of residence was the other factor that demonstrated a negative correlation. From the results, we see that residents of Texas were 3% less aware than residents from California, Florida, New York, or Georgia. Similarly, residents of Ohio were 1% less aware than residents from Texas, or 4% less aware than residents from California, Florida, New York, or Georgia.

Knowledge Stepwise Regression. The Knowledge construct regressions revealed three factors that contributed significantly to an individual's knowledge of what legislation exists to protect individual data privacy rights. As illustrated in Table 8, race and education were the two factor groups contributing significantly to knowledge.

The first factor identified as having a statistically significant impact on knowledge was race. According to the data, white respondents were 8% more knowledgeable than non-white respondents were. Education, however, showed both a positive and negative correlation. Those respondents with a maximum of a high school education were 7% less knowledgeable than respondents with more than a high school education. For respondents with a master's degree, they were 5% more knowledgeable than respondents with more than a high school education but less than a masters. Additionally, respondents with a master's degree were 13% more knowledgeable than respondents with no more than a high school education.

Table 8

Stepwise Regression Analysis for the Knowledge Construct

	Unstandardized Coefficients			
Variables	B	Std. Error	t	Sig.
(Constant)	0..39	.01	28.19	.00
RACE_WHITE	.08	.02	4.76	.00
EDUC_HS	-.07	.03	-2.56	.01
EDUC_MAST	.05	.02	2.14	.03

Concern Stepwise Regression. In explaining variation in the Concern construct, three factors contributed significantly to an individual's concern about the fact that no legislation exists to protect individual data privacy rights. As illustrated in Table 9, race and age were the two factor groups contributing significantly to concern.

The first factor identified as having a statistically significant impact on concern was age. According to the data, respondents between the ages of 25 -38 years old were 3% less concerned about the lack of legislation than respondents who are over 38 years old. Respondents over 65 years old were 5% more concerned than respondents between 39 - 65 years old, and 8% more concerned than respondent

between 25 – 38 years old. Race was the second factor that demonstrated less concern with the lack of legislation. According to the responses from respondents, whites were 3% less concerned than all other races.

Table 9

Stepwise Regression Analysis for the Concern Construct

	Unstandardized Coefficients			
Variables	B	Std. Error	t	Sig.
(Constant)	.89	.01	77.57	.00
AGE25_38	-.03	.01	-2.60	.01
OVER65	.05	.02	2.49	.01
RACE_WHITE	-.03	.01	-2.14	.03

Desire Stepwise Regression. The Desire construct regression revealed a total of four factors that contributed significantly to an individual's desire to see legislation enacted to protect individual data privacy rights. As illustrated in Table 10, age and state of residence were the two factor groups contributing significantly to desire.

The first factor identified as having a statistically significant impact on desire was age. According to the data, respondents between the ages of 18 - 24 years old were 8% less interested in seeing legislation enacted than all other age groups. Respondents who were over 65 years old were 3% more desirous to see legislation enacted than respondents between 25 and 54 years old. This also means that respondents over 65 were 11% more desirous than respondents between 18 – 24 years old. The group most desirous of seeing legislation enacted are those between the ages of 55 – 65 years old. This group was 0.3% more desirous than those over 65 years old.

State of residence was the other factor that demonstrated that it was a statistically significant factor. As shown in Table 10, residents of Georgia were 4% less desirous to see legislation enacted than residents from any other state.

Table 10

Stepwise Regression Analysis for the Desire Construct

	Unstandardized Coefficients			
Variables	B	Std. Error	t	Sig.
(Constant)	.90	.01	145.68	.00
AGE55-65	.04	.01	3.12	.00
OVER65	.03	.01	2.24	.03
AGE18-24	-.08	.04	-2.38	.02
GA_RES	-.04	.02	-2.14	.03

Summary

After careful consideration of the elements that would influence the creation of this study's survey instrument, the resulting data was able to clearly answer each of the three research questions. The first two research questions focused on gaining insight into respondents understanding and interest in each of the four assessed constructs: Awareness, Knowledge, Concern, and Desire, while question three sought to determine which factors most significantly influenced participant's responses.

The resulting data for the Awareness construct demonstrated that although 71% of respondents had at least an adequate level of awareness about the data collection activities of DROs, 29% of the sample population had a less than adequate awareness. Additionally, education, age, sex, race, and state of residency were statistically significant factors when determining respondents' awareness levels.

The results for respondent knowledge revealed that more than half (57.3%) of all respondents had a poor knowledge of existing legislation to protect individual data privacy rights, and only 9.4% of

respondents had a knowledge level that rated superior. Interestingly, the two factor groups that contributed significantly to respondents' knowledge levels were race and education.

Concern was where we began to see more significantly grouping of interest across all respondents. The data demonstrated that 85.9% of all respondents had either an intermediate or a high level of concern about the lack of legislation to protect individual data privacy. The two significant factors contributing to respondent answers were age and race.

Desire to see legislation enacted was the fourth of the constructs measured. The data demonstrated that 98.7% of all respondents had either an intermediate or a high level of desire to see legislation enacted to protect individual data privacy, with only 0.1% of respondents expressing little or no interest in seeing legislation enacted. The influencing factors with the greatest significance were age and state of residence.

CHAPTER FIVE

DISCUSSION

As the final chapter in this research study, the goal was to finalize the details of this study and prepare for future research. To achieve this objective, the chapter will begin with a brief review of the study purpose, ensuring that the initial intention of this research was met by the outcome. This will be followed by a review of the methodology applied to gathering and analyzing the research, inclusive of both a recap of the instrument design and the three purposed research questions. To ensure clarity, I then present a summary of the finding for each of the three research questions, inclusive of how they relate to any of the literature reviewed for this study and what implications the findings might have for policy and practice in the future. In closing, this chapter will identify some known limitations and share recommendations for future research.

Purpose

The idea for this study launched from an awareness of the growing online data collection industry, and the knowledge that there is virtually no legislation in place to protect individual Personally Identifiable Information (PII) collected and commercialized by organizations participating in the data collection industry. In addition, there was a widely held belief that most individuals were unaware of how much data was being collected or what was being done with that data (Federal Trade Commission, 2014; Somerville, 2017). Interestingly, even though there was no research to determine individuals' interest in seeing legislation enacted to protect PII, the data brokerage industry was represented by some of the strongest lobbying entities in Washington (Guynn, 2018), focused on mitigating the enacting of legislation to oversee their industry. It was this lack of clarity or understanding that outlined the details of the purpose of this research: to analyze the attitudes and level of interest that

constituents have in seeing legislation enacted to monitor and control the collection and commercialization of PII and to protect individual privacy rights.

Methodology

This study did groundbreaking research into understanding where individual U.S. constituents stand on the need for federal legislation to monitor and control the collection and commercialization of PII collected from internet connected personal devices. To provide a concise representation for how each of these constituents feels about the topic of federal legislation surrounding PII collection and use, the quantitative research method employed a combination of exploratory and descriptive research (Pratap, 2018) utilizing a cross-sectional approach. By providing an overview in three areas—i.e., (a) an analysis of how personal data is monetized by different types of companies, (b) a complete literature review to learn about existing legislation to protect individuals' privacy and a discovery of how privacy rights have developed in the U.S., and (c) an examination into the history and valuation of the internet—a solid foundation was created for the development of a survey instrument containing critical context and informed questions.

To gather data relevant to the purpose of this study, I developed a survey instrument that was used to gather information from a sample of the U.S. population of registered voters in six of the most populous states: California, Florida, Texas, New York, Ohio, and Georgia. The instrument was administered using the online survey tool/service, Qualtrics, and consisted of only quantitative, closed ended questions. The use of an online method of data collection allowed for efficient data collection and a more rapid data analysis. The list of possible respondents was taken from a market research company's available database. Each respondent was asked to answer a series of qualifying questions to ensure that they met the requirements of living in one of the six selected states, being a registered voter, and being an active online user. In total, there were 892 completed survey responses.

The survey assessed four constructs: Awareness, Knowledge, Concern, and Desire. The Awareness construct sought to understand the level of awareness that respondents had about whether data was being collected and from where that data was collected. The Knowledge construct determined whether respondents know if legislation exists to protect individual PII and to oversee the activities of data reliant organizations (DROs). The Concern construct's purpose was to understand the level of concern that respondents had about the lack of legislation in place to protect their PII. And the Desire construct identified how desirous respondents were to see federal legislation enacted to protect their personal data privacy.

Findings

From this research, there are several, highly insightful pieces of information that can be used by anyone interested in understanding how constituents feel about the current state of the data commercialization industry and the need for legislation to protect PII. However, it is important to note that I will be unable to reference prior research in this section. This is not a result of lack of interest or desire to include these references, but instead is a result of the fact that it has been established that there is little to no valid or reliable research around individuals' level of interest to see legislation enacted to protect PII collected by DROs. Only two studies were discovered that contained any information closely related to this study. The first finding published no data to substantiate the research's validity or reliability, and the researchers refused to provide any additional detail when I contacted them (*About Us | Campaign for Accountability*, n.d.). The second study contained only two questions about respondents' interest in legislation to allow access to personal data and the ability to request that personal data to be deleted (Hoofnagle et al., 2012). However, the purpose of the study was focused on differences among age groups to various types of questions and the two legislation questions were focused only on websites that collect data, not data gathering as an industry. For these

reasons, there will not be an attempt made to align the findings from this study's research with the findings from either of the other two pieces of literature discovered during the review process.

For consistency, I will attempt to address the major findings in the same order as the research questions have been presented. However, before assessing the findings that were unique to each question, it seems appropriate to first address the findings that were ubiquitous throughout the research findings.

Factors Not Contributing To Explained Variation

Depending on certain perceptions, the factors that demonstrated no statistical significance in explaining variation in the four constructs may be the most surprising. According to the research, political affiliation did not significantly contribute to any of the four constructs or respondents' scores. This lack of variation between parties may not be as incredibly insightful when assessing the awareness of individuals across party lines. However, the lack of any significant difference in party affiliation when assessing knowledge of legislation, concern about the lack of legislation, and desire to see legislation enacted may come as a surprise to people on both sides of the aisle. Also of interest is the fact that community type plays no significant role in people's opinions on any of the four constructs. It would not be unusual to expect to see strong differences within any of the four constructs when comparing across different community types. However, according to the results, this factor had no significant impact on respondents' results.

Question Summary

There were three research questions proposed for this study. Below are the findings from the research for each of the three questions.

Research Question 1: To what extent are constituents aware that personal data is being collected about them when their devices are connected to the internet?

The first question sought to identify how aware respondents are about data being collected about them while they are online. To facilitate the assessment of awareness, a scoring system was assigned to the Awareness construct. Within the Awareness construct there were a total of ten possible questions for respondents to answer. Each question has an assigned value from zero to one point. This meant that respondents could generate as total possible score of between zero and ten for the entire Awareness construct.

Respondent scores determined which of four awareness categories respondents would be included in: Poor/Low, Basic, Adequate, or Superior. In total, 71% of all respondents had either an adequate or superior level of awareness about from where and the type of data being collected about them while they are using an online connected personal device. The remaining 29% of the sample demonstrated a less than adequate level of awareness.

Research Question 2: For those respondents that are aware that such data is being collected, or believe data might be collected, are constituents knowledgeable about what state or federal legislation, if any, exists to monitor and control the collection and commercialization of individuals' Personally Identifiable Information (PII); in the absence of state or federal legislation, to what extent do respondents feel concern for the lack of legislation; and, do respondents feel that there should be federal legislation in place to monitor and control what and how DROs are collecting and using their personal data?

Research question two has three sub-questions within it that require answering separately. Each of these three sub-questions relates to each of the remaining three constructs.

Sub-question A. This question sought to identify how much knowledge each respondent had about what legislation already exists to monitor and control the activities of DROs participating in the collection and commercialization of PII obtained from individual online activity. Within the Knowledge construct, there were eight questions for respondents to answer. Each question has an assigned value from zero to one point. Possible scores for respondents had a range between zero and eight.

Respondent scores determined which of four knowledge categories respondents would be included in: Poor/Low, Basic, Adequate, or Superior. In total, 22.6% of all respondents had either an adequate or a superior level of knowledge about what legislation does or does not exist to protect individual data privacy. The remaining 77.4% of the sample demonstrated a less than adequate level of knowledge.

Sub-question B. The focus of this question was to determine what level of concern each respondent had to the fact there is no state or federal legislation exists to monitor and control DROs participating in the collection and commercialization of PII or to protect individual privacy within the industry. Within the Concern construct, there were seven possible questions for respondents to answer. Each question has an assigned value from zero to one point. Possible scores for respondents had a range between zero and seven.

Respondent scores determined which of four concern categories respondents would be included in: Little/No, Some, Intermediate, or High. In total, 85% of all respondents had either an intermediate or a high level of concern about the lack of legislation to protect individual data privacy. The remaining 15% of the sample demonstrated little and some levels of concern.

Sub-question C. This question intended to identify what level of desire each respondent had to see legislation enacted that would provide oversight and control of companies participating in the collection and commercialization of PII obtained from online activities. Within the Desire construct, there were

seven possible questions for respondents to answer. Each question has an assigned value from zero to one point. Possible scores for respondents had a range between zero and seven.

Respondent scores determined which of four concern categories respondents would be included in: Little/No, Some, Intermediate, or High. In total, 98.7% of all respondents had either an intermediate or a high level of desire to see legislation enacted to protect individual data privacy. The remaining 1.21% of the sample demonstrated little and some levels of desire.

Research Question 3: Of the seven demographic factors identified in this survey; party affiliation, state of residence, sex, age, education, race/ethnicity, and community type; which have a significant impact on respondents' level of awareness, knowledge, concern, and desire?

The final research question used stepwise regression analyses to understand which demographic factors most significantly influenced the results of the score for each construct. In estimating these regressions, the $p \leq .05$ threshold was used for variable inclusion.

Awareness Stepwise Regression. It is interesting to now know that a majority of the population (71%) have an adequate or higher level of awareness of the activities around personal data collection while online. This awareness is in contrast to the beliefs of some (Federal Trade Commission, 2014; Somerville, 2017), and likely something that would be of interest to legislators. Another fact resulting from the data is that almost one third of all respondents (32.2%) have a superior level of awareness. As mentioned above, political affiliation and community type played no significant role in the level of awareness of respondents.

When considering the regression analysis to better understand those factors that are significantly correlated with awareness, a couple of interesting factors presented themselves, which may be of value to those interested in leveraging the results of this study. The first is that beginning with a bachelor's degree, the more educated an individual is, the more aware they are about the activities of online data

collection. Specifically, respondents who have a bachelor's degree were 2.9% more aware than respondents with less than a bachelor's degree, while those with a master's degree were 0.7% more aware than respondents with a bachelor's degree, and respondents with a doctorate were 1.3% more aware than those with a master's degree. This information could be valuable to both future researchers as well as legislators considering a position to take on proposed legislation.

Other factors that could provide value to both future researchers and legislators are the fact that white people were 3.2% more aware than non-whites and that men were 2.8% more aware than women. It is also of potential value to know that people 55 and over were 4.3% less aware, and residents in Texas and Ohio were less aware than those in California, Florida, New York, or Georgia.

Knowledge Stepwise Regression. In contrast to the Awareness construct scoring results, the majority of respondents scored below adequate when questioned about knowledge of existing legislation to protect PII. There is likely value in knowing that only 9.4% of respondents had a superior level of knowledge about existing legislation and more than 77% of respondents had a less than adequate level of knowledge.

Demonstrating their significance again, race and education were shown to contribute to knowledge of existing legislation. White respondents demonstrated legislative knowledge 7.7% greater than other races. In addition, people with a high school education or less were 7.3% less knowledgeable than all others while those with a master's degree or higher were 4.5% more knowledgeable than respondents with more than a high school education. Once again, this information is potentially valuable to both future researchers and to legislators.

Concern Stepwise Regression. It is beginning with the Concern construct that we see a large majority of respondents aligning on their positions around a topic. It is clear, with 85.9% of respondents sharing an intermediate or high level of concern, that the lack of legislation in place to protect individual data

privacy is worrisome for a significant portion of the population. It is important to note that of the remaining 14.1% of respondents, 7.1% expressed some level of concern, meaning that only 6.6% of the population had little to no concern about the lack of legislation.

Race and age were the two factors that had the most significant impact on the level of concern of respondents about the lack of legislation to protect data privacy. Interestingly, whites were 2.7% less concerned that all other ethnic groups. Also of interest is the fact that respondents over 65 were more concerned than any other age group, while respondents who were between 25 and 38 years old were 3.4% less concerned about the lack of protective legislation.

Desire Stepwise Regression. The Desire construct had the greatest respondent alignment of sentiment among the constructs. With an almost unanimous result, 98.7% of respondents had either an intermediate or a high level of desire to see legislation enacted to protect individual data privacy. It is also important to note that another 1.2% demonstrated some level of interest in seeing legislation enacted. This means that only 0.1% of respondents expressed little or no interest in seeing legislation enacted.

The influencing factors with the greatest significance on sentiment about desire to see legislation enacted were age and state of residence. Not surprisingly, respondents at each end of the age group spectrum had different perspectives, with respondents between 18 and 24 years old being 8.2% less interested in seeing legislation enacted than all other age groups, and respondents over 65 years old being 3.2% more desirous than those over 24 years of age. State of residence was the other factor that demonstrated that it was a statistically significant factor, with residents of Georgia being 3.5% less desirous to see legislation enacted than residents from any other state.

Implications

Overall, the findings should be incredibly valuable to legislators and DROs. It is clear from the results of this study that the majority of respondents were not aware that legislation to protect PII gathered by DROs does not exist at either the state or national level. However, when respondents were informed that legislation does not exist to control the activities of DROs, and that they have little to no rights to know what data is being collected or stored about them, the levels of concern and desire were quite high. It is worth noting, again, that 98.7% of respondents had intermediate or high levels of desire to see legislation enacted, and 99.9% of respondents expressed at least some desire.

It is likely fair to state that there are only a small number of things that people across the aisle agree upon at a level of almost 100%. Based on the results of this study, it would be surprising that legislators at all levels did not begin to look to make significant changes in the areas of monitoring and controlling the activities of DROs dealing in the collection and commercialization of PII. However, even if the result is not an immediate focus on the proposal of legislation, it is reasonable to expect that legislators will begin to do additional research to identify sentiments from their own constituents and to gain greater insight into understanding specifically what aspects of data privacy protection are of the greatest and most immediate concern.

Limitations

As the first known attempt to understand constituent sentiments around the topic of legislation to protect PII, it should be no surprise that limitations exist. Moreover, although there may be many limitations that could be identified, for the purpose of this study, I focused on only those four that presented the greatest level of concern during the execution and analysis of this study. The first known limitation surfaced during the literature review. As discussed, there has been little to no research done around the topic of this study, which limits learning from other researchers. The second limitation

presented itself while considering various data sources for the online survey. As discussed, the database used for gathering respondent insights came from a mystery shopping company's database of mystery shoppers. The third limitation presented itself when deciding on how to ensure that a large enough sample of party affiliated respondents was obtained. To achieve this objective, the decision was made to only consider respondents from the Democratic and Republican political parties. The final limitation presented itself during the reliability testing of each of the constructs. The seven questions in the Desire construct only produced a Cronbach's alpha reliability score of 0.61. Each of these limitations is discussed in more detail in the discussion that follows.

Although an exhaustive attempt was made to find any reliable research on the topic of constituent sentiment around interest to see legislation enacted to monitor the activities of DROs and to protect PII, the efforts turned up virtually nothing. This is not to say that such a limitation would suggest a reason not to pursue the topic, but it certainly is more challenging to address a truly nascent subject in an area that has rapidly growing attention from many different interested parties.

Finding a data source for surveying a sample of the population presented quite a challenge. For the purposes of expediency and efficiency, as well as the fact that the literature review presented no existing research to leverage as part of this study, the decision was made to use an online survey instrument as the first attempt to gather data on this topic. The next challenge was to find a database of possible respondents who would be willing to share, honestly, the level of personal information necessary to make the study valuable. And to be fair, the irony of needing to acquire PII from respondents while researching the topic of protecting PII was not lost on me. That said, the database of possible respondents needed to be one that would produce a sufficient number of respondents to generate a representative sample of the population in reasonable quantities. In addition, the survey was going to be quite long, so respondents needed to be willing to invest about 25-30 minutes of their time responding to these highly personal questions. When considering other databases, the constant

concern was whether people would not be willing to share highly personal information with an unknown source. It was for that reason that I decided to use a group of possible respondents who are part of an existing database that asks for their opinion and input on many topics. Certainly, there are opportunities to discuss the diversity of the demographics of the database or the similarities among a group of people who choose to do the same type of work, but similar arguments could be made for almost any database. It is possible that other databases could have produced similar numbers of responses in a similar timeframe. However, with the known limitations in place before launching the survey, I am confident that the results are sufficient to justify the database decision.

Deciding to include only Democrat and Republican respondents was a difficult choice and a known limitation that would need to be addressed. There were several reasons for this decision, which include ensuring that the database contained a sufficient number of each group to gain a representative sample and the fact that this was the first study in this area. The respondent selection criteria leveraged published party affiliation for both federal representatives and voter results in prior elections. The number of representatives from other parties did not align itself well with the chosen method for sampling. In addition, the data available around voter results in prior elections from outside of either the Democratic or the Republican parties was not as deep or rich as it was for these two parties. Therefore, the decision was made that for this first study only the two parties would be included. However, future research will likely include respondents from other groups.

The final limitation addressed in this section is the relatively low reliability score of the Desire construct questions. A score of 0.61 is not an ideal when trying to establish reliability for an instrument. In addition, the fact the previous construct produced a reliability score of 0.9, only serves to highlight this limitation even further. However, as mentioned earlier, this is the first research being done in this area. There is little doubt that future research will continue to improve upon the work done here and the hope is that a more reliable construct will be found.

Recommendations

As of the writing of this final chapter, major events are occurring in the area of legislative action to protect PII. California has officially launched the first widespread state legislation to enforce some level of oversight over DROs. Virginia has become the first state to proactively take action to pass legislation that will provide similar levels of protection for individuals' data privacy. In addition, the current federal presidential and congressional administrations are known to endorse considering greater oversight over DROs. Add to this the incredible growth in data collecting devices/processes that are part of our everyday lives (e.g., smart home devices, on-board automobile computers, biometric scanning, smart clothing, etc.), and personal data collection is an inescapable part of every moment of our lives. In light of these factors, as well as growing mainstream media chatter around the importance of data privacy, now is the time to continue to pursue additional research in this area.

As an immediate follow up to this research, I have identified three areas of focus for additional research. The first will require no additional data gathering and will be able to leverage the data that has already been collected for this study. In addition to the seven demographic factors collected during this study, the data gathered included the zip codes for all 892 respondents. This information will allow future researchers to overlay known data about populations within zip codes to provide further insight and comparisons by geographic location.

The second opportunity, and a logical next step would be to speak directly with state and federal legislators to understand their positions on protective legislation for individual PII. Much like visibility into constituent sentiments about the importance of protective legislation, there is no single resource for constituents to know how representatives feel about this topic or what position they are taking.

The final recommendation for additional research would be to expand on the work already done in this study. This could include querying respondents who align with other political parties. Deeper

research could also investigate further individuals' knowledge of other data sources used to collect personal information. Alternatively, researchers could choose a qualitative approach to gain richer and more contextualized understandings of participants responses.

This topic is poised to become much more central to political conversations in the near future and I am confident that this research, as well as the research that follows, will contribute greatly to providing for what is in the best interest of all constituents.

REFERENCES

18 USC 2710: Wrongful disclosure of video tape rental or sale records, Pub. L. No. 18 U.S. Code § 2710 (1988). http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2710&num=0&edition=prelim

A Summary of Your Rights Under the Fair Credit Reporting Act. (2003). https://www.ssa.gov/seattle/neg/HRC79.pdf

About IAB. (n.d.). Retrieved January 4, 2019, from https://www.iab.com/news/interactive-shoppable-ads-drive-relationships/

About Us | Campaign for Accountability. (n.d.). Retrieved January 17, 2019, from https://campaignforaccountability.org/about/

Anti-Phishing Act of 2005, (2005). http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=33.&article=

Bertot, John; Palmer, K. (n.d.). *U.S. Public Libraries Provide Access to Computers, the Internet, and Technology Training - Bill & Melinda Gates Foundation*. Bill & Melinda Gates Foundation. Retrieved October 4, 2018, from https://www.gatesfoundation.org/Media-Center/Press-Releases/2005/06/Support-Needed-for-Library-Technology

Congressional Review Act, Pub. L. No. 5 U.S. Code § 801, Congressional Research Service 21 (2001). https://www.senate.gov/CRSpubs/316e2dc1-fc69-43cc-979a-dfc24d784c08.pdf

Betz, C. (2011). *Personal Data: A New Asset Class? | Wolters Kluwer – The Intelligent Solutions Blog*. Wolters Kluwer. http://solutions.wolterskluwer.com/blog/2011/04/personal-data-a-new-asset-class/

Bischoff, P. (2018). *Which US states best protect privacy online? - Comparitech*. Comparitech.Com. https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/#gref

Blum, D. (2018). *The Poison Squad: One Chemist's Single-Minded Crusade for Food Safety at the Turn of the Twentieth Century* (1st ed.). Penguin Press.

Boutin, P. (2016, May). Sexual Orientation - The Secretive World of Selling Data About You. *Newsweek*. https://www.newsweek.com/secretive-world-selling-data-about-you-464789

Bureau of Labor Statistics, U. S. D. of L. (2016a). *Employment by major industry sector*. https://www.bls.gov/emp/tables/employment-by-major-industry-sector.htm

Bureau of Labor Statistics, U. S. D. of L. (2016b). *The Economics Daily*. https://www.bls.gov/opub/ted/2016/employment-population-ratio-59-point-7-percent-unemployment-rate-4-point-7-percent-in-may.htm

CA Civil Code for Data Breaches, Pub. L. No. 1798.82, California Legislative Information Page (2016). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

CA Health and Safety Code for Data Breaches, Pub. L. No. HSC 1280.15, California Legislative Information Page (2014). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=1280.15

Caldano, J. (2018). *What's the value of the Internet of Things? – Frontier presents evidence at Big Data conference in Valencia | Frontier Economics*. http://www.frontier-economics.com/uk/en/news-and-articles/news/news-article-i2134-what-s-the-value-of-the-internet-of-things-frontier-presents-

evidence-at-big-data-conference-in-valencia/

California Consumer Privacy Act of 2018, (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

California Data Security, Pub. L. No. Cal. Civ. Code § 1798.81.5 (2015). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5

California Shine the Light Law. (2003). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV

CES 2017: What to expect at the Consumer Electronics Show, the year's biggest tech showcase in Las Vegas - CBS News. (n.d.). Retrieved January 8, 2019, from https://www.cbsnews.com/news/ces-2017-consumer-electronics-show-las-vegas/

CES 2018: everything you need to know about the world's biggest tech show | TechRadar. (n.d.). Retrieved January 8, 2019, from https://www.techradar.com/news/ces-2018

CES Consumer Electronics Show Las Vegas 2019. (n.d.). Retrieved January 9, 2019, from https://www.tradefairdates.com/CES-Consumer-Electronics-Show-M11423/Las-Vegas.html

Children's Online Privacy Protection Rule (COPPA) | Federal Trade Commission. (1998). FTC.Gov. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Commissioner, O. of the. (2018). *FDA Basics - When and why was FDA formed?* Office of the Commissioner. https://www.fda.gov/aboutfda/transparency/basics/ucm214403.htm

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Consumer Financial Protection Bureau. (n.d.). *The Bureau*. https://www.consumerfinance.gov/about-us/the-bureau/

Cornish, A. (2009). *NHTSA Outcry - Congress' Safety Agenda Faces Obstacles : NPR*. Npr.Org. https://www.npr.org/templates/story/story.php?storyId=120688230

CPSC Outcry. (2007). CQ Almanac. https://library.cqpress.com/cqalmanac/document.php?id=cqal07-1006-44908-2047770

Deighton, John; Kornfeld, Leora; Gerra, M. (2017). *Economic Value of the Advertising-Supported Internet Ecosystem*. https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-20180614-SD005.pdf

Deighton, J. (2012). *Economic Value of the Advertising-Supported Internet Ecosystem*. https://www.hbs.edu/faculty/Publication Files/EVASIE_2012_September_9d78c1c2-51be-4431-9a11-e19e26f71b80.pdf

Deutsch, A. L. (2018). *The 5 Industries Driving the U.S Economy*. Investopedia. https://www.investopedia.com/articles/investing/042915/5-industries-driving-us-economy.asp

Directory of Representatives | House.gov. (2019). U.S. House of Representatives. https://www.house.gov/representatives

Driver's Privacy Protection Act | ASPE. (2014). U.S. Department of Health & Human Services. https://aspe.hhs.gov/report/minimizing-disclosure-risk-hhs-open-data-initiatives/4-driver's-privacy-protection-act

Early Postal Legislation. (n.d.). Retrieved November 2, 2018, from https://about.usps.com/publications/pub100/pub100_004.htm

Eby, M. (1993). Validation: choosing a test to fit the design. *Nurse Researcher*, *1*(2), 27–33. https://doi.org/10.7748/nr.1.2.26.s4

eCFR — Code of Federal Regulations. (n.d.). Retrieved November 20, 2018, from https://www.ecfr.gov/cgi-bin/text-idx?SID=50aa19d46a91816536da1cd3c6ba5c6c&mc=true&node=pt16.1.312&rgn=div5#se16.1.312_110

Electronic Communications Privacy Act of 1986. (n.d.). U.S. Department of Justice. Retrieved January 24, 2019, from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Ex parte Jackson :: 96 U.S. 727 (1878) :: Justia US Supreme Court Center, Pub. L. No. 96 U.S. 727 (1878). https://supreme.justia.com/cases/federal/us/96/727/

FACTA Disposal Rule Goes into Effect June 1 | Federal Trade Commission. (2005). https://www.ftc.gov/news-events/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1

Fair and Accurate Credit Transactions Act of 2003 | Federal Trade Commission, Pub. L. No. 15 USC CHAPTER 41, SUBCHAPTER III (2003). https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003

Fair Debt Collection Practices Act | Federal Trade Commission. (n.d.). Retrieved January 24, 2019, from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-debt-collection-practices-act-text

Family Educational Rights and Privacy Act (FERPA). (2018, March 1). U.S. Department of Education; US Department of Education (ED). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FDA Outcry - The Pure Food and Drug Act | US House of Representatives: History, Art & Archives. (1906). History.House.Gov. https://history.house.gov/Historical-Highlights/1901-1950/Pure-Food-and-Drug-Act/

Federal Trade Commission. (1970). *Fair Credit Reporting Act | Federal Trade Commission*. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act

Federal Trade Commission. (2014). *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission*. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

Financial Institutions and Customer Information: Complying with the Safeguards Rule | Federal Trade Commission. (2006). Ftc.Gov. https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Finn, J. E. (2006). *Civil Liberties and the Bill of Rights, "Part I: Lecture 4: The Court and Constitutional Interpretation"* (pp. 52, 53, 54). The Great Courses.

S.J.Res.34 - 115th Congress (2017-2018): A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"., (2017). https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34

H.R.4173 - Dodd-Frank Wall Street Reform and Consumer Protection Act, (2010) (testimony of Barney Frank). https://www.congress.gov/bill/111th-congress/house-bill/4173/text

FTC Outcry - Federal Trade Commission (FTC) - Encyclopedia - Business Terms | Inc.com. (n.d.). Inc.Com.

Retrieved October 17, 2018, from https://www.inc.com/encyclopedia/federal-trade-commission-ftc.html

FTC Seeks Comment on Disposal Rule | Federal Trade Commission. (2016). Ftc.Gov. https://www.ftc.gov/news-events/press-releases/2016/09/ftc-seeks-comment-disposal-rule

FTC What We Do | Federal Trade Commission. (n.d.). Ftc.Gov. Retrieved October 17, 2018, from https://www.ftc.gov/about-ftc/what-we-do

Gellman, R., & Dixon, P. (2013). *Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens*. http://www.worldprivacyforum.org/wp-content/uploads/2013/10/WPF_DataBrokersPart3_fs.pdf

General Law - Part I, Title XV, Chapter 93H, Section 2, Pub. L. No. Part I, Title XV, Chapter 93H, Section 2, malegislature.gov. Retrieved November 21, 2018, from https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section2

Glancy, D. J. (1979). THE INVENTION OF THE RIGHT TO PRIVACY. *ARIZONA LAW REVIEW* , *21*(1). http://law.scu.edu/wp-content/uploads/Privacy.pdf

Gramm-Leach-Bliley Act | Federal Trade Commission, Pub. L. No. 15 U.S.C. § 6801 (2010), ftc.gov (2010). https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Green, K. (2017). *Projected new jobs by major industry sector, 2016–26 : Career Outlook: U.S. Bureau of Labor Statistics*. Bureau of Labor Statistics, U.S. Department of Labor. https://www.bls.gov/careeroutlook/2017/data-on-display/projections-industry-sectors.htm?view_full

Greenberg Quinlan Rosner. (2018). *Campaign for Accountability Polling Memo*. https://campaignforaccountability.org/wp-content/uploads/2018/06/CfA-GQR-Polling-Memo-6-

26-18.pdf

Greenberg Qunilan Rosner Research. (2018). *Campaign for Accountability Results from a National Poll*. https://campaignforaccountability.org/wp-content/uploads/2018/06/CfA-National-Poll-Results-PowerPoint-6-26-18.pdf

Guynn, J. (2018, September 26). Lobbying for Limitations - Amazon, AT&T, Google want online privacy bill to preempt stronger Calif. law. *USA Today*. https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/

Hamilton Consultants; Deighton, John; Quelch, J. (2009). *Economic Value of the Advertising-Supported Internet Ecosystem*. https://archive.iab.com/www.iab.net/media/file/Economic-Value-Report.pdf

Head, T. (2018). *The Origins and History of the Right to Privacy*. https://www.thoughtco.com/right-to-privacy-history-721174

Health Breach Notification Rule 16 CFR Part 318 | Federal Trade Commission. (2010). https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule

HIPAA History. (n.d.). Hipaajournal.Com. Retrieved October 29, 2018, from https://www.hipaajournal.com/hipaa-history/

Historical Presidential Election Information by State. (2019). https://www.270towin.com/states/

History.com Editors. (2009). *Facts about Thomas Jefferson - HISTORY*. History.Com. https://www.history.com/topics/us-presidents/thomas-jefferson

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2012). How Different are Young Adults from Older Adults

When it Comes to Information Privacy Attitudes and Policies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1589864

Internet Privacy Requirements, Pub. L. No. Cal. Civ. Code § 22575 (2002). http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

Jefferson Memorial Features - Thomas Jefferson Memorial (U.S. National Park Service). (2017). Nps.Gov. https://www.nps.gov/thje/learn/historyculture/memorialfeatures.htm

Joseph Yates (judge) - Wikiquote. (2016). Wikiquote.Com. https://en.wikiquote.org/wiki/Joseph_Yates_(judge)

Kotler, P., & Armstrong, G. (Gary M. . (2006). *Principles of marketing* (11th ed.). Pearson Prentice Hall. https://books.google.com/books/about/Principles_of_Marketing.html?id=B1DDQgAACAAJ

Kroft, S. (2014). Shocked to learn how data brokers are watching you? - CBS News. *CBSNews, CBS Interactive*. http://www.cbsnews.com/news/shocked-to-learn-how-data-brokers-are-watching-you/

Legislation Survey; What Americans Think About Tech Companies | Campaign for Accountability. (2018). https://campaignforaccountability.org/work/what-americans-think-about-tech-companies/

Letter from Thomas Jefferson to Samuel Kercheval | Teaching American History. (n.d.). Retrieved October 10, 2018, from http://teachingamericanhistory.org/library/document/letter-to-samuel-kercheval/

Lohrmann, D. (2018). *New Guide on State Data Breach Laws*. Govtech.Com. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-guide-on-state-data-breach-laws.html

Luetkemeyer, B. (2018). *H.R.6743 - 115th Congress (2017-2018): Consumer Information Notification Requirement Act*. https://www.congress.gov/bill/115th-congress/house-bill/6743/text

Manyika, J., & Roxburgh, C. (2011). *The great transformer: The impact of the Internet on economic growth and prosperity*. https://www.mckinsey.com/~/media/McKinsey/Industries/High Tech/Our Insights/The great transformer/MGI_Impact_of_Internet_on_economic_growth.ashx

Mass Law 201 CMR 17. (n.d.). Retrieved November 7, 2018, from https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf

Massachusetts Data Security Law Signals New Challenges in Personal Information Protection. (2010). http://www.oracle.com/us/products/database/data-security-ma-201-wp-168633.pdf

Massachusetts Law Raises the Bar for Data Security | Jones Day. (2010). Jones Day. https://www.jonesday.com/Massachusetts_Law_Raises/#

McFarland, M. H. (2004). *SEC Outcry*. https://www.sec.gov/rules/sro/cboe/34-49916.pdf

McLeod, B. (2018). *60+ Small Business Digital Marketing Statistics 2018 | Blue Corona*. https://www.bluecorona.com/blog/29-small-business-digital-marketing-statistics

Mnuchin, S. T., & Phillips, C. S. (2018). *State vs Federal Legislation - A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation Report to President Donald J. Trump Executive Order 13772 on Core Principles for Regulating the United States Financial System Counselor to the Secretary*. https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

National Conference of State Legislatures. (2018a). *2018 Security Breach Legislation*. Ncsl.Org. http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx

National Conference of State Legislatures. (2018b). *50 States Have Security Breach Notification Laws*. Ncsl.Org. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

National Conference of State Legislatures. (2018c). *Data Disposal Laws*. Ncsl.Org. http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

Nevada Expands Personal Data Definition in Breach Notice, Data Encryption Law | Bloomberg Law. (2015). Bloomberg Law: Privacy & Data Security. https://www.bna.com/nevada-expands-personal-n17179927057/

New at CES 2016: eCommerce Marketplace. (n.d.). Retrieved January 8, 2019, from https://ces.tech/News/Press-Releases/CES-Press-Release.aspx?NodeID=528f1716-a9e2-4e1b-9855-193dcb0ccee0

NHTSA History - Understanding the National Highway Traffic Safety Administration (NHTSA) | US Department of Transportation. (2017). Transportation.Gov. https://www.transportation.gov/transition/understanding-national-highway-traffic-safety-administration-nhtsa

O'Brien, S. A. (2017). *Equifax data breach: 143 million people could be affected*. Money.Cnn.Com. https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

H.R.1 - 111th Congress (2009-2010): American Recovery and Reinvestment Act of 2009, Pub. L. No. 123 Stat. 115 (2009). https://www.congress.gov/bill/111th-congress/house-bill/1/text

Office for Civil Rights. (2002a). *What does the HIPAA Privacy Rule do?* https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html

Office for Civil Rights. (2002b). *Who must comply with HIPAA privacy standards | HHS.gov*. https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html

Office for Civil Rights. (2009a). *What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?* Hhs.Gov. https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

Office for Civil Rights. (2009b). *What does HIPAA require of covered entities when they dispose of PHI | HHS.gov*. https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

Office for Civil Rights. (2017). *HIPAA Compliance and Enforcement | HHS.gov*. Hhs.Gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

Our Documents - Bill of Rights (1791). (n.d.). Ourdocuments.Gov. Retrieved November 2, 2018, from https://www.ourdocuments.gov/doc.php?flash=false&doc=13

Peterson, C. L. (2016). *New report evaluates Consumer Financial Protection Bureau track record | UNews*. University of Utah UNEWS. https://unews.utah.edu/new-report-evaluates-consumer-financial-protection-bureau-track-record/?doing_wp_cron=1545415302.1578550338745117187500

Phelan, Colin; Wren, J. (2006). *Exploring Reliability in Academic Assessments*. University of Northern Iowa. https://chfasoa.uni.edu/reliabilityandvalidity.htm

Popken, B. (2018). *Google sells the future, powered by your personal data*. Nbcnews.Com. https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-

n870501

Pratap, A. (2018). *Research design and its types: Exploratory, descriptive and causal - cheshnotes*. Chestnotes. https://www.cheshnotes.com/2018/07/research-design-and-its-types-exploratory-descriptive-and-causal/

Privacy | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute. (n.d.). Retrieved November 1, 2018, from https://www.law.cornell.edu/wex/privacy

Privacy Laws | State of California - Department of Justice - Office of the Attorney General. (n.d.). Retrieved November 26, 2018, from https://oag.ca.gov/privacy/privacy-laws

Puente Cackley, Alicia; Bromberg, Jason; Bowsky, Michelle; Chatlos, William R.; DeMarcus, Rachel; Siegel, Beth; Sinkfield, J. (2013). *INFORMATION RESELLERS Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace United States Government Accountability Office*. https://www.gao.gov/assets/660/658151.pdf

Punch, K. (1998). *Introduction to social research : quantitative and qualitative approaches*. https://us.sagepub.com/en-us/nam/introduction-to-social-research/book237782

Ramirez, E., & Brill, J. (2014). *Data Brokers A Call for Transparency and Accountability Federal Trade Commission*. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Rao, G. A. (2017, August 24). Analysing the Birth of “The Right to Privacy” and the Process Behind its Legal Justification. *Huffington Post*. https://www.huffingtonpost.com/entry/analysing-the-birth-of-the-right-to-privacy-and-the_us_599e8197e4b0a62d0987ace4

Registered Voters by State. (2018). http://www.centerforpolitics.org/crystalball/articles/registering-by-

party-where-the-democrats-and-republicans-are-ahead/

Roberts, Paula; Priest, Helena; Traynor, M. (2006). Reliability and validity in research. *Nursing Standard*, *20*(44), 4. file:///C:/Users/gdeme_000/Downloads/RobertsandPriestReliabilityandValidity.pdf

Ross, K. N. (1978). Sample design for educational survey research. *Oxford: Pergamon Press*. file:///C:/Users/gdeme_000/Downloads/Sampledesignforeducationalsurveyresearch (1).pdf

Ryan, C. (2018). *Computer and Internet Use in the United States: 2016*. https://www.census.gov/library/publications/2018/acs/acs-39.html

SEC.gov | The Laws That Govern the Securities Industry. (2013). Sec.Gov. https://www.sec.gov/answers/about-lawsshtml.html

Shiroff, J. (2015). *The Nevada Data Breach Law | Data Privacy and Protection Blog*. http://www.swlaw.com/blog/data-security/2015/04/30/the-nevada-data-breach-law/

Siwek, S. E. (2015). *Measuring the U.S. Internet Sector*. http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf

Solove, Daniel J.: Schwartz, P. M. (2017). *Information Privacy Law*. Wolters Kluwer Law & Business.

Solove, D. J. (2006). *A Brief History of Information Privacy Law*. https://scholarship.law.gwu.edu/faculty_publications/923/

Somerville, H. (2017). Tech Firms Collecting Data: How Much Do Consumers Know or Care? *Insurance Journal*. https://www.insurancejournal.com/news/national/2017/01/17/438931.htm

Staff of Chairman Rockefeller. (2013). *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-

08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf

State Consumer Protection Offices | USAGov. (n.d.). Retrieved October 17, 2018, from https://www.usa.gov/state-consumer

Steele, B. D. (2015). *The Vague and Ambiguous US Constitution | Marmalade*. https://benjamindavidsteele.wordpress.com/2015/12/01/the-vague-and-ambiguous-us-constitution/

Summary of U.S. State Data Breach Notification Statutes. (n.d.). Retrieved October 24, 2018, from https://www.dwt.com/statedatabreachstatutes/

Summary of U.S. State Data Breach Notification Statutes. (2018). https://www.dwt.com/files/Uploads/Documents/Publications/State Statutes/BreachNoticeSummaries.pdf

The Bill of Rights: How Did it Happen? | National Archives. (n.d.). Retrieved November 2, 2018, from https://www.archives.gov/founding-docs/bill-of-rights/how-did-it-happen

The Cambridge Business English Dictionary. (n.d.). *Definition of Data Breach*. Retrieved October 26, 2018, from https://dictionary.cambridge.org/us/dictionary/english/data-breach

The Constitution: How Was it Made? | National Archives. (n.d.). Retrieved November 2, 2018, from https://www.archives.gov/founding-docs/constitution/how-was-it-made

The Definitive Guide to U.S. State Data Breach Laws. (2018). https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf

The Progressive Era (1890 - 1920). (n.d.). Retrieved October 17, 2018, from

https://www2.gwu.edu/~erpapers/teachinger/glossary/progressive-era.cfm

Fair Credit Reporting Act, Pub. L. No. 15 U.S.C. § 1681 et seq, 108 (2012). https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf

U.S. Consumer Product Safety Commission. (n.d.). *Who We Are - What We Do for You*. Retrieved October 17, 2018, from https://www.cpsc.gov/Safety-Education/Safety-Guides/General-Information/Who-We-Are---What-We-Do-for-You

U.S. Senate: Our States. (2019). https://www.senate.gov/senators/states.htm

Upton Sinclair, Whose Muckraking Changed the Meat Industry - NYTimes.com. (2016, June 30). *The New York Times*. https://www.nytimes.com/interactive/projects/cp/obituaries/archives/upton-sinclair-meat-industry

US States - Ranked by Population 2018. (n.d.). Retrieved November 7, 2018, from http://worldpopulationreview.com/states/

Varian, H. (2013). *The value of the internet now and in the future - Technology*. The Economist. https://www.economist.com/free-exchange/2013/03/10/the-value-of-the-internet-now-and-in-the-future

H.764 Vermont Data Broker Legislation, (2018) (testimony of Vermont House and Senate). https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/06/H-0764.pdf

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Weinburg, A. & L. (1964). *The Muckrackers: The Era in Journalism that Moved America to Reform, the*

Most Significant Magazine Articles of 1902–1912. Capricon Books.

Wikipedia contributors. (2018a). *Boyd v. United States - Wikipedia*. Wikipedia. https://en.wikipedia.org/wiki/Boyd_v._United_States

Wikipedia contributors. (2018b). *Griswold v. Connecticut - Wikipedia*. Wikipedia. https://en.wikipedia.org/wiki/Griswold_v._Connecticut

Wikipedia contributors. (2018c). *Millar v Taylor - Wikipedia*. Wkipedia. https://en.wikipedia.org/wiki/Millar_v_Taylor

Wikipedia contributors. (2018d). *Poe v. Ullman - Wikipedia*. Wikipedia. https://en.wikipedia.org/wiki/Poe_v._Ullman

Wikipedia contributors. (2018e). *Roe v. Wade - Wikipedia*. Wikipedia. https://en.wikipedia.org/wiki/Roe_v._Wade

Wikipedia contributors. (2018f). *Video Privacy Protection Act*. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Video_Privacy_Protection_Act&oldid=863556711

Wikipedia contributors. (2018g, September 19). *American lawyer*. Wikipedia. https://en.wikipedia.org/wiki/Samuel_D._Warren

Wikipedia contributors. (2018h, December 14). *United States Constitution - Wikipedia*. Wikipedia. https://en.wikipedia.org/wiki/United_States_Constitution

Wikipedia contributors. (2019a). *Red states and blue states*. Wikipedia, The Free Encyclopedia. https://doi.org/10.1080/2330443X.2013.856147

Wikipedia contributors. (2019b, January 23). *Computer Fraud and Abuse Act*. Wikipedia, The Free Encyclopedia. https://doi.org/10.1177/1527476408323345

Williams, Rebecca L.; Greene, Adam H.; Barash, Louisa; Eckels, Jane; Rauzi, Edwin D.; Thurber, Kent B.; Blanchette, K. R. (2013). *New Omnibus Rule Released: HIPAA Puts on More Weight - Advisories & Blogs - Davis Wright Tremaine*. Dwt.Com. https://www.dwt.com/new-omnibus-rule-released-hipaa-puts-on-more-weight-01-23-2013/

World Economic Forum. (2014). *Personal Data: The Emergence of a New Asset Class | World Economic Forum - Personal Data: The Emergence of a New Asset Class*. http://www.weforum.org/reports/personal-data-emergence-new-asset-class

Appendix A

Survey Questions

Text in italics was not shown to respondents taking the survey. In addition, respondents did not see question numbers or group number information.

QUALIFYING QUESTIONS (all respondents)

1 During the past 12 months, have you accessed the internet at least once a month using one or more of the following devices: personal computer (desktop or laptop), tablet, or smartphone?

- ○ Yes
- ○ No

2 Were you a registered voter in your state of residence in 2018 or 2019?

- ○ No - I was not registered to vote.
- ○ Not Sure - I am not sure if I was registered to vote.
- ○ Republican - Yes, I was registered to vote as a Republican.
- ○ Democrat - Yes, I was registered to vote as a Democrat.
- ○ Independent - Yes, I was registered to vote but did not choose a political party.
- ○ Other – Yes, I was registered to vote as a member of a party not listed above.

**Respondents who answered 'No' to question one or something other than 'Republican' or 'Democrat' to question two were exited from the survey.*

AWARENESS CONSTRUCT (all respondents)

3 When using your personal device(s) to access the internet, do you believe that personal information about you is being gathered and stored while you are connected to the internet?

- ○ Yes
- ○ No
- ○ Maybe

4 Which of the following groups, if any, do you think are collecting and storing personal information about your activity when you use their service or visit their websites?

<u>Select all that apply</u>

- ☐ Your internet service provider
- ☐ The internet browser that you use (e.g., Chrome, Firefox, Internet Explorer/IE, Safari, Edge, etc.)
- ☐ Social Media Websites (e.g., Facebook, YouTube, Instagram, Twitter, WhatsApp, Reddit, LinkedIn, Pinterest, etc.)
- ☐ Online shopping sites (e.g., Amazon, eBay, Walmart, etc.)
- ☐ I do not believe that any websites or online services collect personal data about me.
- ☐ I don’t know if any websites or online services collect personal data about me.

5 What percentage of websites do you believe are actively collecting and storing personal data about you when you visit their site?

- ○ Less than 25% of all websites collect data about me when I visit their site.
- ○ 25-50% of all websites collect data about me when I visit their site.
- ○ More than 50% of all websites collect data about me when I visit their site.
- ○ I do not believe any websites are collecting or storing my personal information.
- ○ I have no idea what percentage of websites collect data about visitors.

6 Select from the options below all instances when you believe data is being collected about you.

Select all that apply

☐ When I am actively using my personal device(s) for online activity (e.g., internet browsing, online shopping, or social media/entertainment portals).

☐ When I am actively using my personal device(s) for purposes other than online activity (e.g., using mobile apps, playing games, or streaming music).

☐ When I am not actively using my personal device(s) but the device(s) has not been powered down (e.g., apps working when device is not being used, automatic software updates, or system backups).

☐ I don't think data is collected about me during any of the instances described in this question.

☐ I believe data about me is being collected, but I do not know when it is happening.

7 When personal data about you is collected, how do you think that data might be used?

Select all that apply.

☐ It is only used by the original data collector for internal purposes and is never shared with, or sold to, anyone outside of the company.

☐ My personal data is never shared, but it is sometimes used by the original data collector to allow advertisers on the data collector's website to deliver targeted to me.

☐ It is sometimes sold by the original data collectors to others who want access to my personal information.

☐ Nothing is done with my personal data and the companies collecting it do not currently use the data in any way.

☐ I don't know how my data is used.

8 <u>True or False</u>

There are companies that collect personal data by placing data tracking files on users' computers, which allows these companies to legally track and gather personal information anytime the users go online?

- ○ True
- ○ False
- ○ I'm not sure.

9 <u>True or False</u>

The companies collecting the data referenced in the previous question will build and maintain individual profiles on all people from whom they are collecting personal data?

- ○ True
- ○ False
- ○ I'm not sure

10 True or False

There are companies whose primary business function is to collect personal information from many different sources (both online and offline), creating detailed individual profiles, and then they sell those profiles to anyone willing to pay for them.

- ○ True
- ○ False
- ○ I'm not sure

11 True or False

Some websites collect personal information from individuals visiting their sites, combining it with data from other sources to create individual visitor profiles. Those websites then sell ads that allow advertisers to use the personal profiles to more accurately deliver advertisements to website visitors.

- ○ True
- ○ False
- ○ I'm not sure

12 Google and Facebook both make the majority of their revenue in the same way, as do other similar types of companies. How do you think Google and Facebook make the majority of their income/revenue?

Select One Answer

○ The majority of the revenue generated by these two companies comes from the simple act of people visiting and using their sites; the more people who go to their sites the more money they make.

○ Both companies generate the majority of their revenue by selling targeted ads, using the profiles that they have created on individual users who have visited their sites or who have created accounts.

○ I know how these companies generate the majority of their revenue, but I do not see the correct option provided here.

○ I am not sure how they make money.

**Respondents who answered 'False' to both questions 10 and 11, classified as Group Three, were routed to B Path, question 16, then to the demographic questions, and finally exited from the survey.*

All respondents who qualified as Group One followed the A Path of questions. All respondents who qualified as Group Two followed the B Path of questions.

Group One

KNOWLEDGE CONSTRUCT

For the remainder of this survey, we will use two terms with the following definitions (both definitions are true, and companies do exist that perform these types of functions):

"Data Broker" - Private companies whose primary business is collecting personal information about adult individuals (from both online and offline sources) and selling that information to others. More simply stated, Data Brokers buy and sell personal data

"Data Collector" - Private companies that collect personal information about adult individuals (from both online and offline sources), using that information only to sell advertising space on their websites (e.g., Google or Facebook). More simply stated, Data Collectors collect personal data for the purpose of selling advertising space on their websites. They are different from "Data Brokers" because they do not sell individual personal profiles directly to anyone. Instead, they sell the right to deliver targeted advertisements to people based on personal profile details.

For the purposes of this survey, the following industries are EXCLUDED from both definitions and SHOULD NOT be considered when answering any questions: healthcare, finance, and credit reporting.

NOTE: For the purposes of this survey, the following industries SHOULD NOT be considered when answering questions: healthcare, finance, and credit reporting. Only think about companies outside of those three industries.

13A True or False

In the U.S. there are laws that give all citizens the right to review personal data profiles held about them by any organization.

- ○ True
- ○ False
- ○ I'm not sure

14A True or False

In the U.S. there are laws that give all citizens the right to request corrections to inaccuracies found in the personal profiles held about them by any organization that gathers or sells their information.

- ○ True
- ○ False
- ○ I'm not sure

15A True or False

By law, before any organization can sell information about an individual, they are first required to obtain permission from the individual.

- ◯ True
- ◯ False
- ◯ I'm not sure

16A True or False

By law, if you prefer not to have your personal information sold by a Data Broker or Data Collector, you can simply submit a form requesting not to have your information sold.

- ◯ True
- ◯ False
- ◯ I'm not sure

REMINDER: Data Brokers buy and sell personal data. Data Collectors collect personal data for the purpose of selling advertising space on their websites.

17A True or False

The activities of Data Brokers and Data Collectors are currently regulated by federal legislation?

- ○ True
- ○ False
- ○ I'm not sure

18A True or False

The activities of Data Brokers and Data Collectors are currently regulated by state legislation?

- ○ True
- ○ False
- ○ I'm not sure

19A True or False

You have the legal right to request to opt-out from having data collected about you by Data Brokers or Data Collectors?

- ◯ True
- ◯ False
- ◯ I'm not sure

REMINDER: Data Brokers buy and sell personal data. Data Collectors collect personal data for the purpose of selling advertising space on their websites.

20A How many states do you believe have legislation currently in place that regulates how Data Brokers or Data Collectors can collect or sell your personal data?

- ◯ At least one state, but fewer than 10 states
- ◯ 10 – 25 states
- ◯ 26 – 50 states
- ◯ No U.S. states currently have legislation in place to regulate how Data Brokers or Data Collectors collect or sell personal data
- ◯ I have no idea

21A In what year do you believe was the first federal legislation enacted in the U.S. to regulate the data collection and data sales activities of either Data Brokers or Data Collectors?

- ○ 1993
- ○ 1997
- ○ 2010
- ○ 2017
- ○ There are currently no federal laws to regulate the data collection and data sales activities of either Data Brokers or Data Collectors
- ○ I have no idea

CONCERN CONSTRUCT

NOTE: For all remaining questions, please exclude companies working in the healthcare industry, the finance industry, and the credit reporting industry from consideration. Only think about companies outside of those three industries. REMINDER: Data Brokers buy and sell personal data. Data Collectors collect personal data for the purpose of selling advertising space on their websites

FACTS: Individuals have no legal rights to review the data contained in their personal profiles. There are no laws that regulate what type of security must be in place to protect the personal data files held by Data Brokers or Data Collectors. Anyone (individual or business) can purchase profile information from Data Brokers.

22-24A Please rate your level of concern with the following:

	Extremely concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Extremely unconcerned
- That inaccurate information might be contained in profiles that have been created about you?	○	○	○	○	○
- That Data Brokers and Data Collectors are able to independently decide what kind of data security they will provide to protect your personal information?	○	○	○	○	○
- That Data Brokers and Data Collectors are allowed to sell the profiles they have created about you to anyone willing to pay for the information?	○	○	○	○	○

25A Because anyone can purchase individual personal profiles from Data Brokers and Data Collectors, do you believe that state and federal governments are purchasing personal information about you from these organizations?

- ○ Yes
- ○ No
- ○ I'm not sure

FACT: State and Federal agencies are purchasing data from companies that collect and sell personal information.

26A Please rate your level of concern about the below situation.

	Extremely concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Extremely unconcerned
- State and federal governments are purchasing personal information about you from Data Brokers and Data Collectors.	○	○	○	○	○

FACT: Currently, there is no state or federal legislation enacted in the U.S. that regulates the activities of Data Brokers or Data Collectors specific to how they collect or sell your personal information.

27-29A Please rate your level of concern with the following:

	Extremely concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Extremely unconcerned
- The amount of personal data collected about you?	○	○	○	○	○
- How your personal data is being shared with others?	○	○	○	○	○
- The absence of legislation that would regulate the activities of these organizations?	○	○	○	○	○

DESIRE CONSTRUCT

30A Do you believe it is necessary that some form of legislation be created to protect the personal information rights of U.S. citizens?

○ Yes

○ No

○ I'm not sure

REMINDER: Data Brokers buy and sell personal data. Data Collectors collect personal data for the purpose of selling advertising space on their websites.

Select one option below that completes the statement summarizing your opinion about how Data Brokers and Data Collectors should be treated by any laws that are created to oversee their industries.

31A I believe that any law designed to protect individual personal data rights should...

- ○ be applied to BOTH Data Brokers and Data Collectors.
- ○ be applied ONLY to Data Brokers and NOT be applied to Data Collectors.
- ○ NOT be applied to Data Brokers and should ONLY be applied to Data Collectors.
- ○ I don’t know or I don’t have an opinion.

FACT: Currently there are no state or federal laws requiring Data Brokers or Data Collectors to give individuals access to the profiles that have been created about them. Additionally, there are no laws that require these companies to correct inaccurate information in anyone’s personal profile.

32-34A How strongly do you agree or disagree with the three sentences that complete the following statement?

I believe that there should be legislation requiring Data Brokers and Data Collectors to...

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
provide individuals with access to their personal profiles so that people are aware of what information has been compiled about them.	○	○	○	○	○
provide individuals with the opportunity to request corrections to inaccurate information contained in a personal profile.	○	○	○	○	○
reveal to an individual all of the sources that were used to build an individual's personal profile.	○	○	○	○	○

35A If it is decided that legislation is to be introduced to oversee the both the Data Brokerage and Data Collection industries, which of the following would be your preferred approach to creating and implementing this new legislation?

- ○ I believe that one piece of federal legislation, enforced in all 50 states, would be the best approach for achieving a comprehensive and complete solution to protect all citizens' personal data.
- ○ I believe that individual state-level legislation, with unique sets of laws created and enforced by each individual state, would be the best approach for achieving a comprehensive and complete solution to protect all citizens' personal data.
- ○ I am not sure which option would be best.

36A How quickly do you believe legislators should begin the process of creating new legislation to oversee the Data Brokerage and Data Collection industries?

- ○ Immediately, making it a top legislative priority
- ○ Sometime within the next 6 - 12 months
- ○ Within the next 12 - 24 months
- ○ Although important, it does not require attention anytime within the next 24 months
- ○ It is not important enough yet to set a timeline

37A With an estimated 4,000+ Data Brokerage companies operating in the U.S., and countless other companies and websites collecting and selling personal data, which of the following choices do you believe is the best solution for individuals who want to manage or protect how their personal information is collected and/or sold?

○ I believe there should be one centralized system where individuals can view all data collected about them by any organization participating in data collector or data sales in one place and request changes to inaccurate information.

○ I believe that things should not change and that companies participating in the collection and/or sale of personal data should not be required to allow individuals to have access to their own profiles or to request changes to inaccuracies.

○ I believe that individuals should have access to their profiles and that they should be allowed to request corrections to inaccuracies. However, I do not believe that it is necessary to centralize the process. Instead, I believe that everyone should be responsible for contacting each of the 4.000+ companies separately to access to their profiles and to request changes.

○ I do not care what information is collected or sold about me, so I do not care about managing my profile with any of the companies collecting data about me.

○ I don’t know or I don’t have an opinion.

**After question 37, all respondents are directed to the demographic questions.*

Group Two

KNOWLEDGE CONSTRUCT

NOTE: For the purposes of this survey, the following industries SHOULD NOT be considered when answering the remaining questions: healthcare, finance, and credit reporting. Only think about companies outside of those three industries.

13B True or False

In the U.S. there are laws that give all citizens the right to review personal data profiles held about them by any organization.

- ○ True
- ○ False
- ○ I'm not sure

14B True or False

In the U.S. there are laws that give all citizens the right to request corrections to inaccuracies found in the personal profiles held about them by any organization that gathers or sells personal information.

- ○ True
- ○ False
- ○ I'm not sure

15B True or False

By law, before any organization can sell information about an individual, they are first required to obtain permission from the individual.

- ○ True
- ○ False
- ○ I'm not sure

16B True or False

By law, if you prefer not to have your personal information sold by companies that collect or sell personal data, you can simply submit a form requesting not to have your information sold.

- ○ True
- ○ False
- ○ I'm not sure

17B True or False

The activities of companies that collect or sell personal data are currently regulated by federal legislation?

- ○ True
- ○ False
- ○ I'm not sure

18B True or False

The activities of companies that collect or sell personal data are currently regulated by state legislation?

- ◯ True
- ◯ False
- ◯ I'm not sure

19B True or False

You have the legal right to request to opt-out from having data collected about you by companies that collect or sell personal data?

- ◯ True
- ◯ False
- ◯ I'm not sure

20B How many states do you believe have legislation currently in place that regulates how companies can collect or sell personal data?

- ○ At least one state, but fewer than 10 states
- ○ 10 – 25 states
- ○ 26 – 50 states
- ○ No U.S. state currently has legislation in place that regulates how companies collect or sell personal data
- ○ I have no idea

21B In what year do you believe was the first federal legislation enacted in the U.S. to regulate the data collection and data sales activities of companies that collect or sell personal data?

- ○ 1993
- ○ 1997
- ○ 2010
- ○ 2017
- ○ There are currently no federal laws to regulate the activities of companies that collect or sell personal data
- ○ I have no idea

CONCERN CONSTRUCT

NOTE: For the purposes of this survey, the following industries SHOULD NOT be considered when answering questions: healthcare, finance, and credit reporting. Only think about companies outside of those three industries.

FACTS: Individuals have no legal rights to review the data contained in their personal profiles. There are no laws that regulate what type of security must be in place to protect the personal data files held by companies that collect or sell personal data. Anyone (individual or business) can purchase profile information from companies that sell personal data.

22-24B Please rate your level of concern with the following:

	Extremely concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Extremely unconcerned
- That inaccurate information might be contained in profiles that have been created about you?	○	○	○	○	○
- That companies that collect or sell personal data are able to independently decide what kind of data security they will provide to protect your personal information?	○	○	○	○	○
- That companies that collect personal data are allowed to sell the data they have collected about you to anyone willing to pay for the information?	○	○	○	○	○

25B Because anyone can purchase personal profiles from companies that collect or sell personal data, do you believe that state and federal governments are purchasing personal information about you from these organizations?

- ○ Yes
- ○ No
- ○ I'm not sure

FACT: State and Federal agencies are purchasing data from companies that collect and sell personal information.

26B Please rate your level of concern about the below situation.

	Extremely concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Extremely unconcerned
- State and federal governments are purchasing personal information about you from companies that collect or sell personal data.	○	○	○	○	○

FACT: Currently, there is no state or federal legislation enacted in the U.S. that regulates the activities of how companies collect or sell your personal information.

27-29B Please rate your level of concern with the following:

	Extremely concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Extremely unconcerned
- The amount of personal data collected about you?	○	○	○	○	○
- How your personal data is being shared with others?	○	○	○	○	○
- The absence of legislation that would regulate the activities of these organizations?	○	○	○	○	○

DESIRE CONSTRUCT

30B Do you believe it is necessary that some form of legislation be created to protect the personal information rights of U.S. citizens?

○ Yes

○ No

○ I'm not sure

31B Please select one option below that completes the following statement summarizing your opinion about how companies that collect or sell personal data should be treated by any laws that are created to oversee this industry.

I believe that any law designed to protect individual personal data rights should...

- ○ be applied to ALL companies equally, regardless of whether they sell personal data to make money or if they use data to sell more targeted advertising space.
- ○ be applied ONLY to companies that sell personal data and NOT be applied to companies that use data to sell target advertising space.
- ○ NOT be applied to companies that sell personal data and should ONLY be applied to companies that use data to sell targeted advertising space.
- ○ I don’t know or I don’t have an opinion.

FACT: Currently, there are no state or federal laws requiring companies that collect or sell personal data to give individuals access to the profiles that have been created about them. Additionally, there are no laws that require these companies to correct inaccurate information in anyone’s personal profile.

32-34B How strongly do you agree or disagree with the three sentences that complete the following statements?

I believe that there should be legislation requiring companies that collect or sell personal data to...

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
provide individuals with access to their personal profiles so that people are aware of what information has been compiled about them.	○	○	○	○	○
provide individuals with the opportunity to request corrections to inaccurate information contained in a personal profile.	○	○	○	○	○
reveal to an individual all of the sources that were used to build an individual's personal profile.	○	○	○	○	○

35B If it is decided that legislation is to be introduced to oversee both the personal data collection and data sales industries, which of the following would be your preferred approach to creating and implementing this new legislation?

- ○ I believe that one piece of federal legislation, enforced in all 50 states, would be the best approach for achieving a comprehensive and complete solution to protect all citizens' personal data.
- ○ I believe that individual state-level legislation, with unique sets of laws created and enforced by each individual state, would be the best approach for achieving a comprehensive and complete solution to protect all citizens' personal data.
- ○ I am not sure which option would be best.

36B How quickly do you believe legislators should begin the process of creating new legislation to oversee the data collection and data sales industries?

- ○ Immediately, making it a top legislative priority
- ○ Sometime within the next 6 - 12 months
- ○ Within the next 12 - 24 months
- ○ Although important, it does not require attention anytime within the next 24 months
- ○ It is not important enough yet to set a timeline

37B With an estimated 4,000+ companies collecting and selling personal data in the U.S., which of the following choices do you believe is the best solution for individuals who want to manage or protect how their personal information is collected and/or sold?

○ I believe there should be one centralized system where individuals can view all data collected about them by any organization participating in data collector or data sales in one place and request changes to inaccurate information.

○ I believe that things should not change and that companies participating in the collection and/or sale of personal data should not be required to allow individuals to have access to their own profiles or to request changes to inaccuracies.

○ I believe that individuals should have access to their profiles and that they should be allowed to request corrections to inaccuracies. However, I do not believe that it is necessary to centralize the process. Instead, I believe that everyone should be responsible for contacting each of the 4.000+ companies separately to access to their profiles and to request changes.

○ I do not care what information is collected or sold about me, so I do not care about managing my profile with any of the companies collecting data about me.

○ I don’t know or I don’t have an opinion.

**Groups One and Two both respond to the same demographic questions.*

Group Three

Qualifying Question *(this question is only given to Group Three before directing them to the demographic questions)*

Not including healthcare companies, financial companies, and credit reporting companies, do you believe that any other companies collect personal data about you?

- ○ Yes
- ○ No

Appendix B (Demographic Questions)

Demographic Factor Groups and Factor Group Categories. These questions were given to all respondents: Groups 1-3.

38 What is your Sex?

- ○ Male
- ○ Female

39 What is your age range?

- ○ 18 - 24
- ○ 25 - 38
- ○ 39 - 54
- ○ 55 - 65
- ○ Over 65

40 What is your highest level of completed education?

- ○ I did not complete high school
- ○ High school graduate, diploma or the equivalent
- ○ Some college credit, no degree
- ○ Trade/technical/vocational training
- ○ Associate degree
- ○ Bachelor's degree
- ○ Master's degree
- ○ Professional degree
- ○ Doctorate degree

41 What is your race/ethnicity?

- ◯ White
- ◯ Hispanic or Latino
- ◯ Black or African American
- ◯ Native American or American Indian
- ◯ Asian / Pacific Islander
- ◯ Other

42 In what type of community do you live?

- ◯ City/Urban
- ◯ Suburban
- ◯ Rural/Farm

43 What zip code do you live in?

_____