2020

Elite Theory Application to Social Privacy Concerns During Domestic Government Surveillance

George Vahn
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

George Vähn

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. George Larkin, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Lynn Wilson, Committee Member,
Public Policy and Administration Faculty

Dr. Victoria Landu-Adams, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Elite Theory Application to Social Privacy Concerns

During Domestic Government Surveillance

by

George Vähn

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

November 2020

Abstract

Policy professionals would benefit from a social theory capable of suggesting policy change ramifications prior to public implementation. There is a research analysis shortfall concerning the usefulness of elite theory in modern social change. This study was an investigation of the effectiveness of elite theory to inform public policy analysts of behavioral outcomes following policy creation or change. Elite theory is the theoretical foundation that guided the framework of this study. The research question examined the effectiveness of elite theory to suggest behavioral outcomes in response to reduced personal privacy due to domestic government surveillance. A correlational research design was integrated with a thematic methodology to analyze 8,223 secondary data points obtained from a randomized sample of 1,537 adult, English speaking panel participants across the United States from the years 2013 through 2015. Selective coding using key word, key phrase, and subject matter matching was employed to assign categorical values to panel responses about privacy and personal behavior. Themes were identified and triangulated with themes regarding privacy and behavior that emerged from the literature that was reviewed. The results indicated that individuals have strongly held beliefs regarding privacy but do not undertake sustained behavior to protect it. The results point to an alignment with elite theory suggesting that the social theory may be used in policy development. This research is significant for both government policy professionals and grassroots social change organizers as they navigate the potential effects of policy change.

Elite Theory Application to Social Privacy Concerns During Domestic Government Surveillance

by

George Vähn

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

November 2020

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Generally, public policy refers to a system of decision making by the state from which laws and actionable strategies are promulgated upon the public to address some identified issue in society; public policy is government policy that affect the whole population (Merriam-Webster., n.d.). In the United States, national security policy is a broadly defined phrase that is rooted in the overarching need to protect the structure, integrity, and framework of the state as well as the physical security of the citizens therein (Aftergood, 2012). National security policy is initially formed by federal agencies such as the National Security Council (NSC), and the Homeland Security Council that advise the President who makes policy decisions. (Whittaker, 2011). Policy is ultimately implemented through a regulatory framework created by and interpreted by the three separate and distinct branches of government.

Governmental policy touches on virtually every aspect of life including food, education, healthcare, personal access to goods and services, domestic law enforcement, national defense, and individual privacy through the implantation of laws, administrative codes, and local ordinances. Policy development on a national level results from the federal government's internal planning and response to an actual or perceived threat, social need, or requirement of government. This includes public health, civil order, physical safety from external extra-domestic threats, or homegrown domestic threats.

Background

Following the terror attacks that occurred on September 11, 2001, policy experts were faced with a challenging new group of responsibilities both domestically and abroad. In the decade following the attacks, international security threats morphed from a predominately physical risk of attack like those occurring on 9/11, to bioweapon and epidemiological attacks, cyber-attacks, infrastructure failures, data hacks, and direct or indirect foreign influence campaigns. To combat this new terrorist paradigm, defense policy shifted in large part from a boots-on-ground approach to a more complex information-based 22 agency defense network capable of identifying terror threats in their pre-execution phase (U.S. Department of Homeland Security, 2017).

Humans require safety in their everyday lives second only to physiological needs like air and water. (Maslow, 1954). However, inherence to information-based safety policy is often a tradeoff wherein security becomes more robust at the expensive of increased data aggregation and the diminishment of individual civil liberties (Eidam, 2017). Citizen data donors may not be consciously aware of or involved in the data aggregation network that underlies data surveillance programs. Government data mining is most often accomplished through nontransparent mechanisms and third-party commercial data venders that are associated with social media, tele-communications, and private utility companies (Leetaru, 2019).

Even those individuals generally resistant to data sharing in a perceived low-threat environment may choose purposeful data donation when they believe they are in a

high-risk threat environment believing it may move them from a higher to a lower risk state. Even when individuals are aware that their data will be shared with the government, they are often unaware why, how, or to whom the data is ultimately being provide (see Pew research datasets below).

The relationship between high and low risk states may be described as a secure-freedom continuum. Many individuals will exchange degrees of safety and security along this continuum for rights and freedoms including privacy. In the human hierarchy of needs safety is paramount (Maslow, 1954). National security policy professionals and legislators are challenged to position the population in the safety continuum such that society will achieve an acceptable balance of safety, privacy, and freedom.

The social effects of security policy changes may not be known during the policy creation stage and it is not until they are implemented, with social feedback generated and analyzed that determinations of effectiveness can be understood. There are only a few mechanisms available to policy professionals that assist them in intelligently choosing one policy creation scenario over another with some level of outcome-based certainty. Individuals tasked with obtaining policy objectives may benefit from an additional theoretical model capable of assisting with predicate outcomes of collateral social consequences. If a reliable outcome-based theory could be implemented at the beginning of policy creation, outcomes could align more accurately with policy objectives.

One potentially useful theoretical tool for suggesting future social behavior is elite theory. Elite theorists suggest that only a relatively small, elite sub-group of groups or individuals can make sound social policy decisions (Pareto, 1935). If this theory is accurate it could be applied to a variety of policy judgments and may allow for the virtual disregard of collateral social effects when forming initial policy strategy. I designed this study to test the hypothesis that elite theory may be employed as a tool for understanding social change. I am not aware of another study designed to inform scholars whether elite theory may be an instrument of social policy analysis.

My study used public awareness of the United States government's domestic data surveillance and eavesdropping program to evaluate individuals' reaction in response to threats against a civil liberty (privacy), and to determine whether there is a relationship between the two. I examined if elite theory may be useful as an analysis component during initial drafting of security policy. The result of this study may provide insight into the viability of adopting elite theory as a modern tool applicable to the creation and analysis of other national security policy.

This first chapter will serve to establish the significance of the research, introduce the reader to the content in the remainder of the study, discuss important terms, explain assumptions, and identify possible limitations of the study. A thematic analytical approach is used to synthesize different types of scholarly literature, pre-existing studies, and publicly sourced secondary data to offer a perspective not previously available to policy professionals.

Statement of the Problem

In the aftermath of 9/11, policy makers across the nation were confronted with the task of protecting the American public from exposure to catastrophic attacks in the future. The methods used by terrorists on 9/11 drew attention to a different tactic of terrorism not previously encountered on such a scale. The terror offensive used civilian aircraft as guided weapons achieving a high fatality ratio on domestic soil and it became clear that this form of terrorism could not be neutralized by conventional wartime tactics as there was no direct state actors involved. Instead, nonlinear dynamic defense strategies would have to be created to meet the new threat. This would ultimately be accomplished not by using more munitions against the enemy but by using more information. Policy makers concluded that the most effective way to fight terror on American soil was to pre-emptively prevent actions during their initial preattack phases. This could be accomplished through domestic and international offensive information campaigns but would require enormous quantities of data.

An active participation and prevention strategy would require local law enforcement and federal government agencies to acquire, analyze, and share massive amounts of data on every individual in the country to stay one step ahead of terrorist planning and execution. Operationally, staying ahead requires unobstructed access to current, dynamically updated information regarding enemy access to planning and resources. Obtaining information on a scale large enough to be effective means creating a virtual digital fishing net capable of extracting and amassing enormous volumes of data

from the lives of hundreds of millions of individuals while simultaneously developing an algorithmic system robust enough to analyze and report on it in near real time.

With the integrating of proprietary government technologies and large private corporations' access to individuals' data, U.S. intelligence agencies were able to develop programs capable of obtaining and retaining incredibly large volumes data on American citizens including the Utah Data Center (UDC) which is said to be capable of storing over 5 zettabytes of private information on individuals; equivalent to 100 years of worldwide communication (Berkes, H. 2013). Although this could yield information potentially useful to predict and prevent future terror attacks (albeit with debatable effectiveness), the capability came at a price paid in privacy. The fundamental challenge to policy makers is to balance the security requirements of the government while anticipating the collateral social consequence associated with a specific policy. If it were possible to employ a policy proposal mechanism prior to policy implementation then legislators and analysts could focus on policies that would be effective while simultaneously not producing unanticipated implementation results. I was not able to find literature addressing this specific subject and so the potential for using elite theory as a model was worth considering.

This study was designed to address a gap in the literature by examining the relationship between domestic government surveillance programs (the independent variable), and changes in individual protective privacy behavior (the dependent variable). The results could inform policy scholars and advisors on whether a program may or may

not be implemented with anticipation of social repercussions. This knowledge would assist policy professionals as they craft new policy or modify existing policy to satisfy national security goals.

Purpose of the Study

This study was designed to evaluate the potential relationship between the independent variable (government-sanctioned reductions of the civil liberty *personal privacy*), and the dependent variable (society's individual privacy-protective behavior in consideration of the government's known domestic monitoring programs). The study was undertaken following my realization that no other found research has directly addressed whether elite theory could be used to suggest social response following governmental policy action.

The research result could suggest whether elite theory may be useful in current national security policy analysis. The study is designed to test the hypothesis that elite theory is a reliable indicator of how the United States' population may behave in response to a forced reduction in civil liberty (privacy) and by extension to other aspects of changed social policy.

Elite theorists suggest that a nonelite population is largely apathetic to [national security] policy and is devoid of sustained investment in the protection of individual privacy rights (Pareto, 1935). I was unable to locate any other study that suggests whether elite theory may be used to evaluate social change outcomes. This study was undertaken to fill that void in the literature. The research will assist security policy makers, analysts,

and academics in their understanding of how elite theory may be used as a modern policy tool capable of describing social change outcomes.

Research Question

I sought to understand whether there is a relationship between knowledge of the government's secret domestic spy programs and subsequent changes in individual behavior in response to it. The study independent variable (IV) was the public knowledge of government covert domestic personal data collection programs and the dependent variable (DV) was the individual behavior-based social response to it.

These variables were analyzed alongside Pew research secondary datasets using Statistical Package for the Social Sciences (SPSS) software to identify relationships between the variables. Effect size and trend information are also considered when determining significance and strength of any relationship identified. The research question and testable hypothesis is as follows:

RQ1: Using existing studies and secondary data; what is the nature of the relationship among the independent variable (domestic government monitoring) and the dependent variable (individual protective behavior)?

$H_0$1: There is a positive and significant relationship between the independent variable (domestic government monitoring), and the dependent variable (individual protective behavior).

H_a1: There is no significant relationship between the independent variable (domestic government monitoring), and the dependent variable (individual protective behavior).

Conceptional Framework

The methodology used to evaluate this question is based on elite theory and used both thematic analysis and secondary datasets facilitating a quantitative examination of the hypothesis that there is no significant relationship between the variables, domestic government monitoring and individual protective behavior.

A thematic analysis of several prior research studies was used to inform my analysis of Pew research data sets providing broad access to a large sample population not otherwise available in consideration of financial and logistical constraints while at the same time offering a concise evaluation of whether a population will respond to surveillance. Chapter 3 will outline the datasets provided by Pew research and the methodology used to choose the informational elements included in the statistical analysis. Statistical information from the Pew datasets will be combined with a thematic analysis of existing scholarship and legal caselaw to provide a robust research result.

Single slice and multiple instance data from Pew were combined with scholarly articles and journals providing the reader with an understanding of the data in an overarching context. Datasets were selected using a specific criterion developed for use in this study to minimize bias and maximize use of the thematic analysis technique.

Assumptions

The following assumptions were necessary for this study because there were no reasonable ways to independently verify the veracity or eliminate assumptions of quality of the data. Deductive thematic analysis using a latent approach applied to multiple source research may in a more valid and more useful result than a single source option would have. The Pew data was assumed to be accurate and the participants honest in their answers. The data was assumed to be acquired using a proper and scientifically sound technique according to the methods indicated by the Pew research survey methodology (Pew, 2020).

Limitations

There may be limitations associated with sample-based studies that use structured-question data (normally associated with quantitative data collection methods), that exclude the flexibility associated with (qualitative) open-ended questions. Research limitations may also include constraints on the generalization and future applicability of the research results that have been produced from a finite, self-reporting sample population.

The Institutional Review Board (IRB) of Walden University preapproved the plan for my research under approval number 08-17-18-0512335 ensuring that the assumptions and modeling were designed within the appropriate limitations of hypothesis testing acceptable for an academic paper. This ensured not only that the research was ready for publication but that it was suitable for use in future studies as well.

Significance of the Study

Drafting and fine-tuning public policy in a way that fulfills the requirements of national security while simultaneously integrating into a social construct and a pre-existing legislative framework may be challenging. There may be social and political implications associated with any policy decision but those associated with national security may rank among the most important in constituent value and public concern. The research presented in this paper is significant because the result addressed these challenges and provided national security professionals with an understanding necessary to mitigate predictive challenges associated with creation and implementation of national security policy. The potential effect of this research with respect to social change may be profound.

If policy advisors can predict how a society or subvariant will behave in response to policy change then the implementation of policy will no longer be susceptible to reactionary unknows. Rather, policy makers may be able to predetermine responses and craft domestic policy with relative impunity and with the knowledge that their decisions will ultimately be accepted by society. This study may broaden the policy communities' understanding of how theory informs policy development and how policy professionals may take advantage of that relationship.

Summary

This research study was necessary to assist policy experts facing security challenges that require predictable strategies for achieving policy objectives. The

research allows analysts to review cause and effect relationships necessary to make predictions that assist in the policy drafting and implementation process. The design uses Pew research data obtained through structured data-collection techniques and uses statistical analysis to show the response of a national population. Chapter 2 of this study explains how thematic analysis of existing research is used to provide context and identify common effect across research studies.

Chapter 2: Literature Review

Meaningful social change may benefit from the creation and implementation of newly formed social policies effecting society at both the national and individual level. Drafting new social policy without predictable outcomes creates a challenge for policy professionals. They are left to guess how policy changes could affect populations far into the future. Policy experts may also need to account for the potential of collateral social consequences not intended by the primary policy goal. For example, a social policy requiring gun owners to register their firearms may primarily offer safety related benefits but may also be construed as an unconstitutional infringement of second amendment rights resulting in reduced compliance and increased government distrust.

The use of a social theory as a screening tool for proposed policy changes prior to implementation of those changes may be useful in mitigating collateral consequences. As a theoretical tool social-theory constructs may be included in the framework of a proposed policy and potentially used to suggest outcomes. Foresight into how a new policy will render over time may be invaluable to those tasked with creating it and may help to protect social structures from undesirable collateral changes.

Pareto described the elite theory social construct as social representation of a nonelite general population that is unable or unwilling to produce more desirable social outcomes than those in the elite class (Pareto, 1935). This paper examined whether there the theory may be used to suggest population behavior. If elite theory operating as a

policy analysis tool can provide social forecasting then it may prove to be a critical component in the creation of social change.

In this study I investigated whether there is a significant relationship between changes in perceptions about privacy and changes in individual privacy behavior. A relationship between these variables may signal the appropriate use of elite theory as a tool for informing policy makers of a population's future action prior to policy implementation.

I examined elite theory as applied in a post-9/11 security paradigm wherein there is a bipolar relationship between personal privacy and governmental intrusiveness. The post-9/11 environment in conjunction with leaked top-secret intelligence information provided a unique window of opportunity for research into government data monitoring programs and the effects they may produce in society. This research is important because national security policy touches every individual in the United States population. The ability to predict policy outcomes may be important to ensure that a proposed social change will benefit society or result in conformance with the primary intent of those implementing it.

Literature Relevance

The timing of this study was relevant because government mass monitoring programs are by nature highly secretive and the classified materials needed to understand them are not normally available to the public, academics, or nongovernment analysists (Federation of American Scientists, n.d.). However, following several prominent leaks of

top-secret information into the public domain beginning in 2013 (Sottek & Kopfstein, 2013), academics and private citizens were offered insight into some of the government's secret data collection programs and the associated policy strategies that the government had chosen to use.

I found research referencing privacy and elite theory to be compartmentalized and not addressing the usefulness of elite theory as a predictor of social policy outcomes in a modern population. This research study was necessary to better understand that relationship and to accurately assess elite theory as a potential policy tool. I addressed this topic within a holistic framework so that the reader may be better able to integrate theory with practice than would be otherwise be possible.

Literature Search Strategy

The literature review was undertaken to provide scholars and policy creators with a contextual framework from within which to understand the underlying components of privacy and surveillance discussed in this study. It was a jumping off point designed to provide readers with a predigested review of existing information related to the topics analyzed in the study.

Using information obtained from legal cases, historical documents, media sources, and peer reviewed journals this review provided a synthesized understanding of the how privacy is defined, what government mass monitoring in the United States looks like, and what the components of the elite theory social construct are.

Theoretical Foundation

The theoretical foundation for this study was elite theory. Social theorists have tried to explain the function and phenomena of societies and modern social science appears to finds its roots in interdisciplinary social theory. Individual social theories vary in both depth and breadth as they attempt to explain everything from the nature of an individual's behavior in society to a broad accounting for why entire populations behave as they do. The most recent trends include the adaptation and merging of multiple theories (to the exclusion of single theory explanations), to explain how a society will function (Webber, 1968). It is life experience and a personal orientation disfavoring elitism and privilege that brings me to the social construct of elite theory. I have tried to develop an overarching understanding of national security, government function, and social policy in order to present the topics in a coherent, research driven paper that may help others understand it as well.

A better understanding of elite theory may support policy decision making by equipping researchers with a theoretical basis from which they can analyze policy. Elite theorist may seek to describe the relationship of a population's power distribution in specific societal contexts and the decision-making powers that flow from that relationship may provide broad applicability to policy review in consideration of the current social backdrop in the United States.

Elite theory may offer a parallel explanation describing the differences between those in power and those in nonpower positions in society. Elite theory appears broader

and more applicable than periphery concepts like asymmetrical power structures, a state of exception, counter laws, or sovereignty double-speak (Morwood, 2012).

As a social concept elite theory may explain the counterintuitive relationship demonstrated by a society that appears to assign high value to individual privacy while simultaneously acquiescing to the dissolution of basic privacy protections. Although the effectiveness of applying elite theory may be questionable in other nations like Russia, North Korea, or China where the top-down political power structure is different than in America, the theory appears valid for use in this study because of an inherent accounting for the structure, form, and function of the quasi-democratic political system and diverse social makeup of the population of the United States.

Elite theorist posited that a small subsection of society (designated as elites or chosen ones) will inevitably control the affairs of the public (López, 2013). Ideologically, this may be because the traits of those most suited to govern (wealth, stature, intelligence, power, etc.) are distributed to only a small fraction of potential leaders. The theorists suggest that the remainder of the populous is uninformed, incapable of making policy decisions, or prone to anarchy and civil disturbance (López, 2013). Historically, the theory may be described in several variations including cost, crisis, and lack of willpower.

The idea of an uninformed public that is described by elitism may closely parallel other historical theories of public disconnect relating to civil policy. In 1957, Downs (2003) first spoke of the nonelite's rational ignorance. The theory conforms to the idea

that the public will avoid the purchase of knowledge or information (when it has a cost associated with it), because the public does not believe the cost will outweigh the benefit to them (e.g. that their vote could realistically impact an election, or a restriction on freely available information would materially affect their lives, (Downs, 2003).

Years before Downs' (1957) work, Lippmann (1922) opined that the public is apathetic, uninformed, and careless in their perceptions. Lippmann suggested a more modern yet parallel social theory that described public opinion as forming around crisis and subsequently fading over time. Lippmann's work argued that the public exhibit this absence of informed opinion due to a disinterest and lack of will to engage the time and resources required to be informed (Lippmann, 1922).

In 2016, Somin (2016) laid out a background explaining the long history of assumed ignorance by the public when it comes to politics and national policy and described the potential threat that it poses to democracy. Somin wrote that because individuals can not directly impact elections it is rational to assume that there is no incentive in becoming an informed voter despite acknowledging that this would potentially result in an unwanted outcome at the collective level (Somin, 2016).

Ignorance of policy and related decision making may not mean uninformed individuals cannot or do not affect policy. Where government action is largely positive or negative and individuals can see and identify with such an action or event those individuals may vote accordingly irrespective of valid rationality. It may be that the result

of ignorant voting is to further policies allowing for the future manipulation of that ignorance by those elected (Somin, 2016).

Elite theory may be described using multiple contextual components that have several related yet different meanings (Domhoff, 2010). Generally, elites may be those individuals or groups in a society that hold status, power, money, or other interest(s) in a greater quantity or strength than the rest of the population who are by necessity a majority. Interestingly, it may be possible for nonelites like the newly wealthy to overcome this neo-elite status and be assimilated into the traditional elites if offered the proper tools and context from within which to do so.

Elite theory may best be understood as a flexible set of ideas capable of integrating different components into an overarching theory. For example, elitism may be used to describe characteristics of a democracy wherein the elite hold power but the population are those who are able to influence political policy making. This democratic example does not account for inherent differences among those making up the median.

Gilens and Page (2014) explained that political elite groups may be diverse and include powerful special interest groups, lobbyists, Federal Advisory Committees (FAC), as well as the wealthy (or economic elite). In their research study, the authors point out that current views of the elite model include multiple elite sectors. While the most studied and referred to sector is the political elite there are also sectoring of elites in the military, religious, corporate, and other social environments (Gilens & Page, 2014). One may even envision the elite structure of a grade school playground wherein a power hierarchy

among the children plays out every day; one child is larger, one is more liked, another is smarter, and another may share candy to effect influence. These sectors may interact, compete, and influence one another at the elite levels of society.

Domhoff (2010) addressed these and other related issues in the example of a generalizable link between government officials, their economic backgrounds, stature, and distributed powers. Domhoff explored the FAC sector and its direct influence over policy. It was suggested that while the public has virtually no policy influence; it is a (mixed) theory of corporate, group, and individual elites that strongly influence policy (Domhoff, 2010). The Gilans et al. (2014) study of economic elites indicated that where a majority seeks to preserve the status quo of policy it is likely to be preserved. When a majority seeks to change the policy status quo but it is opposed by the elites it is unlikely to take place (Gilans, 2014).

The neo-elite models consist of integrations and cohesive agreements among elite groups that can form into ‘elite settlements’ and the establishment of a new order (López, 2013). Settlements may also be created because of stressors on the elites by nonelites over their interests (López, 2013). This is theorized to be the first step in elite convergence wherein the elites come together forming a functional, united political system (López, 2013). A failed example of this may be the United States’ attempt to democratize Iraq. That effort may have failed in part because the Iraqi elites were not able to realize this idealized formation.

Social inputs from nonelite population such as uprisings and poverty may also impact the elite function. The perception of social threat may be a necessary component in the continuation of stable democracies because it may pressure elites to allow nonelite input into the political system. That idea may also be applicable to elites' tolerance levels for poverty. Poverty in the population may be considered desirable for elites or not desirable depending on the context and current prevailing social modeling of the involved country. For example, poverty may be a positive attribute if considering social dominance or providing cheap labor but may not be positive for preventing the spread of disease or the mitigating the proliferation of violence and threats against the elite due to social unrest or desire for social change.

While there may be competing interests between the elite and nonelite populations, there does not appear to be a necessary divergence between the interests of the two. There may be circumstances where the interests of both converge and be a complementary goal of both groups like the desire for safety from nondomestic forces taking over the homeland. However, these congruencies appear to be the result of coincidental external circumstances and not a functional result of the theory itself.

Whether or not elite theory can be used to explain a population's response to government monitoring may be directly related to whether the population's common social structure values privacy and to what degree. Much of this chapter was dedicated to understanding what privacy is and means. My research suggested that privacy may be considered a strongly held ideal for many Americans. Defining that ideal however

appears to be a concept that is curiously complex, nebulous, and difficult to define with certainty. The ambiguity may result in part because privacy seems to be describable only as it is being observed through different contextual lenses as outlined below.

Understanding Privacy

In his 1965 dissenting opinion penned under the Griswold v. Connecticut Supreme Court case; Justice Black described the issue of privacy as a, "broad, abstract and ambiguous concept" (Griswold v. Connecticut 381 U.S. 479, 1965). Griswold represents the first and most seminal in a line of cases establishing the legal notion of privacy. Later cases continued to support the idea of legal protections of individual privacy establishing a virtual 'right' to privacy; simultaneously opening windows through which a judge's pen could reach to carve out exceptions to that protection.

Right to Privacy

Traditionally, rights or quasi-rights like privacy may be thought of as being created by legislation. But in practice they may actually grow outwardly from the judicial system. It is the courts that offer individuals civil and criminal protections and it is the courts that restrict personal actions; thus, defining how a nation will describe its social boundaries. In the United States legal policy has historically supported a citizen's 'right' to personal privacy. Individuals have had some protection from excessive government intrusion and overreaching into their private life.

Interestingly, the U.S. Constitution does not explicitly guarantee a right to privacy (U.S. Const.). To the extent that privacy is protected, the courts have established the

protections through case law derived mainly from the 1st, 3rd, 4th 5th, and 14th Constitutional Amendments. Privacy may be described as a somewhat flimsy and contextually malleable socially constructed quasi-right expectation of law. This is an important aspect of privacy because involuntary surveillance and the associated violations of a perceived privacy protection may affect individual behavior.

In 2015, a University of Richmond Law Review article suggested that the mere expectation of community surveillance is enough to affect the behavioral outcomes of individuals (Kaminski, Margot, Witnov, & Shane, 2015). The paper provided a comprehensive review of First Amendment theory in the context of both the historical and modern decision making process. The authors highlighted potential censorship issues connected to the conforming effects inherent in community behavior and group social interactions (Kaminski, et al., 2015).

The study suggested that community conformance has a direct impact on how policy is generated and how people decide social issues. Conformance fears may increase anxiety levels in individuals that are undecided on specific issues. It may even change closely held beliefs that are nonconforming resulting in cognitive dissonance within the individuals (Kaminski, et al., 2015). Researchers identified knowledge or awareness of privacy issues as a potential cause for changed perceptions and perceptions inside of a physical community (like a neighborhood or social group), and play a role in altered behavior.

This chapter in my study describes privacy development over the past few decades as it has been interpreted by the courts in physical, personal, and digital forms. The march of technological progress has contributed to change by amplifying the inherent push-pull of privacy and public safety. That continued tension is demonstrated throughout the numerous privacy cases in the United States court system. The following analysis of privacy related case law demonstrates the uncertain nature of privacy related judicial outcomes and I discuss the categories that seem to frame the current legal review of privacy.

Physical Privacy

Courts have used the subjective expectation of privacy of individuals targeted by the government to define the limits of government intrusion (Smith v. Maryland, 1979); a case involving the State's use of a pen register to secretly record a defendant's phone call numbers. However, in Greenwood the court demarcated a limit to that expectation. The Greenwood case compares a defendant's individual notion of privacy to society's objective view of a legitimate expectation (California v. Greenwood, 1988).

In Greenwood, the court found that garbage placed at the curb of a suspect's residence does not meet the (narrower) societal expectation; effectively negating any 4th amendment claim from protecting the garbage bag's contents. These criteria are embodied in the 'Katz test'. In Katz, the defendant was recorded by the federal government while having 'private' conversations in a public telephone booth. The court determined that such conversations were, in fact, private and thereafter created a privacy

test consisting of two prongs. Under the test a defendant must demonstrate a subjective expectation of privacy and the objective public must be willing to recognize that expectation as legitimate (Katz., et al).

Expectations of privacy depend heavily on an individual's privacy sensitivity level. This level will temporarily rise (Farid, 2015), and specific civic behaviors can be artificially changed when people are made aware that their activities are being monitored (Panagopoulos, 2011). In response, some people choose to utilize anonymizing technologies to insulate themselves from monitoring (Madden & Rainie, 2015); or they may censor their actions entirely (Marthews & Tucker, 2014).

However, other studies suggest that a larger segment of the public does not care about monitoring and that any level-increases diminish over time as people become immune to a heightened surveillance environment (Oulasvirta, 2012). According to the Pew Research Center, nearly half of U.S. citizens approve (or do not disapprove), of their government monitoring private communications (PRC, 2013).

In 2015, an exploratory study of 30 cases were undertaken to determine whether short term privacy sensitivity levels could be manipulated in people exposed to video clips about privacy. The 'treatment' video clips were designed to inform the cases of the importance of privacy, surveillance, protecting personal information, and new technology (Farid, 2015). The control group was not exposed to the video clips about privacy and both groups responded to questionnaires' regarding privacy.

The research demonstrated that neither group had an adequate understanding of privacy or surveillance related issues. It was only after the treatment group watched informative videos that their knowledge increased enough to understand the questions regarding RFID and other technology inquiries. Statistical analysis of the data obtained by Farid, 2015 revealed that exposure to the new information did significantly raise privacy expectation levels and personal privacy concerns (at least temporarily), and that women were disproportionately affected though the study did not offer a definitive reason why (Farid, 2015). While the study did evidence immediate changes in perceptions it did not comment specifically on whether those perceptions would result in changed behavior.

A 2011 study by Panagopoulos went beyond individual perceptions and quantitatively examined large amounts of secondary data from an earlier 2008 analysis (demonstrating that community voter turnout could be artificially manipulated by informing community members that there voting activities were being monitored). The study found that people are 'highly reactive' to information suggesting their community would know whether they voted; and noted that the size of the community was not a significant predictor of the behavior change (Panagopoulos, 2011).

The Panagopoulos study suggested that social pressure and the desire to exhibit community compliant social behavior occurs when people are confronted with concrete information that they're behavior is not only monitored but reported and would be shared with other community members. The behavior change will occur from the mere 'threat'

of surveillance and exposure of non-conforming behaviors as the experiment offered no evidence that the people were actually being reported (Panagopoulos, 2011).

Based on federal cases like the 1991 U.S. v. Penny-Feeney decision, one would suspect that the Supreme Court of the United States decision penned a decade later in the 2001 Kyllo case would have protected the privacy of a defendant (against such things as the use of heat-sensing Forward Looking Infrared (FLIR) by law enforcement). However, in Penny-Feeney, the district court upheld the use of FLIR by law enforcement (without a warrant), explaining that defendants did not demonstrate a subjective expectation of privacy regarding the "heat waste" they created, nor did they attempt to exercise dominion over the waste preventing it from venting to the public.

With the notable exception of Kyllo, the courts generally continue to view FLIR as a constitutionally acceptable method of warrantless surveillance by the government. Kyllo appears to have supported States rights' instead of following the federally established history of cases. In 2001 Justice Scalia and the Kyllo majority opined that a FLIR device used by police to identify a hotter than usual house effectively explored the intimate details inside a private home; something normally requiring physical intrusion and therefore a warrant. Scalia wrote that, "to withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment". The minority noted that there should be a distinction between through the wall and off wall surveillance, arguing that through the wall is intrusive by nature.

The Eleventh Circuit court in United States v. Ford attempted to remedy this seeming inconsistency by determining that, “the thermal imagery at issue here appears to be of such low resolution as to render it incapable of revealing the intimacy of detail and activity protected by the Fourth Amendment”, U.S. v. Ford, 34 F.3d 992 (1994). FLIR technology has advanced since that opinion and is now very detailed.

The court in both Myers and Pinson agreed that a FLIR device is passive and non-intrusive. It does not intrude in any way into the privacy and sanctity of the home and that it operates by sampling the thermal waste given off by a structure without requiring beams or rays or any other penetration into the structure. This is very similar to the court’s interpretation of airspace above a residence. Airspace has been viewed by the courts as publicly assessable and not within the protections of the 4th amendment, thereby upholding law enforcement’s right to surveillance of properties from private aircraft without a warrant. It is like the ‘open field’ theory as outlined by Hester v. United States, 265 U.S. 57 (1924). Hester stands for the legal principle that an individual may not (legitimately) expect privacy outside the home except in areas immediately adjacent to the structure, even if they are on private property.

Individual Privacy

Privacy as an expansive protection extending beyond the 4th Amendment provisions of one’s home was expanded to include the actual individual. Over time, this idea has broadened to include aspects of the individual like reputation, intellectual

products, and spiritual nature. Privacy of the individual may be important because people may alter their behavior when they demonstrate concern over surveillance-risk levels.

A study was undertaken to analyze a finite community of high-risk individuals following the events of September 11, 2001. The study was framed around the legal holding in the Heart of Atlanta Motel court case; one of the leading cases to address race issues and the exclusion of a specific race from accessing an otherwise public resource. This study was designed to parallel the experiences of the Sikhs in America following 9/11; most of who refrained from air travel, and self-imposed travel restrictions to avoid embarrassment for some period.

The study analyzed the post 9/11 Internet behavior of over three hundred (311) Muslim-Americans. Results suggested that among a minority of individuals who indicated that they believed their Internet use was being monitored only a very small percentage took actions to mitigate it (Sidhu, 2007). Some behavior change was observed, but not at a significant level. What explains this seemingly contradictory result? Could it be attributed to the surveillance source that was monitoring the community? Could it be due to a six-year 'acceptance' period following 9/11? Is there a relationship between short term perception and long term behavioral changes linked to knowledge of surveillance?

A study by Oulasvirta suggested that humans will adapt to long-term surveillance whether they want to or not. In 2012, 10 households participated in a 6 month longitudinal observation focused on analyzing the perceptions and behaviors of

individuals affirmatively opposed to monitoring (Oulasvirta, 2012). The study consisted of invasive in-home camera monitoring of the households and was based on a theory of Social Identity. That result suggested that an individual's level of surveillance tolerance depends on the surveillance source – in favor of a shared identity (Oulasvirta, 2012). For example, people may be likely to share information (even very sensitive information), about their personal life on Facebook or Twitter because they have a shared identity with those 'friends' in the social community they are connected to. They may be far less likely to voluntarily share that same information with people outside that pre-selected friend community.

The Oulasvirta study demonstrated that the anxiety levels of the participants decreased with time even though the surveillance level and invasive camera monitoring did not. The only departures from the result occurred when participants had to explain the cameras and monitoring equipment to household visitors or guests not aware of the study. This was attributed to the dissonance created in the minds of the study participants when visitors were not accepting or not understanding of the experiment (Oulasvirta, 2012). This again appears to confirm that community social acceptance plays a very important role in surveillance tolerance levels.

While many of the characteristics of individual privacy perception and personal-space expectation contain amorphous and flexible components, an individual's DNA is arguably the most intimate and unchanging. Presumably, intrusions into this sacred domain would be the last to be relinquished through population acceptance. In June 2013

the U.S. Supreme Court decided a case, Maryland v. King, 569 U.S. 435, 133 S. Ct. 1958, 186 L.Ed.2d 1 (2013). The court held that the defendant's cheek swab was a minor (and brief), intrusion on privacy and that the warrantless collection of saliva DNA was reasonable under the Fourth Amendment. The majority equated obtaining a suspect's DNA with other standard tasks of the post-arrest pre-conviction 'booking' procedure like photographing or fingerprinting a suspect.

Conversely, the case of drawing blood from a suspect (specifically following a DWI), is quite the opposite. In McNeely the court determined that when an officer can reasonably obtain a warrant for blood draw they must do so, in keeping with the 4th amendment protections of an individuals' right to be free from unreasonable searches (Missouri v. McNeely, 2014). It should be noted that live blood draws for the purpose of law enforcement are held in different regard than the retrieval of dried blood from under a suspect's fingertips. The Supreme Court of the United States earlier held in Cupp v. Murphy that dried blood was essentially evanescent evidence and that a suspect could begin to remove it from his hands before police had a chance to obtain a warrant to preserve it (Cupp v. Murphy, 1973). The McNeely court found a blood draw to be an unreasonable search because there were no legitimate circumstances present that would constitute an exception to the requirement for a warrant, unlike Schmerber where there was a legitimate exception (Schmerber v. California, 1966).

Data Privacy

The privacy of an individual's blood or DNA has been addressed by the courts for several decades. However, the legal system has only recently begun to address the complexity of issues involved in defining the extent of privacy with respect to one's personal digital data. This may be due in large part to the relatively recent developments in technology and a lagging court response to emerging technological issues combined with the absence of traditional caselaw. Although courts may grapple with the application of new developments in technology every day, issues specific to privacy are particularly difficult to navigate due to the required balancing of personal interest in privacy with the State's interest in security.

The government's ability to utilize personal data inferentially poses additional unique issues; most notably with error. An example from everyday life is easily imagined. An individual's grocery shopping habits are often preserved in digital form through the ubiquitous use of membership and loyalty cards. These digital data records may demonstrate purchases of large quantities of fatty foods every week.

Inferential analysis of the data could suggest that the purchaser is at a higher risk of health issues (high cholesterol, high blood pressure, or diabetes), and therefore could be subject to higher health insurance premiums; or at least continuous more invasive long term monitoring. What the individualized data points do not demonstrate is that while the shopper is buying the fatty foods the food is actually being fed to highly specialized sled dogs that require a high fat diet. This simple example demonstrates that a known

interrelationship among data points is required to avoid error and make accurate assessments. Merely having access to data is far more complex than it may initially appear and could result in very unfavorable consequences by government actors.

It is this kind of potential for error that can occur when law enforcement seeks to access an individual's cell phone data. As the Riley v. California (2014) court stated: "[c]ellphones have become important tools in facilitating coordination and communication among members of criminal enterprises that can provide valuable incriminating information about dangerous criminal – [p]rivacy comes at a cost". The Riley court upheld (at least in part), individual privacy rights when it comes to data stored on a cell phone. The court indicated that while a search of the physical aspects of a cellphone are immune from the warrant requirement; the information stored in a cell phone generally does require a warrant to access.

Law enforcement may not without a warrant search the data on a cell phone seized from an arrestee (excluding longstanding exceptions to warrantless searches under the 4th amendment like exigent circumstances). Supporting this rule a warrant can often be obtained digitally within minutes of law enforcement's request using real-time interconnected technologies. Data on a cell phone can easily be preserved indefinitely by simply shutting the phone off or removing its battery. The exigent circumstances exception may be used to negate the rule where circumstances reasonably require it. This relatively new 'cellphone rule' contrasts the usual probable cause searches that have been found to be reasonable when incident to a lawful arrest (Chimel v. California, 1969).

Digital data in its hard form (on the computer or hardware storage device), can be also be searched by the government under several warrantless conditions including the usual plain view, consent, and exigent circumstance exceptions. Border crossings and the border crossing exception (see 19 C.F.R. 162.6; authorizing warrantless searches of electronic devices at the border), offer yet another loophole in the requirement for a warrant to obtain a person's electronic data; this with potential 'soft data' implications.

The border exception began with the diminishment of an individual's expectation of privacy in an automobile. Courts have consistently held that drivers may be stopped at border crossings into the U.S. and their vehicle contents searched without a warrant or probable cause (Terry v. Ohio, 1968). Border searches may be made in the absence of any individualized suspicion at border checkpoints within reasonably geographical boundaries (United States v. Martinez-Fuerte, 1976), (Carroll v. United States, 1925). It is now well established that border authorities may search computers and digital storage devices without the usual need for a warrant or even probably cause; this is a blanket exception that includes all international airports.

Access to and utilization of an individual's personal digital data regardless of its mechanism of acquisition can lead to substantial inferential errors. While access to multiple points of data can serve to mitigate this compartmentalization issue, aggregating data points can create different but equally important privacy issues.

Public Privacy

The courts have consistently upheld the notion that relatively minor augmentation of standard policing does not change the nature of the acquired information which itself may or may not be protected by privacy provisions. One persuasive line of cases in support of personal privacy derives from the court's mosaic theory.

The mosaic reasoning was exercised by the United States Supreme Court in U.S. v. Jones, (2012). The that while individuals relinquish their expectation of privacy by disclosing information publicly (under the Third-Party Doctrine and Public Disclosure Doctrines), that information cannot be used 'in the aggregate' by law enforcement because it has the potential to disclose far more personal information than the target would otherwise reasonably believe (Rosenzweig, 2017).

The theory was specifically applicable in a case where a law enforcement target's car was tracked over the course of several months. While the travel route of the car was public and therefore immune from 4th amendment protection, the travel routes of the car over the course of multiple months was not. It is not reasonable that the travel routes of a person over such a long course of time would be considered available to the public unless the person was being targeted (U.S. v. Jones, 2012). The 4th amendment argument regarding Mosaic theory may also be seen in the 2018 case Carpenter v. United States, (2018). The court indicated that individuals have an expectation of privacy in the government tracking their movements over a period of time. In that case Carpenter argued that cell phone signal data required a warrant and not merely a court order to

access. The majority court based its reasoning on a reasonable expectation of privacy, while a dissenting opinion believed the 4th amendment argument was better supported by a protection of personal property or location data (Carpenter v. U.S., 2018).

In either instance, an aggregate of information could tell law enforcement much more about a target than a public location alone, developing into evidence of personal, 'intimate' actions or associations that could be protected by the 4th amendment. One of the notable problems for the mosaic theory is the indefinable nature from which the idea derives. That is, what is a reasonable amount of surveillance or how much surveillance is required before it jumps the hurdle of improper aggregation. In Carpenter, it was argued that 24 hours was the line that should not be crossed (Carpenter v. United States, 2018), but the question was left undefined may allow courts to make individual assessments and case outcomes become unpredictable.

The government has utilized Mosaic theory referencing national security concerns in defense of non-transparency and the refusal to release otherwise non-sensitive information (Pozen, 2005). The label of Mosaic as applied by the Court and government was later developed into a working theory by Pozen and is now widely accepted and used to describe a variety of situations where aggregated data may be formed into something greater than the individual data (Pozen, 2005).

One question arising from this scenario (in the context of digital data), is directly related to application of the Third-Party Rule. During normal daily activities data is knowingly relinquished from computers to third-party traffic handling systems, mass data

storage units, and Internet Service Providers (ISPs). This is the case for all Internet users including those who utilize email, social networking, or even so-called private websites.

Like short car trips, limited social network data may reveal only a small amount of public information; but large amounts of data (like car trips added up over the course of several months), can reveal very private or intimate information about an individual such that an entire character profile may be developed. Theories of aggregation of mass surveillance data like Mosaic leave open questions regarding levels of intimacy, relationship characteristics, and how what levels of privacy protection they should be afforded in email, Internet searches, or social media connections.

The potential issues associated with third party aggregation of surveillance data are easily understood. Suppose Mary, an individual on the phone with her friend Bob (who is on holiday in a country with limited Internet access), uses a search engine to look up information on a particularly unpleasant sexually transmitted disease. This is done so that relevant medical information could be relayed to Bob who is working abroad and does not have adequate Internet access to do the research himself. Mary's research (captured and stored by the search engine), may later be combined with a digital receipt for antibiotics (purchased by her daughter at the local pharmacy using her mom's discount card), may lead an analyst to the misguided conclusion that Mary has a sexually transmitted disease. In fact, she did not. Although multiple data points and references were used in the assessment, the inference was not aligned in context and would not yield an accurate assessment because the data were not in context.

These examples begin to shed light on why defining privacy limitations and protections is so important. Many law-abiding citizens may be tempted to advocate for a version of privacy best described as ‘when one has nothing to hide, one requires only a minimum level of privacy’. If privacy is required at all it can exist where it is not requiring complete segmentation from the government.

However, the more informed scholar may see that privacy is not necessarily a veil behind which evil must per se be taking place. Rather, it is better described as a protective barrier that exists between an individual and their government. It is necessary to prevent tyranny, mistake, poor decision-making or policy implementation based on inaccurate or incomplete data obtained from invaded portions of one’s life (Solove, 2018).

Surveillance

Historically, no discussion of surveillance and privacy would be complete without discussion of Bentham’s theoretical Panopticon (Semple, 1993). The Panopticon may be described as an architectural design that envisioned a penal building designed to facilitate persistent monitoring of inmates. It utilized a tall central structure surrounded by multiple levels of pie-shaped circular cells, each with a window at their outermost side. The window would illuminate the cells with outside light but the center viewing structure would remain dark. The monitoring agent would be able to view all the inmates, but the inmates would not be able to see the monitor.

The effect produced inmates who would not know when they were being watched but that they could be watched at any or all times. In theory, the result of this structure may be a (prison) population that will alter their behavior always in conformance with prison regulations to avoid punishment because there is no way for an inmate to predict when they are being monitored. The assumptions supporting panopticon monitoring may parallel the unseen mass surveillance programs used by the government. The government could watch the population but the population is unable to see it watching.

I was unable to identify research analyzing the impact of one way mass surveillance programs on society in the context of privacy. This may have been due in part to the relatively recent introduction of social media as a tool of mass surveillance for large populations or it may be attributed to the relative lack of conscious awareness of surveillance programs by the public prior to 2013. My research offered some insight into these programs and the associated public policies impacts they may have on society.

Personal privacy may mean the protection of individual data or metadata so that they do not become susceptible to abuse, misuse, or contextual misunderstanding. One primary area of privacy concern that my research identified was the proliferation of government surveillance powers as counterpoise to an individuals' right to be let alone and be free from excessive government interference (Warren & Brandeis, 1890). However, the ability of the government to monitor and track elements of its population is central to civil administration and governance. Monahan commented that an

understanding of surveillance is a required function to, [order] society through the regulation of individual or group behavior (Jing, 2016).

Government surveillance of citizens is to some degree not defined only by the monitoring of criminal activity or preventing nefarious activities (although one would be hard pressed to argue that some level of surveillance is required to prevent complex criminal enterprises from overtaking society). Nor is government surveillance necessarily as ominous or Orwellian as some have depicted it (see Orwell, 1949). Governments have a legitimate interest in even the most democratic of constructs, in monitoring their citizens for public health disease outbreaks, social order disruptions, infrastructure needs, education compliance, and many other nontotalitarian oversight requirements. Society has an interest in allowing legitimate government surveillance for the same reasons.

Society to a large degree may coexist within an intrusive government surveillance environment due in part to a phenomenon called acceptance. Bauman's 2014 study explained the phenomenon of acceptance in two ways (Bauman, 2014). The 2013 discovery of the government's bulk data collection activities may have surprised the public. However, with the passage of time a phenomenon called 'familiarization' occurs. When individuals are exposed to a shocking event, they will over time, become less shocked and increasingly desensitized to it. The pervasive and ubiquitous nature of surveillance has over time desensitized U.S. society (Bauman, 2014).

Second, individuals in a Web 2.0+ environment of interactivity experience daily social surveillance or peer to peer lateral surveillance between community members. The

idea of monitoring friends and family throughout the day through Facebook or a Twitter feed may be framed as fun and engaging (Bauman et al., 2014). Over time the idea of surveillance as a fun activity overrides the discussion and detracts from the more formal characteristics of surveillance. People may come to expect to be monitored by their social communities and even craft their personal appearance accordingly.

Mass Monitoring Programs

Following the June 2013 release of top-secret documents by former NSA contractor and whistle blower Edward Snowden the United States public became aware that their government was spying on them and acquiring vast quantities of personal data through covert monitoring programs. These programs utilized third-party data collection techniques to obtain private information on virtually everyone in the United States. The programs were based on the use of secret agreements between government spy agencies and private companies, corporate proxies, search engines, as well as Web 2.0 social media platforms like Twitter, Facebook, and Skype (Electronic Frontier Foundation, 2020).

Much of the literature commenting on the event and that comments on these programs include references to the, “privacy – security” spectrum; aka the tension inherent between civil liberties, individual security, and the scope of power required by the government to achieve a specific level of safety. The privacy – security spectrum may be described as a spread or range of amplitudes that define quantities of both ideas. There is no reasonable way to approach privacy as a binary issue wherein there is not a middle

ground. The spectrum represents on one side the private individual and on the opposing side the governmental interest in national security that is supposed to require monitoring and oversight.

The field occupying the spread of space between the two end-points represents either an increase or decrease of civil protections afforded to individuals. It is important to note that the spectrum does not represent an actual level of safety afforded the individual; that relationship would be illustrated by a "privacy – safety" spectrum and that field is different. That would measure the subjective safety of an individual against the increasing or decreasing civil protections afforded that individual. Neither of these spectrums demonstrates a quantifiable objective measure of security, but simply illuminates a relative level of safety when compared against a loss of civil liberties.

To many outside the counterterrorism contingent a policy issue post-September 11, 2001 may be striking a balance between security and privacy. Previous studies suggest a correlation between perceived increases in (personal) threats and the willingness of individuals to relinquish privacy or civil liberties (Davis & Silver, 2004). Whether there is a relationship between the variables or where they intercept(s) on a graphed-curve of security, safety, and privacy may require additional analysis and may not be a foregone assumption. Increased surveillance (decreased privacy), and a safer society may not be a known, definable, or accepted relationship. If such a relationship does exist it may not be assumed that the relationship is necessarily either inverse or proportional.

Perhaps the most prolific examples commenting on the privacy security spectrum in existing literature are related to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, (USA PATRIOT ACT, 2001), and its progeny. Following the terrorist attacks on the United State occurring on 9/11/2001, the Act was officially enacted to protect the American public from further terrorist activities (USA PATRIOT ACT, 2001). However, it soon became clear to outside observers that the legislation was operationally designed to circumvent established legal protections by allowing domestic spying of citizens using police powers not intended by the drafters of the United States Constitution by eliminating checks and balances previously reserved for the judicial branch (Electronic Frontier Foundation, 2020).

The PATRIOT ACT was pass in record time and was a powerful expansion of prior existing legislation allowing the National Security Agency (NSA), to intercept suspect communication but also allowed the agency to listen in on unrelated parties connected with that communication (American Civil Liberties Union, 2020). Among several problematic sections of the Act was Section 203. The section provided law enforcement with among other things, broad abilities to intercept massive amounts of electronic communication and data greatly enhancing the government's ability to share information both inter-agency and extra-agency through the expanded use of intelligence Fusion Centers.

Several follow-up or related legislative actions broadened the Act's powers causing public interest and civil rights advocacy groups to voice concern regarding the expansive nature of the new laws. These included Total Information Awareness Program (TIA), the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), expansion of pre-existing ECPA and FISA, the National Security Letter (NSL) laws, and others (NSL, n.d.). In its wake, Washington created dozens of new intelligence groups, agencies and sub-agencies including the Office of the Director of National Intelligence (ODNI, n.d.).

As time passed in the post 9/11 environment, enhanced 'security' at the expense of civil liberties progressed beyond electronic intercepts and began to include invasive body scans at airports and other physical intrusions. It wasn't until Edward Snowden leaked classified information that the U.S. public became aware of the actual nature and extent of the domestic surveillance that the government was undertaking. Snowden disclosed information on the government's mass population data collection programs (not unlike the less technically sophisticated COINTELPRO of the 1970s), and data mining programs Xkeyscore, Quantuminsert, Bullrun, Dishfire, and one codenamed PRISM. The PRISM program allowed government agents to retain and sort vast amounts of citizen-data by contracting with telecommunications and Internet Service Providers.

Snowden also disclosed information about the top-secret government program codenamed UPSTREAM. This program along with Quantuminsert, tapped into transatlantic sub-sea fiber cables to intercept virtually all incoming and outgoing Internet

communications. The program was authorized under Section 702 of the 2008 Foreign Intelligence Surveillance Act (FISA); all without a warrant or informing individuals they were being monitored.

In 2014 a quantitative study looked at whether the Snowden event triggered changes in Internet use. Using Internet search data derived from hundreds of common keywords compiled from the Google search engine the study examined whether people modified their Internet search keyword behavior immediately following Edward Snowden's 2013 release of top-secret information regarding domestic government surveillance. The study design utilized keyword assignments to one of three (3) categories ranging from 'less private' to 'more private' or 'sensitive'. The keywords ranged from personal disease inquiries to questions about the CIA or other overtly sensitive government issues (Marthews & Tucker, 2017).

The study found that search word usage following the 2013 Snowden event (assigned to the high-sensitivity category), fell by ten (10) percent (Marthews et al., 2017). This means that for every ten (10) searches done prior to the Snowden event only nine (9) were done after it. While not a large change per se the study found that the change was statistically significant. The study authors suggested that the result had the potential to influence international commerce as people may stop using U.S. search engines do to fear of loss of privacy (Marthews, et al., 2017).

This paper reviewed information obtained from legal cases, academic journals, research and dissertation database papers, peer reviewed social science articles, and

public information sources published in years 2011 through 2016. A few resources outside the traditional five-year publication window will also be included to present relevant information in an accurate historical context.

The Walden University library research databases ProQuest and EBSCOhost will be used to access many of these sources. Electronic search terms entered in to those databases include privacy, privacy defined, elite theory, classical elite theory, 9/11, post-9/11, USA PATRIOT ACT, Snowden, privacy perceptions, government monitoring, Total Information Awareness (TIA), The Foreign Intelligence Surveillance Act (FISA), and big brother. While additional sources are analyzed to ensure a broad understanding of the subject matter, many will be intentionally excluded because they are deemed to be redundant, outside the scope of the study, or non-conforming to the inclusion protocol. Ultimately, the literature review will provide the reader with a solid foundation from which to understand the research material and overarching theory presented in the study.

Summary

My research suggested that many Americans consider privacy and security to be an important aspect of their personal life. Those views may translate into emotional and sometimes negative reactions when new social policy affecting their privacy is proposed. However, a review of literature and an analysis of the emergent themes discussing these phenomena revealed that many individuals may not understand what privacy is or how privacy doctrines apply in everyday life.

My review of available literature did not find information addressing the potential application of elite theory to national security and privacy policy. This highlighted an area of study that may not be readily available to policy creators who are trying to avoid unwanted collateral policy outcomes like social disruption or noncompliance.

The elite theory social construct may prove to be significant to the understanding of how society will respond to a given change in public policy. By using secondary data and thematic analysis techniques my study inquired whether elite theory could be utilized by policy professionals to suggest social outcomes prior to policy implementation. The implications for policy professional are potentially far reaching and may apply to social change across a broad spectrum of individuals. Policy modeling tools may be used to shape policy without the requirement of social discourse and could potentially be used to bypass the normative democratic structure of decision making.

This study evaluated the different types of privacy, described how privacy is defined in America, and analyzed the relationships required to maintain an effective partition of privacy between the state and the population. I then identified the threshold associated with overcoming that partition and identified the point at which individuals will shape their behavior around changes in privacy perceptions.

This research may have applicability to national security policy involving privacy, population monitoring, or data gathering. It may also extend into collateral areas of social policy like the use of advanced interrogation techniques or offsite detention facilities. The result of the research may be relevant to the drafting and implementation of nearly all

future domestic security policies and could offer policy professionals more freedom as they endeavor to balance the needs of the government against the responsibilities of an inclusive democracy.

Chapter 3: Methodology

In this chapter I discussed the methodological approach used to address a missing area of literature pertaining to the use of elite theory in security and privacy policy analysis and addressed whether elite theory may be used as an analytical component when drafting national security policy. The research examined the potential relationship between the United States government's domestic eavesdropping programs and the public interest of protecting individual privacy.

The purpose of the study was to test the hypothesis that elite theory can be applied in an assessment of how a population will behave in response to privacy intrusions by the government. The theory suggests that a nonelite population is generally apathetic to security policy and is largely devoid of sustained investment in the protection of individual privacy rights (Pareto, 1935). This research was undertaken to assist national level policy makers, analysts, and academics in their understanding of elite theory as a tool of modern policy development.

To be effective, the post-9/11 national security posture of the United States required increasing quantities of highly detailed intelligence obtained at the cost of individual privacy (American Civil Liberties Union, 2020). As such, it may be reasoned that national security policy accounted for the social impact created from the acquisition of that intelligence. If elite theory can suggest behavior than policy creators may be free to disregard the voices of the non-elite, focusing instead on aggressive intelligence gathering methods.

This chapter addressed the primary research question, methodology rationale, theoretical approach, threats to validity, ethical considerations, and overall study design. I discussed secondary data analysis of the relationship between privacy (in a pre-Snowden environment), and variations present in a post-Snowden enhanced monitoring environment. The acquisition and use of secondary data as well as statistical research tools utilized in the analysis were also explained. Finally, the possible dissemination and future use of the resultant research was addressed.

Research Questions and Design

This study was designed to examine the relationship between domestic government surveillance programs (an independent variable) and changes in individual privacy behavior (a dependent variable). I investigated whether elite theory may be used as a tool to assist with policy decision making. My review other research studies established this nonexperimental correlational analysis using archival data. The study is informed by thematic analysis of carefully selected topical sources. The research question and testable hypothesis are as follows:

RQ1: Using prior studies and secondary data; what is the nature of the relationship among the independent variable (domestic government spying), and the dependent variable (individual privacy behavior)?

$H_0$1: There is a relationship between the independent variable (domestic government spying), and the dependent variable (individual privacy behavior). Domestic government surveillance will affect individual behavior.

H_a1: There is no relationship between the independent variable (domestic government spying), and the dependent variable (individual privacy behavior). Domestic government surveillance will not affect individual behavior in a significant manner.

Using a thematic analysis of existing research offers a unique perspective of aggregated data not available to the original individual researcher (Braun & Clark, 2008). Thematic analysis offers broad access to a wide variety of data that would not otherwise be obtainable considering financial and logistical constraints, while at the same time offering a more concise evaluation of the research question (Braun & Clark, 2008). This study was undertaken to analyze prior study outcomes and identify previously undiscovered relationships. The thematic analysis of multiple existing study results is used to inform my analysis of secondary data from pre-existing archived data sets. The data will provide increased assessment capabilities and offer significant advantages over single-slice data acquisition techniques.

Methodology

While both the thematic and secondary data analysis techniques selected for this research offer advantages there are several challenges that were addressed. First, because there was a degree of freedom to choose data that was used in the secondary study, I was aware of the potential of introducing selection bias. I took care in not purposefully selecting data that supported the hypothesis. Second, I was aware that the data obtained from secondary sources could have come prepackaged with interpretations of that data

and those could have been transferred to my study so I was careful to avoid that. Third, the internal validity of the secondary data relied on an outside source (Pew's research methods and safeguards), and not one specifically designed by me. I independently analyzed and verified that their research design met the same criteria I would have used to acquire the secondary data as my own primary data and was satisfied that it did. Even with these challenges (common to both the secondary data analysis and thematic analysis methods), the analysis tools I used provided a solid methodology for discovering new patterns and relationships. Each of the challenges were mitigated with solid research technique combined with careful attention to detail and the awareness of and elimination of potential bias.

A comprehensive synthesis of the secondary data with results obtained from the thematic analysis provided a robust understanding of population sentiment relating to domestic government surveillance and individual privacy. The research offers insight into the viability of elite theory as a predictive tool in the context of national security policy creation.

Modern social science offers two primary methodological research design approaches: quantitative and qualitative. Both offer advantages and disadvantages depending on the type of data used, data characteristics, and the research outcome that is preferred. Both methods are useful to explain phenomena but approach the explanation from different perspectives.

Qualitative analysis uses an inductive methodology to explain an observable behavior or condition through a subjective lens (Suter, 2012). Data acquisition is largely exploratory and may be obtained several different ways including through the descriptive life experiences of subjects (Suter, 2012). The goal of qualitative research design is to record and explain lived experiences (from which inferences may later be drawn about larger populations), and to explore and understand how phenomena unfold (Suter, 2012). Data is not number based and can include narratives, pictures, objects, or observations. This qualitative approach offers significant flexibility allowing it to change as the study progresses (Suter, 2012). A qualitative design is best suited for use in the investigatory phase of understanding new a phenomenon or for understanding the deeper social meaning behind an event (Suter, 2012).

Quantitative analysis is an objective, structured methodology that allows a researcher to numerically analyze statistically significant attributes obtained from a representative sample of the population (Creswell, 2003). The deductive design of a quantitative methodology affords high external validity, is objective, deductive, and relies on an experiment-based framework to validate a theory or confirm a hypothesis (Creswell, 2003). Quantitative analysis uses structured data to examine any correlational relationship between two variables (Mertler, 2018). Because results are replicable and there is an inherent cause and effect involved in this type of analysis, the result may often be used to support predictions (Mertler, 2018).

One characteristic of a quantitative study is the high level of external validity (Creswell, 2003). This refers to the ability of the study to be later generalized to a larger population. In quantitative research, external validity is high because the design inherently eliminates outside variables and external factors (Flick, 2017). For example, in my study the data are preexisting and will remain accessible to other researchers who may replicate the experiment in the future while still obtaining the same result.

A quantitative approach was best for this study because it solidly aligns with both the research question and hypothesis test. The structured data can be easily understood through numerical analysis and the results applied to a large population. Study data was analyzed using the Statistical Package for the Social Sciences (SPSS) software Version 23, and the analysis will be informed by the results of the metadata.

Data Selection

Data was obtained from applicable English-only key word and phrase searches included in years 2011 through 2016. The searches were conducted using the Walden University Dissertation Database, Walden University online library, ProQuest research databases, Pew research databases, and Google Scholar. Search inquiries offered several thousand results; a small percentage of which are in alignment with the study. These were meticulously synthesized and compared against pre-established inclusion criteria. The selected scholarly works strongly aligned with the study goals. This reflects the effort to include content-appropriate articles in the analysis.

Following an evaluation of potential nationwide data sources, the data sets in this study derived from the Pew Research databases. Pew is a nonprofit, nonpartisan and non-advocacy facts tank that values objectivity, accuracy, and rigor; and is committed to impartial research and data (Pew, 2020). The foundation conducts public opinion polling, demographic research, content analysis and other data-driven social science research. Pew's mission is to inform the public about the issues, attitudes and trends shaping America and the world (Pew, 2020). Table 1 shows the databases and information that were selected from ninety possible sets that are available from Pew:

Table 1

Data Analysis—PEW Datasets

Date Range		Database	*N*
2006	12/01 – 12/30	Digital Footprints	3379
2013	5-Jun	Snowden Leak	x
2013	07/01 – 07/30	Anonymity	1002
2013	08/07 – 09/16	Connectivity	1801
2014	01/10 – 01/27	Privacy Panel (1)	607
2014	08/05 – 09/02	Privacy Panel (2)	498
2014-2015	11/26 – 01/03	Privacy Panel (3)	475
2015	01/27 – 02/16	Privacy Panel (4)	461

Pew's Social and Demographic database as well as its Internet, Science, and Technology database content provided a high level of applicability to my research question. Using more than one data set may increase the number of available data points within a specified frame of time that contrasts with the single-slice data capture technique. While both single-slice and multiset options have merit depending on the specific application that a researcher desires; the latter may offer more robust capture opportunities for this study. It also may account for sentiment change over time, mitigate potential bias created from news of current events, and provide a larger statistical pool from which to draw inferences and it is for these reasons that I selected this method for the study.

Each data set was individually analyzed using key word, key phrase, and subject matter matching, ensuring that the content parallels the framework of the study. Content matches included technological connectivity, surveillance issues, social media use, mainstream media awareness, personal anonymity, communication behavior, social interactives, and community involvement.

While the diversity of the Pew research data provided a solid survey of national privacy perceptions, there were limitations. Sampling errors (the difference between the value derived from the population sample and the actual value associated with the entire population), can occur in any of the data sets (Dodge, 2005). Similarly, survey bias can occur when there is a difference between the surveyed population (sample), and the whole population (Stat Trek, 2020). Subpopulations within the sample can be overlooked,

excluded, or their characteristics not properly accounted for (Stat Trek, 2020). For example, the inclusion of survey answers from a retired law enforcement officer may skew the data obtained; the officer is a member of a subpopulation exhibiting attributes or weight that may not have been properly accounted for (when compared with the population).

While the Pew research data in this study already existed, it was not immune from self-reporting limitations. Respondents may have unintentionally report false answers, exaggerated, or even lied. Additionally, the collection methods used required respondents to provide responses using a limited number of feedback options. These may not have adequately reflect more complex scenarios thus yielding responses of limited usefulness. Data for the study was originally obtained between the year 2013 and 2016. Data obtained before 2013 was generally be excluded from the study because of a limited need for information prior to the Snowden surveillance data dump.

Data Analysis

Analysis was accomplished by assigning government surveillance monitoring programs as an independent variable and an individual's privacy behavior as a dependent variable in the observational model. The model was designed to identify any relationship between the variables and to examine descriptive and thematic patterns if they existed.

Thematic Analysis

A thematic analysis, the examination and synthesis of aggregated information obtained from more than one previously completed study from which themes emerge, are

identified and extracted (Flick, 2017), was chosen to provide a more robust and accurate result than a single study analysis may have. I applied the thematic analysis inclusion criteria across multiple topical research papers to inform the correlational study of the Pew research data in this study.

The emergence of thematic inclusion criteria for the research identified in the literature review section of Chapter 2 included determinations of relevancy of the research inquiry, relevancy of the data, publication date, and peer review status. Studies were selected for inclusion in the analysis if they addressed the issue(s) of right to privacy, government monitoring, changes in privacy behavior, or individual privacy perceptions, and would contribute to an overall understanding of the research problem.

These suggested a strong relationship between an individual's perception of a terrorism threat and a level of acquiesces to the loss of specific civil liberties. They also suggested that both perceptual and behavioral alterations were observed in protective behavior after the Snowden information dump. The behavior data provided useful information but relied on self-reporting. Results may have been generated by sample populations that were potentially influenced by skewing factors like priming bias, suggestion bias, or the Hawthorne effect. This is not necessarily a reflection of deficient study methodology as some limitations are an inherent function of data collection surveys; nonetheless they may fail to provide an ideal tool for policy analysis.

This study was designed to mitigate the limitations associated with single-slice survey timing and survey bias by reporting outcome effect using qualitative descriptors.

The improvement relies on thematic analysis; a widely accepted method of social science inquiry that when implemented properly exhibits a high degree of confidence and error avoidance (Flick, 1998). It is a research tool that allows one to aggregate research results and compare results across multiple studies having similar but not identical characteristics (Braun & Clarke, 2008). A multiple study thematic analysis was selected because it may identify differences and similarities between research outcomes highlighting values not evident in any one single study.

Unlike the t or F statistical tests, this method does not rely upon sample size to describe significance. Rather, it utilizes a methodology to compare the meaningful aspects of data of different studies to determine significance. Thematic analysis is important not only for its ability to compare effects across multiple studies, but also for its ability to combine experimental results from studies with different population sizes (Braun & Clarke, 2012). Even relatively small studies can become more useful when their result is combined with and compared to results from larger studies. Synthesis increases the analytical usefulness of otherwise accurate and descriptive yet less impactful studies (Braun & Clarke, 2012).

Comparing the outcomes of different studies incorporating different population sizes or variable characteristics can present a challenge. While a Null Hypothesis Significance Test result may provide a way to classify a null hypothesis as either ‘likely’ or ‘unlikely’ to occur in the population based upon a defined confidence criterion it does little to increase knowledge about the magnitude or objective importance of the observed

effect. The issue is evident where there is a statistically significant but small effect size that has a high level of real-life importance, or a large effect size having a lower real-life importance. Effect size may be subjective and somewhat arbitrary unless the context from which it is being reported is understood. Effect size is derived from a study's sample size, variability, and outcome (Boslaugh, 2012). Instead of inquiring simply whether an observed result is a function of population or represents a significant effect, effect size analysis inquiries into the magnitude of an observed effect.

Standard significance testing methods indicate the likelihood that an observed result is due to population variances or sampling anomalies. The accuracy of a result subjected to Null Hypothesis Significance Testing is based upon probability inference and relies on population sample size. For example, a sample of five-million data points may yield a 'significant' result because when compared against the null (0) a fractionally small mean difference can appear statistically important; while the same mean difference in a one-hundred-point data sample would not be labeled as significant.

The method selected for this study incorporates an aggregation of statistical inferences to describe cross-study outcomes irrespective of individual statistical significance. It incorporates effect size as an objective standardized measure of the importance of an observed effect (Field, 2005), to compare the magnitude of variation in research outcomes in studies that may have used non-similar measurement scales or variables.

Secondary Data Analysis

Secondary data was analyzed to identify relationships between the variables changes in privacy behavior and domestic government surveillance programs. The analysis was designed to safeguard against the influence of bias, internal, and external variables, selected data sets were aggregated, and responses that are not applicable to the study or that are unable to be normalized were redacted.

Inclusion of archival data was accomplished by using a selection protocol designed to ensure homogeneous data across sets to mitigate potential selection bias. The protocol required that the data selected parallel the nature of this study's variables as closely as possible. The data was place and time appropriate and derived from the national population (individuals residing in the United States and who have access to media). The Pew research data selected for the study is content appropriate, topically consistent, single-sourced, secondary data providing a substantial volume of data points, variety of demographic, and continuity over years that would not otherwise be available in a primary study that is limited by financial and logistical constraints.

The Pew research data included 3,379 data points from year 2006 (prior to the Snowden leak occurring June 5, 2013), 2,803 data points from 2013, 1,580 data points from 2014 (noting a three day overlap into 2015), and 461 from 2015; totaling 8,223 available data points. The data offers valuable insight into individual privacy expectations through a multi-year window and suggesting how the United States population responded to the disclosure of government surveillance programs. The study merges the results of

the secondary data analysis with the information from the thematic analysis. This resulted in a synthesis of data patterns and inferential conclusions about the population response to domestic government surveillance.

While each the Pew data sets were wholly applicable to the question(s) addressed in the study there was a significant degree of variation in both the semantic structure and phraseology. This highlights the importance of the coding structure that was developed for the study.

Coding

The analysis required a degree of reliable data uniformity to operate properly. To achieve this the study relied on coding techniques to translate non-linear variables obtained from multiple datasets into a usable format that could be statistically analyzed. The outcome of each dataset was coded in accordance with the coding scheme described herein and a resultant quantitative effect was captured and reported. Coding the data obtained from the Pew research datasets was undertaken by assigning categorical values to each participant response.

Once the data were coded by the software it was used to generate an analytical result. This informed the study about relationships between mass monitoring and a population response to it. Multiple independent variable logistical regression outputs were correlated and examined to identify statistically significant associations. Logistical regression was chosen as a predictive analysis model for its ability to analyze independent variables and provide a statistical outcome using a categorical dependent

variable. The research was analyzed via the coded outcome of questions posed to participants regarding their thoughts and behavior while being surveilled or monitored by the government. The result informed the research as to whether intrusive surveillance programs influence individual behavior. Results are noted in Chapter 4 of the study.

Trustworthiness

Some studies require the use of an external committee evaluation or a pilot study to test the validity of the study instrument prior to actual implementation. However, because this study utilized secondary data and thematic analysis a pilot study was not required.

Both external and internal validity was paramount to ensuring a reliable study outcome. A lower level of validity may have affected the accuracy of the study's inferences or conclusions. The quantitative orientation of the study lends itself to a higher level of external validity beyond the existing study as it may support the work of a future researcher attempting a similar type of study in a different place and time.

This study was undertaken to understand the privacy behavior of a national population notwithstanding potentially significant changes in the security environment. The sample population was inferred from the national population and is not geographically or demographically restrictive (except the English language requirement). The study results reflected population sentiment and behavior regarding personal privacy over a period of years.

The data in the secondary data analysis was obtained from the Pew research data sets described above. Data points were obtained from a randomized test population using two combined probability sampling methods, random digit dialing (RDD), and address-based sampling (ABS) (Pew, 2020). Both the RDD and ABS methods may offer independent advantages and disadvantages. Utilizing both methods in combination with one another may provide increased sampling accuracy. RDD telephone surveys have historically been the gold standard of obtaining data using surveys (Yeager, et al., 2009).

However, some sample populations may present difficulties if they include individuals who do not use a landline phone, who implement call screening, or who present with a high degree of privacy. The ABS solution offers an economical, less intrusive sampling method that includes the ability to access non-landline households (Yeager, et al., 2009). Utilization of both methods in this study may help with mitigation of potentially missing or misleading data from a diverse sample population.

Internal validity describes the reliability between the dependent and independent variables (Bhandari, 2020). It underlines the statistical analysis methodology and assists the reader in understanding the nature of the measures of association (Bhandari, 2020). Standard internal validity threats like experimental mortality, instrumentation, and maturation were not applicable here because the data is archival and the analysis is a thematic analysis.

Internal validity was accomplished by implementing cross tabulation analysis using the independent variable to identify a correlation with the dependent variable. A

correlative relationship was identified where a change of behavior within the sample population (the dependent variable), corresponded with the public learning that their communications are being monitored by the government, (the independent variable). The statistical analysis was undertaken using SPSS software Version 23.

The reliability characteristic of a research study outcome provides another indicator of the study's robustness and worthiness of the result (BRM, 2019). Reliability refers to a study's level of dependability, consistency, and ability to be repeated in the future by other researchers. One measure of reliability is the test-retest method (BRM, 2019). As the name suggests, this method requires administration of the test instrument two or more times during different time frames and the outcomes of the tests can later be correlated to demonstrate the stability or reliability over time of the test (BRM, 2019). In this study many of the data points available from the Pew research datasets included responses to questions obtained during more than a single time frame. This is useful because it operates like a built-in reliability test ensuring that there is continuity of responses over time.

A second type of statistical reliability is called instrument reliability, a measure of the research study's instrument (or procedure), that will be used in the data gathering phase (Research Rundowns, 2020). Selection of a research instrument is dependent on the type of data, unit of analysis, and study design requirements. Evaluation of the instrument used to gather date for this study was not applicable because the data was acquired from secondary source datasets. However, this study could be susceptible to instrument

reliability errors where aggregated data processing is not undertaken correctly so reliability testing was used to confirm valid performance.

Ethical Considerations

This study had a minimum of ethical considerations. The study did not access protected information or confidential data sources. The University IRB application approval letter was submitted separately and research was not undertaken until permission was granted by the IRB. All data utilized in the study was publicly available and could be obtained from non-human sources with no associated identities attached. The data in both the thematic analysis and secondary data portions of the study had previously passed through the Pew research screening process that include double anonymous, confidentiality protections built in (Pew, 2020). All data and associated study information was securely stored in a password protected Microsoft cloud storage account that is only accessible by me, unless I grant authorization to another. The information will remain securely stored for a minimum of seven (7) years and will be destroyed at the end of the data holding period.

Summary

This research study utilized two different analytical techniques to explore the hypothesis that elite theory has a place in security policy creation and security policy analysis. The research examined the relationship between privacy sensitivity (as a proxy for understanding policy apathy), domestic government mass surveillance spying programs, and change in individual behavior. This chapter provided a review of the

research methodology, an explanation of the design approach, and a detailed overview of the information that was used in the study. A total of nearly 5,000 data points are analyzed for pattern and relationship significance resulting in a test of the hypotheses that follows in Chapter 4.

Chapter 4: Results of the Study

Introduction

The purpose of this research study was to examine the applicability of elite theory as a theoretical tool in social policy modeling and analysis and to investigate whether it may accurately anticipate behavior relating to social change. This chapter explains the result obtained from an analysis of open source data collected from a United States population surveyed on issues of privacy and government monitoring.

This study is useful because it provides a framework for analyzing the research question and assists with understanding the research hypothesis. The results of this study contribute to the depository of scholarly literature available to policy professionals who create and review new social policy.

The study was designed to test the hypothesis that elite theory may explain social behavior and may be used as a theoretical tool in policy creation and analysis. The literature review, study design, and research methodology were developed to contribute to existing research on issues of privacy, social policy, and individual action. A thematic analysis was used to identify and compare current trend-based patterns of individuals across America.

The research hypothesis suggested that elite theory could be useful in social change decision making. The hypothesis was tested by analyzing the relationship between individual privacy change and privacy safeguarding behavior during government mass surveillance. To explain the data and how it applies to the research inquiry this

chapter provides research results in table format, examines the thematic analysis, and explains the secondary data analysis. Chapter 5 will summarize the results and integrate them into the research inquiry.

Thematic Analysis

As mentioned previously, notions of privacy and security are flexible ideas that change over time across a society (Mulligan et al., 2016). It is most appropriate to inspect the concepts through a wide lens from different perspectives. Privacy, whether social or individual continues to occupy an important space in modern life (Mulligan et al., 2016). This is especially true as technological advancements erode existing social configurations of privacy and individuality while government officials attempt to address modern social issues (Mulligan et al., 2016).

It is paramount that stakeholders have tools to assist with the process of adapting new policy to existing sociolegal frameworks. Sociolegal issues around privacy and security appear in some of America's earliest legal cases and continue through present day legislation (Green, A. 2020). For this reason, a thematic analysis of relevant legal and academic studies was chosen to analyze the variables of government, privacy, and civil liberties. To best understand these complex ideas in the context of this paper, 11 studies were analyzed alongside 39 data sets using selective coding techniques.

Significance testing (hypothesis testing) conventionally results in an answer of zero or not zero, meaning that there is a statistically not zero significance in the result (Lund Research, 2018). The result or effect is not zero and therefore the hypothesis null

can be rejected (Lund Research, 2018). The *p* value indicates that the results observed are not statistically by chance (Lund Research, 2018). For example, if an exercise program results in muscle gain than the program is significant to gain muscle, though participants may only have gained a 1% or less increase in lean mass. However, this method of testing does not describe how much muscle was gained or whether those gains are enough to be physically noticed. It only informs that there was in fact some correlation between the exercise program and a gain in muscle. If one wishes to know whether the exercise program will yield a resultant change large enough to be notice in the mirror, this test outcome is not sufficient because it neglects to report on objective program effectiveness or the magnitude of muscle mass change.

In contrast, a thematic analysis uses an objective formula applied to emergent themes (Mulligan et al., 2016). This method is more robust than that of single-outcome method and offers a result based on multiple study outcomes (Mulligan et al., 2016). The intent is to capture the result of more than one study and use them to determine whether the outcomes are significant (Mulligan et al., 2016). This increases the test power of the study and improves effect estimates. It also provides for the reporting of unstandardized effect sizes and synthesizes the result of multiple studies providing a single conclusory summary (Mulligan et al., 2016).

In this study, I examined the relationship between awareness of domestic government surveillance and changes in individual behavior. This inquiry is addressed by a thematic analysis of several different studies to understand how individuals view

privacy and respond to privacy changes. The information in other research studies and the data provided by the Pew research datasets benefited from a thematic analysis because it described multiple case participants over a varied period with changed sample sizes.

Data Collection

Table 2 presents existing research and sources used in the thematic analysis.

Table 2

Sources for Thematic Analysis

Name of Source	Author	Date
An economic theory of democracy	Downs	2003
Democracy and Political Ignorance: Why Smaller Government Is Smarter, Second Edition.	Somin	2016
Who rules America? Power, politics, & social change	Domhoff	2010
Your Data Shadow: An exploratory study of the short-term effect of viewing news and information content on surveillance technologies on perceptions of privacy.	Farid	2015
Americans' Attitudes About Privacy, Security and Surveillance.	Madden & Rainie	2015
Government Surveillance and Internet Search Behavior.	Marthews & Tucker	2017
Long-term effects of ubiquitous surveillance in the home.	Oulasvirta	2012
Social pressure, surveillance and community size: Evidence from field experiments on voter turnout.	Panagopoulos	2011
The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans.	Sidhu	2007
After Snowden: Rethinking the Impact of Surveillance. International Political Sociology.	Bauman	2014
Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America.	Davis & Silver	2004
The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech.	Kaminski, Margot, Witnov, & Shane	2015

Each of these studies was analyzed using thematic analysis to summarize relevant qualitative data in a quantitative manner suitable to inform the Pew research data discussed below. Step 1 was to review, analyze, and code the texts and step two was to sort the coded data into units or related code groups. This procedure was undertaken to allow for the initial emergence of identifiable, describable meanings and relationships across the research that could be documented and applied to the secondary data sets. While the emergence of thematic data in this study does not explain causality or data meaning, it may inform the review of the secondary quantitative data analysis and allow for a better understanding of statistical results. The process of coding is explained below under Themes and Coding.

Survey Data

This study used secondary data from public source surveys obtained from the Pew research website. Survey materials were in the form of electronic data in question-answer format. Each participant responded to the survey and provided an answer to the survey question using a Web-based survey form. The survey inquiries, which are describe below and attached in the appendices, include relevant topics like privacy, security, government, and technology. The data obtained was secured in a password protected cloud vault where it will remain for a period of at least 7 years. Access will be limited to me and my authorized representative if appropriate.

There is no participant identification or personal information associated with the data or attached to the research results. While anonymity may be a benefit to the safety of the research participants ensuring their identities are protected it did limit my ability to attest to the accuracy of the survey question responses. I relied on the representations of the participants that they used their best information and reasoned logic to answer each survey question accurately and honestly. Any data anomalies or missing data was taken into account for purposes of analysis and after careful review of the survey questions, answers, and methods of reporting, I am satisfied that the data obtained and provided in this research paper is accurate and meets acceptability requirements for dissertation level scholarship.

The first data set is from the Pew Research Center's Internet Project/GFK Privacy Panel Survey #1. The survey was conducted online between January 10, 2014 and January 27, 2014 and applied to a sample of *N*=607 English speaking adults age 18 and over who agreed to be part of a group taking online surveys of *current issues, some of which relate to technology*. There were a nationally representative sample of 1,537 individuals invited to join the panel with 60.8% (935) responding and 64.8% (607) agreeing to complete the first of the surveys. The survey data are representative of the national population and are based on a random sample of all 50 states and the District of Columbia and is adjusted for age, family size, gender, education, and race population parameters from the U.S. Census Bureau. The sampling methodology used yields results within three points of the actual population values.

The panel members were obtained through random digit dialing (RDD) and address-based sampling (ABS) methodologies provided by Marketing Systems Group. The selected group includes households with cellphone, landline phones, and no phones. For those without access to Internet, devices and service were provided to them. The 607 member sample accounts for current patterns of Internet access, gender, age, education, race, income, home ownership, and geography to parameters from the Census Bureau's Current Population Survey (CPS), as adjusted for bias due to nonresponse or noncoverage. As a result, the first survey has a sampling error of plus or minus 4.6 percentage points at a 95% level of confidence. The second and third survey have a sampling error of plus or minus 5.6 percentage points. The fourth survey has a sampling error of plus or minus 5.8 percentage points.

The second survey data is from the Pew Research Center's Internet Project/GFK Privacy Panel Survey #2. The survey was conducted online between August 5, 2014 and September 2, 2014 and applied to a sample of *N*=498 English speaking adults age 18 and over. The third survey data is from the Pew Research Center's Internet Project/GFK Privacy Panel Survey #3. The survey was conducted online between November 26, 2014 and January 3, 2015 and applied to a sample of *N*=475 English speaking adults age 18 and over. The fourth survey data is from the Pew Research Center's Internet Project/GFK Privacy Panel Survey #4. The survey was conducted online between January 27, 2015 and February 16, 2015 and applied to a sample of *N*=461 English speaking adults age 18 and over.

My study was designed to facilitate an understanding of how individuals across America view several key areas of personal privacy in consideration of modern technology and social trends. This included specific inquiries about information sharing and whether respondents believe American citizens should be concerned about government monitoring of phone calls, text, and Internet communications.

The central research inquiry was whether elite theory may serve as a working social theory that is applicable to policy-based decision making. The question is important because if elite theory is reliable it may be employed by policy professionals who review existing policies as well as those tasked with creating new social policy. Specifically, if elite theory suggests that it is the elite who control social policy and policy can be designed and implemented with little regard for the nonelite population (Domhoff, 2010), then policy need only be drafted to fulfill the goal of government and the elite stakeholders and not the population.

My study was guided by secondary data obtained from surveys inquiring how individuals view privacy and whether they are invested in securing sensitive information or rather, they are uninterested, uninformed, acquiescing, and need not be strongly considered during policy evaluation.

Themes and Coding

I identified six emergent theme categories from the other research papers using thematic coding procedures and then applied each to the survey questions analyzing data provided by the participants. I then coded the data by assigning a value to each

participant answer based on where the answer fell within each category. For example, Question 19 asks participants if they have changed internet or cell phone use in recent months to avoid having their activities tracked or noticed. The answers were coded (a) not changed; (b) changed; and (c) no answer. They were categorized under “changed behavior”. This provided an easily understood categorization of useable data and eliminated an otherwise complex range of answers associated with many of the questions. The coded survey answers were then combined with other coded data to determine participant views of privacy and their behavioral response to government monitoring.

My analysis of the survey data was designed to test the stated research hypotheses. Data were obtained from answers to survey questions administered to a randomized population of English-speaking adults. The survey responses used in the analysis reflect the ordinal subtypes of the dependent variable (individual privacy behavior), in consideration of government monitoring. Responses are represented below as percentage answers (x percent of responses within each category). Participant responses reveal several emergent themes that are connected to the research question; each triangulated and confirmed. The six themes and their associated code are identified as follows and the questions and coded responses are displayed in Appendix A.

Table 3

Themes and Coding

	Government trust and accountability	Generalized concern about privacy	Changing future behavior	Knowledge of government monitoring	Acceptance of government monitoring	Changed behavior
A	favorable government view	not concerned secure	no change	knowledge	accept	no change
B	not favorable government view	concerned/ not secure	change	no knowledge	not accept	Changed
C	no answer	no answer	no answer	no answer	no answer	no answer

Summary

The research presented in this chapter (data found in Appendix A), are the responses of individuals from a randomized population as they go about daily life in an environment of domestic governmental monitoring. The data suggest that most individuals surveyed do know about government monitoring, have concerns about privacy, and indicate that they would like to do more to protect it.

Although participants describe an ongoing concern for personal privacy and believe government surveillance of private citizens should be limited, my research suggested that they did not take significant and sustained actions to mitigate government surveillance in their personal lives. The research indicated that a majority of people did

not significantly shield their exposure to surveillance or change their personal behavior to reduce the footprints they leave behind on the surveillance landscape.

Chapter 5 provides a detailed compilation of the information and data provided in the previous chapters including the literature review. It offers an analysis of the data in Chapter 4 and provides the reader with a summary of the result. The chapter continues with an in-depth interpretation of the findings, recommendations for future research, and demonstrates a case for the application of elite theory in addressing a real-world policy issue. Finally, I comment on the potential impact of this research on social change and how the outcome may be used by both policy professionals and academics in the future.

Chapter 5: Findings and Discussion

Overview

Shortly after the attacks on September 11, 2001 the U.S. government initiated several new security policies aimed at preventing similar attacks on the United States from happening in the future (American Civil Liberties Union, 2020). Twenty years later, there have been no terror attacks on the United States that were equal in magnitude to the 9/11 attacks (CNN, 2020). This may be evidence that the changed U.S. national security policies have worked though questions persist about the causal relationship between the security policy changes and the 20 years that elapsed between 9/11 and now. This is especially true in light of comments by a top white house official regarding the efficacy of bulk data collection techniques with respect to stopping terrorism wherein he indicated that they found none. (see Isikoff, 2013).

In 2013 a U.S. government contractor named Edward Snowden exposed several top-secret domestic spying programs used for bulk data collection and the relationship between government data analysis, large corporations, commercial big data, and the personal data of every citizen to which the U.S. government had access (Lawfare, 2020).

The purpose of my study was to explore the relationship between the diminution of individual privacy due to those government mass surveillance programs and the societal response to it across the national population. I designed the research question to investigate whether a fractional loss of an established civil liberty would trigger a response within the population (a substantial and sustained increase in privacy protection

behavior). My hypothesis was that (in conformance with elite theory), it would not. If that were the case one could image that any new or changed security policy need not necessarily account for collateral social consequences and that policy could instead focus solely on governmental interests.

Existing literature provided insight into the evolution of individual privacy in America and even touched on societal responses associated with changes in governmental policy but neglected to address whether elite theory (operating as a modern social theory), may be used to suggest social policy change outcomes prior to implantation of a new or changed policy.

Publication of this paper may contribute to a particularized understanding of whether policy professionals may rely upon elite theory to assist them as they gauge whether or not a policy proposal will drive social action toward an undesirable result. It also establishes a base for further academic inquiry into similar areas of research into different social theories and their similar use in policy analysis.

Analysis of the data from this study suggested that a large majority of the population does know that the government collects private information about citizens:

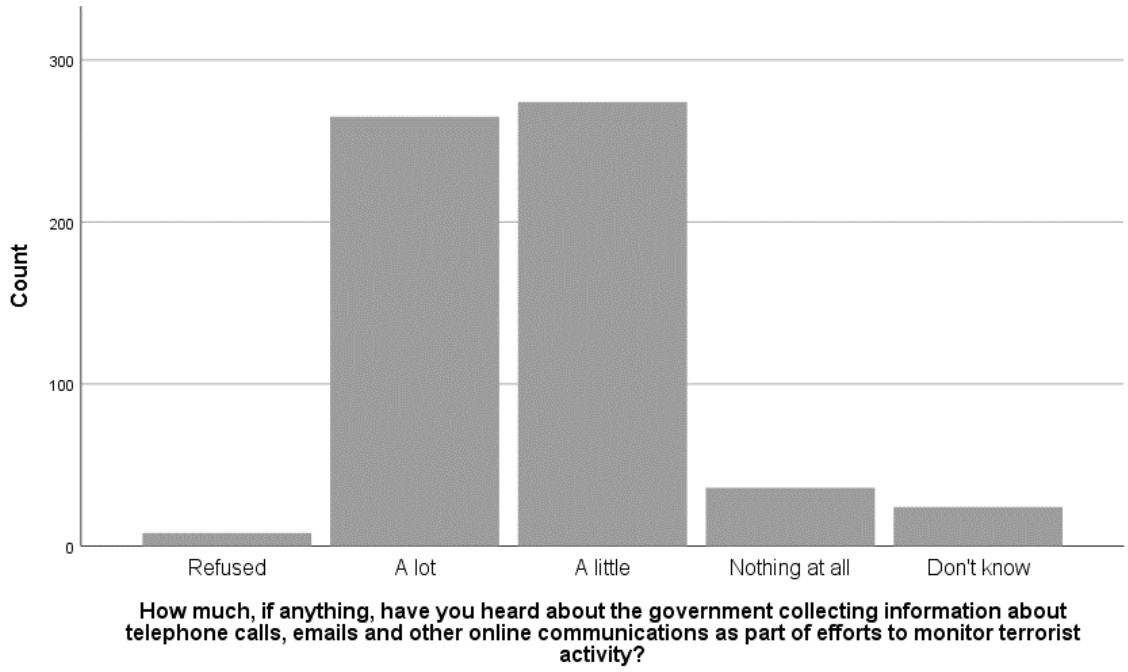


Figure 1. Question 14 (sp17)

The data also suggested that individuals believe citizens should be concerned about the fact that it is happening:

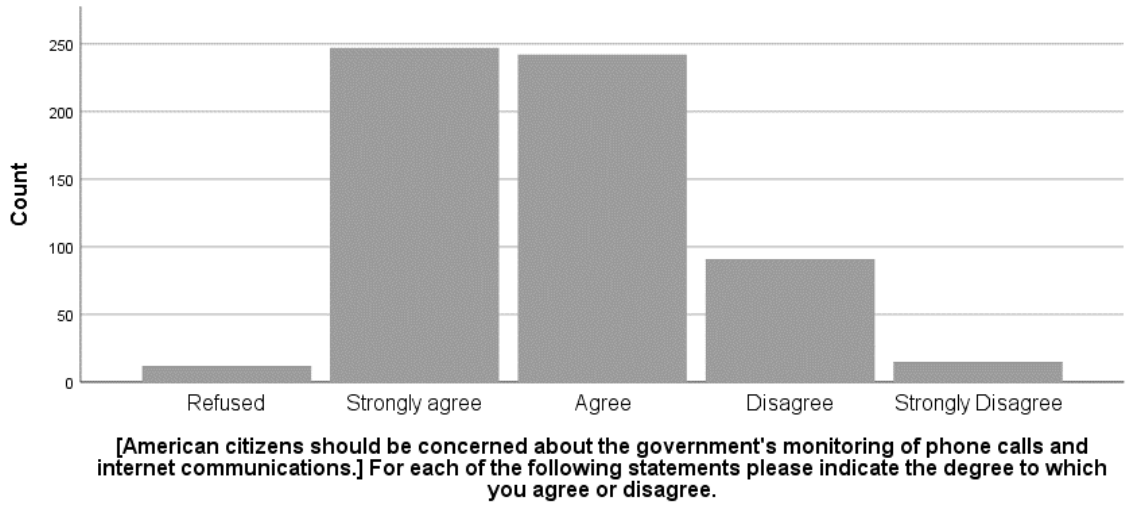


Figure 2. Question 11 (sp9) i

The data further suggested that respondents themselves are concerned about the fact that the government is secretly reviewing information about them:

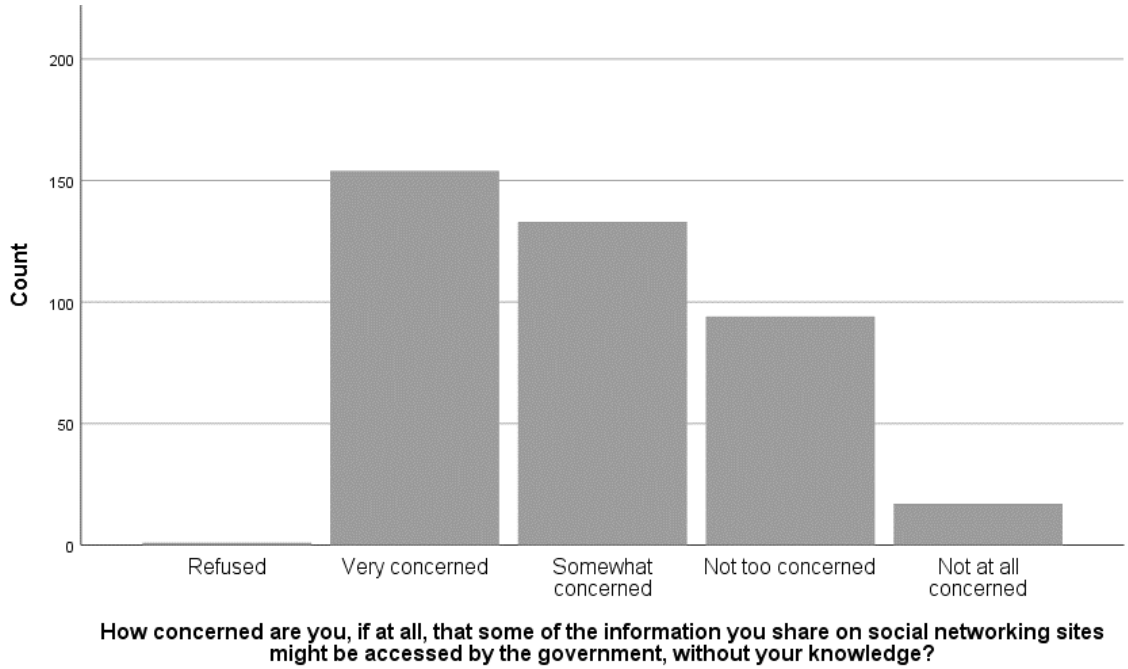


Figure 3. Question 13 (sp11)

Most people surveyed disagree or strongly disagree that it is good for someone to ‘keep an eye’ on their online activity:

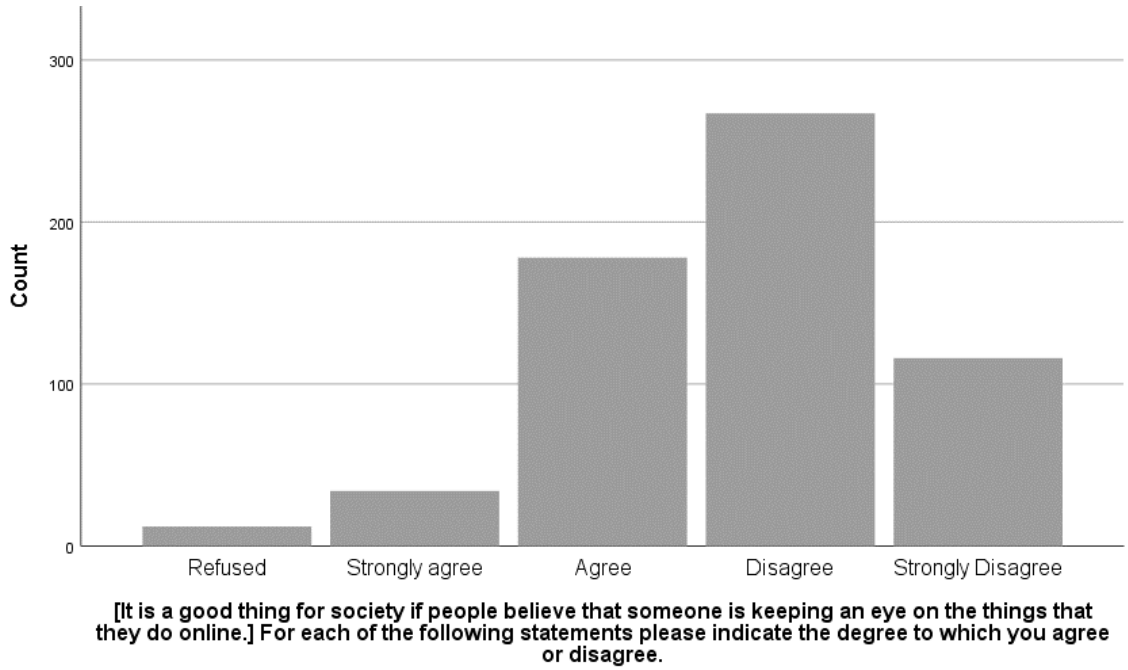


Figure 4. Question 18 (sp28)

A majority of those surveyed believed it is unacceptable for the U.S. government to monitor its own people.

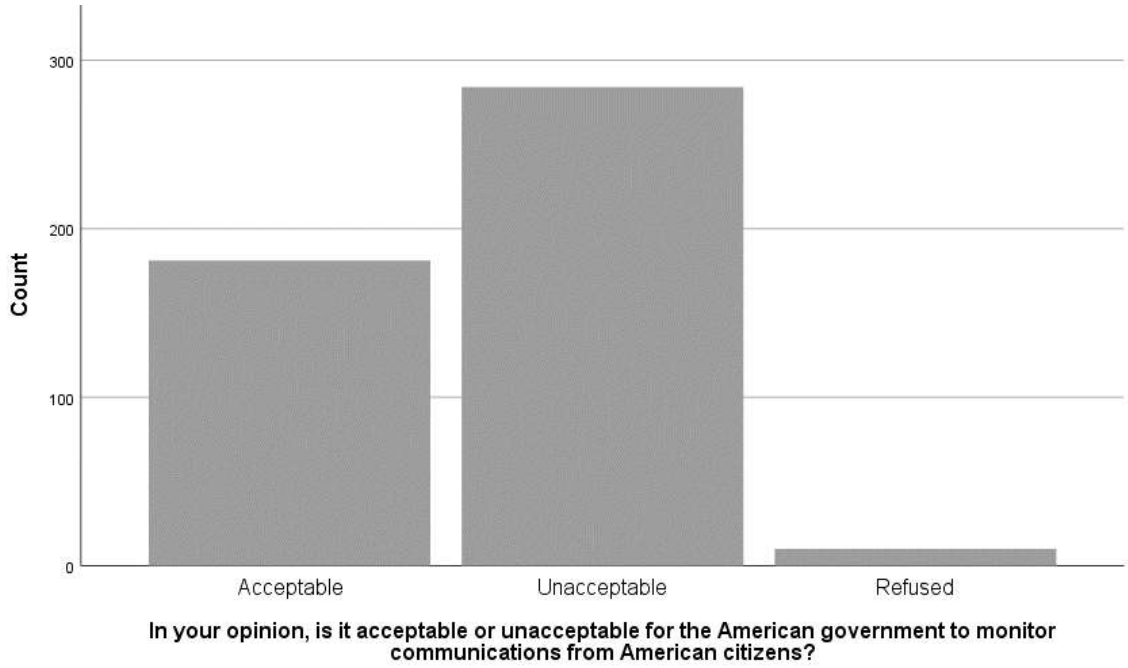


Figure 5. Question 27 (s14)

Respondents considered themselves to be mostly private.

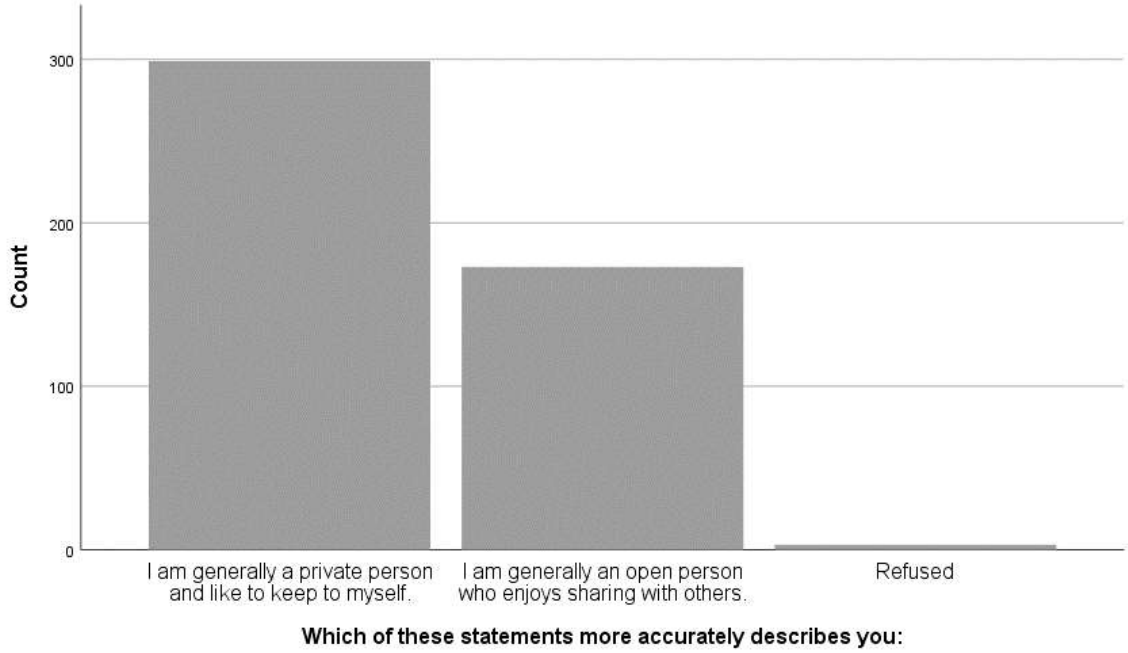


Figure 6. Question 23 (sp9)

They also indicated that the limits on the information that the government can collect about them are not adequate.

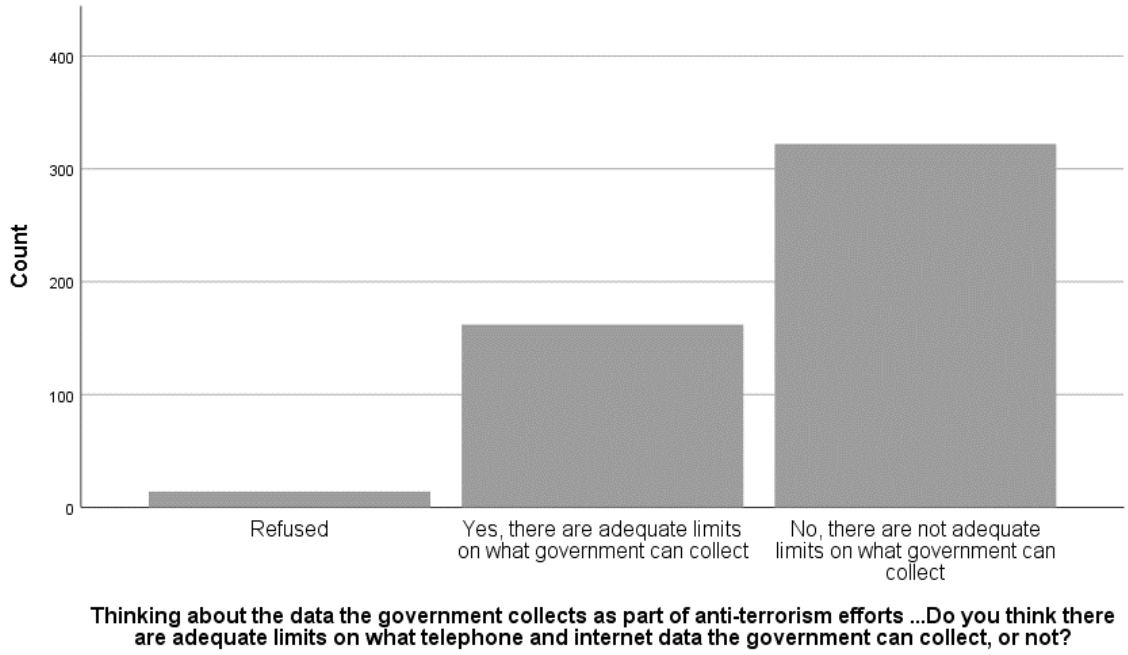


Figure 7. Question 18 (sp28)

People believed that the government can be trusted some of the time or never.

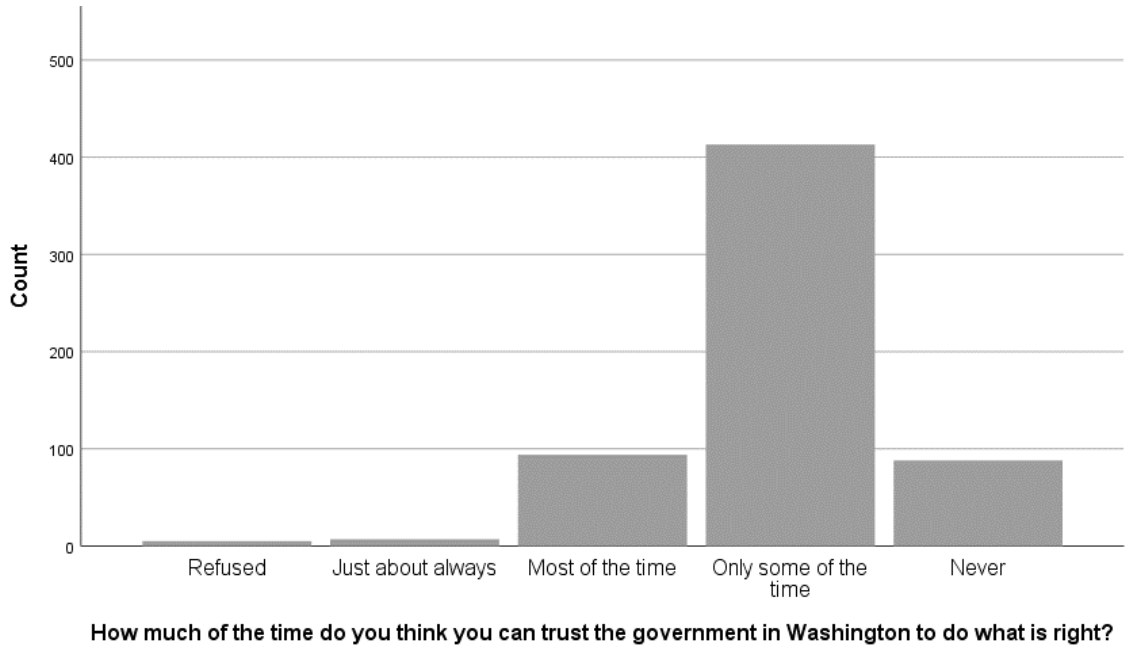


Figure 8. Question 1 (sp2)

The anticipated behavioral response of individuals in a population that maintains an overall distrust of or have a generally unfavorable view of government would be for them to continue or increase privacy shielding behavior(s). A majority of those surveyed stated they do not feel that they do enough to protect their private information.

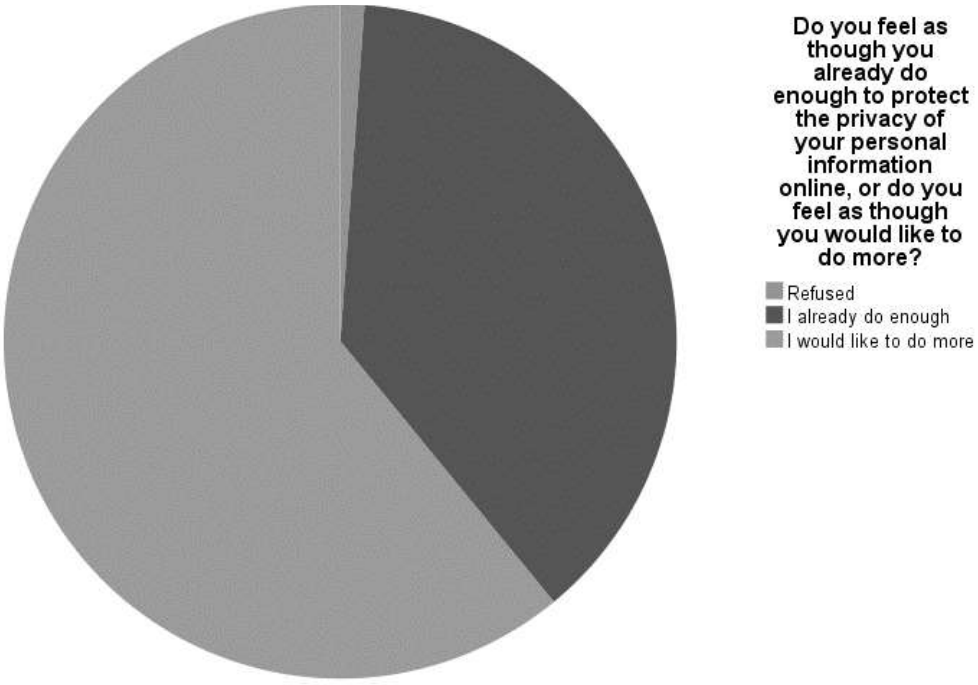


Figure 9. Question 3 (sp6)

Analysis of the combined survey data suggest that most of the population fit within the following criteria:

- were generally private
- had knowledge that the government is secretly monitoring them
- thought that there are not adequate limits on the government
- believed the government should not be trusted
- did not think is good for someone to watch their online activity

- believed others should be concerned about this
- were themselves in fact concerned

Interpretation of the Findings

This study provided a review of personal privacy in the United States and an analysis of population data regarding personal privacy compiled over a multi-year period. The study was designed to facilitate a generally applicable result that is reproducible and can withstand external scrutiny. Following a thematic analysis of existing studies and the statistical analysis of secondary data I was able to extract and interpret several emergent themes using a selective coding technique. Ultimately this led me to conclude that the null hypothesis may be rejected and that the stated hypothesis may be accepted.

The data show that U.S. population behavior generally does adhere to the elements of elite theory. Individuals across the U.S. hold strong views when it comes to personal privacy and freedom from surveillance. Following a disruptive change to domestic security policy one may expect significant changes in the public's collateral privacy behavior. However, as described by the elements of elite theory this is not what actually happens. My research suggests that people did not always behave in accord with their stated views and may not have enacted meaningful behavioral changes to protect their privacy.

A review of the secondary data provided several insights into the U.S. population's perception of government as well as their individual beliefs and behaviors following the 2013 Snowden leak. The literature review provided thematic interpretation

of the theories behind the observed data. Specially, thematic comparison among studies consistently confirmed that individuals are unmoved, uninterested, and remain aloof in the long-term following the release of Snowden's 2013 information about domestic government spying.

This parallels with the expectation of elite theory. In the Sidhu study of Muslims after 9/11 it was already known that the government was using several data gathering tools including Carnivore, Echelon, and Magic Lantern (although the extent to which monitoring was occurring of all US citizens was not known until 2013), to spy on citizens. Yet 86.8% of respondents said they had not changed their general activities due to a concern that the government may be monitoring them, 65.9% of respondents stated that they were not personally aware of any other Muslims in the United States who changed, in any way, their general activities after 9/11 because of a concern that the government may be monitoring their activities, and 89.1% of respondents said they have not changed their Internet usage at all, the sites they visit or the amount of time they spend on the Internet, after 9/11 due to a concern that the government may be monitoring their activities (Sidhu, 2007).

That study used data acquired following 9/11 and specifically examined Muslims (as a group who believe they were to be directly targeted by post-9/11 monitoring). It was acknowledged by the author that, "[w]hat accounts for the difference between the belief that the government is monitoring the Internet activities of Muslim-Americans and

resultant changes in online behavior is unclear" (Sidhu, 2007). My research suggests that the answer could be found in a thorough understanding of elite theory.

In the Marthews and Tucker 2017 study where the authors reported that there *was* variation in search engine query following the 2013 Snowden leak, the data involved a limited subset of search terms comprised of high levels of sensitivity. It makes sense that a downturn in search volume would occur in 'sensitive searches' after people just learned that the government was watching their Google queries. This response is even anticipated by the Oulasvirta and study that suggested when there is a temporary adjustment to new (changed), surveillance monitoring the population will adapt and regress to pre-change behavior. Again, these results are expected by elite theory.

Summary of the Findings

The overarching role of this research study was to provide policy professionals with an insight into whether elite theory may be relied upon when decision makers consider a population's response to the implementation of new social policy. The study results suggested that elite theory is a useful social theory that may be capable of indicating behavioral outcomes to new or different social policy.

The null hypothesis or default assumption of my research asserted that when the U.S. population realizes the government is seriously infringing upon an established liberty (secretly spying on them having surreptitiously inserted mass domestic surveillance into virtually every aspect of their private life), it will change and adopt some affirmative protective behavior in response. The data suggested that this null

hypothesis may be rejected and that a majority of the population does not substantially alter behavior or adopt permanent protective measures in response to policy changes.

Coding theme B (no-change responses) as 2 or above and theme A (yes-change responses) as 1; I obtained mean scores for all the change responses as follows:

Table 4

Descriptive Statistics

	N	Range	Mean	Std. Deviation	Variance
SMEAN(Q19_p2_sp9)	498	3	2	.428	.183
SMEAN(Q20_p2_sp11a)	498	4	2	.684	.468
SMEAN(Q20_p2_sp11b)	498	4	2	.582	.338
SMEAN(Q20_p2_sp11c)	498	4	2	.673	.453
SMEAN(Q20_p2_sp11d)	498	4	2	.669	.448
SMEAN(Q20_p2_sp11e)	498	4	1	.674	.454
SMEAN(Q20_p2_sp11f)	498	4	2	.624	.389
SMEAN(Q20_p2_sp11g)	498	4	2	.564	.318
SMEAN(Q20_p2_sp11h)	498	4	2	.688	.474
SMEAN(Q20_p2_sp11i)	498	4	2	.735	.541
SMEAN(Q20_p2_sp11j)	498	4	2	.652	.425
SMEAN(Q20_p2_sp11k)	498	4	2	.603	.364
SMEAN(Q20_p2_sp11l)	498	4	2	.648	.420
SMEAN(Q20_p2_sp11m)	498	4	1	.711	.505
SMEAN(Q37_p3_sp29b)	498	3	3	.835	.697
SMEAN(Q37_p3_sp29c)	498	3	4	.671	.450
SMEAN(Q37_p3_sp29d)	498	3	3	.814	.663
SMEAN(Q37_p3_sp29e)	498	3	3	.799	.638
SMEAN(Q37_p3_sp29f)	498	3	3	.765	.586
SMEAN(Q37_p3_sp29g)	498	3	3	.855	.732
SMEAN(Q38_p3_sp32a)	498	3	3	.819	.671
SMEAN(Q38_p3_sp32b)	498	3	3	.718	.516
SMEAN(Q38_p3_sp32c)	498	3	3	.881	.776
SMEAN(Q38_p3_sp32d)	498	3	3	.895	.800

SMEAN(Q38_p3_sp32e)	498	3	3	.649	.421
SMEAN(Q38_p3_sp32f)	498	3	3	.719	.517
SMEAN(Q38_p3_sp32g)	498	3	3	.829	.687
SMEAN(Q38_p3_sp32h)	498	3	3	.796	.633
SMEAN(Q38_p3_sp32i)	498	3	3	.646	.418
SMEAN(Q38_p3_sp32j)	498	3	3	.722	.522
SMEAN(Q38_p3_sp32k)	498	3	3	.738	.545
SMEAN(Q39_p3_sp35a)	498	3	3	.708	.501
SMEAN(Q39_p3_sp35b)	498	3	3	.603	.364
SMEAN(Q39_p3_sp35c)	498	3	3	.592	.351
SMEAN(Q39_p3_sp35d)	498	3	2	.825	.681
SMEAN(Q39_p3_sp35e)	498	3	3	.651	.424
SMEAN(Q39_p3_sp35f)	498	3	3	.733	.537
SMEAN(Q39_p3_sp35i)	498	3	3	.616	.379
Valid N (listwise)	498				

As this tables demonstrates, of the data samples collected there were only two samples that indicated a change behavior. All other samples indicate no change in behavior was identified.

Additional Research

Several questions related to issues of security policy and social change are ripe for additional inquiry. As of the writing of this paper there have been no publicly reported mass terror incidents anywhere on the globe similar in magnitude to those that occurred in the U.S. on 9/11 (CNN, 2020). Is this attributable to America's changed national security policies over the past twenty years? If so, was the reduction in civil liberties a reasonable tradeoff? Must those policies continue or even be amplified to maintain domestic safety? Was 9/11 a one-off that would not have repeated even if intrusive government monitoring programs were not employed? What happens to civil rights if another 9/11 type-event occurs? How would security policy change again? To what

extent would the civil liberties of citizens change? My research did not address these questions or the assumption that increased monitoring of the population by the government causally effects citizen safety in a significant and positively correlated way and all of these questions remain.

If the 2013 Snowden leak or similar release of classified information had not occurred, I would not have been able to undertake this research and American society would likely have remained in the dark with respect to these questions. Twenty years after 9/11 and seven years after the Snowden leak, the public is still not privy to details of national security policy or its true effectiveness because it remains classified and insulated from public inquiry. While my research has shown that privacy and civil liberties have decreased and the government has more information than ever about each one of us, there is no data, no statistics, no transparency, no way to quantify security policy effectiveness without additional information releases.

Social Change and Future Public Policy Implications

The research question addressed in this paper goes well beyond whether citizens will accept losses of civil liberties in exchange for perceived increases of general security. I inquired whether the input of millions of nonelites matter at all. Elite theory seems to suggest that the nonelite public have little to no regard for policy and that over time even the majority of those with strongly held policy contradicting beliefs will adapt to policy changes. This research is applicable to several divisive current day social policy questions.

In the years following the start of this dissertation and after media coverage of dozens of mass shooting incidents occurring since 2014 (defined as a shooting involving three or more fatalities), increasing numbers of Americas voiced support of stricter national gun control policies. In response to those incidents U.S. government officials proposed several new or modified policies regarding legal gun ownership. Most notable was an official policy statement that guns should be outlawed and even confiscated from lawful U.S. owners (Biden, 2020).

While many of the proposals are probably unconstitutional and may be politically motivated others represent serious strategies for closing purchasing loopholes and decreasing ease of access to potential non-lawful owners. As a result, policy professionals may use theoretical tools to make educated estimations regarding gun control policy outcomes. According to my research if policy can be justified through general threats to safety the collateral social consequences need not require exceptional scrutiny by policy makers.

If lawful gun owners reject new or changed regulation and even forced confiscation my research suggests a majority of individuals will adapt and acquiescence. As goes the case for a reduction in a civil liberty like privacy may go the case for a reduction in 2nd Amendment rights. One may expect that some gun owners would exhibit defiance (similar to the few individuals who attempt to anonymize their data footprint), but the overall majority would not and a majority of those that do will eventually acquiesce.

In early March 2020, the United States was faced with responding to the Pandemic disease COVID-19. Among the (very delayed), policies implemented by the U.S. government in an attempt to minimize and mitigate the harm done by virus spread was the wearing of masks and the virtual lockdown of travel and small businesses by federal and state officials. Many legal safeguards were abandoned in the name of health and safety as State governors exercised orders of increasingly strict measures in order to protect the public from itself. In an April, 2020 interview on the Fox News channel by Tucker Carlson, the New Jersey state Governor stated that, “I wasn’t thinking of the Bill of Rights when we did this…”. An admission from the highest-ranking authority in the State of New Jersey that policies were put into place without concern for civil legal protections.

As predicted by the results of this research, while some individuals initially voiced concerns against lockdowns and mask wearing the vast majority acquiesced despite contradictory indicators and lacking scientific evidence. By late September, 2020 daily masking wearing become normalized and business offered many different styles for consumers to purchase. These social policy examples of gun control, quarantine, and mask wearing exemplify additional areas of policy beside privacy to which this area of research may be applicable.

The research results indicated in this paper do not suggest that policy professionals must or even should incorporate elite theory into decision making. Rather, my intention was to offer this research as guidance to other academics and researchers

who are interested in understanding how social policy change decisions may be acted upon and to be guided accordingly.

References

19 C.F.R. § 162.6. Title 19 – Customs Duties. Part 162 – RECORDKEEPING, INSPECTION, SEARCH, AND SEIZURE

American Civil Liberties Union, (2020). Surveillance Under the Patriot Act. Retrieved from https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act

American Civil Liberties Union, (2020). Surveillance Under the USA/Patriot Act. Retrieved from https://www.aclu.org/other/surveillance-under-usapatriot-act

Aftergood, S. (2012, October 17). Secrecy news: The purpose of national security policy, declassified. *Federation of American Scientists*. Retrieved from fas.org/blogs/secrecy/2012/10/nsdd_238/

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, D. L., Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology 8*(2), 121-144. doi:10.1111/ips.12048

Berkes, H. (2013). Amid Data Controversy, NSA Builds Its Biggest Data Farm. Retrieved September 25, 2020, from https://www.npr.org/2013/06/10/190160772/amid-data-controversy-nsa-builds-its-biggest-data-farm

Biden, J., (2020). The Biden Plan to End Our Gun Violence Epidemic. Biden Harris. Retrieved from https://joebiden.com/gunsafety/

Boslaugh, S. (2013). Statistics in a nutshell. Sebastopol, California. O'Reilly.

Braun, V. & Clarke, V. (2008). Using thematic analysis in psychology. *Qualitative Research in Psychology.* Retrieved from https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa?journalCode=uqrp20

Braun, V. & Clarke, V. (2012). Thematic analysis. In H. Cooper (Ed.), Handbook of research methods in psychology. Washington, DC: APA Books.

BRM (2019). Research reliability. Business Research Methodology. Retrieved from https://research-methodology.net/research-methodology/reliability-validity-and-repeatability/research-reliability/#:~:text=In%20simple%20terms%2C%20research%20reliability,times%20produces%20the%20same%20results.

California v. Greenwood, 486 U.S. 35 (1988).

Carpenter v. United States, 38 S. Ct. 2206 (2018).

Carroll v. United States, 267 U.S. 132 (1925).

Chimel v. California, 395 U.S. 752 (1969).

CNN, (2020). US Terrorist Attacks Fast Facts. CNN Editorial Research. Retrieved from https://www.cnn.com/2013/04/18/us/u-s-terrorist-attacks-fast-facts/index.html

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed method approaches*. Thousand Oaks, CA: SAGE Publications.

Cupp v. Murphy, 412 U.S. 291 (1973).

David E. Pozen, 115 Yale L.J. 628 (2005).

Davis, D. & Silver, B. (2004). Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. *American Journal of Political Science*. 48. 28 – 46. doi:10.2307/1519895

Dodge, Y. (2003). The Oxford Dictionary of Statistical Terms. The International Statistical Institute. Oxford University Press. Retrieved from https://stats.oecd.org/glossary/detail.asp?ID=2377

Domhoff, G. W. (2010). Who rules America? Power, politics, & social change. Santa Cruz, CA: Prentice-Hall.

Downs, A. (1957). An economic theory of democracy. University of Michigan. Harper and Row.

Eidam, E. (2017). Privacy vs. Security: Experts Debate Merits of Each in Tech-Rich World. Retrieved from https://www.govtech.com/policy/Privacy-vs-Security-Experts-Debate-Merits-of-Each-in-Tech-Rich-World.html

Electronic Frontier Foundation, (2020). NSA Spying. Retrieved from https://www.eff.org/nsa-spying

Electronic Frontier Foundation, (2020). PATRIOT Act. Retrieved from https://www.eff.org/issues/patriot-act#:~:text=The%20USA%20PATRIOT%20Act%20(officially,the%20September%2011%2C%202001%20attacks.&text=Bush%20on%20October%2026%2C%202001.

Farid, N. (2015). Your Data Shadow: An exploratory study of the short-term effect of

viewing news and information content on surveillance technologies on perceptions of privacy (Master's thesis). Carleton University, Ottawa, Ontario. Retrieved https://curve.carleton.ca/system/files/etd/b6035412-e5c0-47b8-8f75-963935be7f19/etd_pdf/016a8496d0cd6dce8b11fe622faeb4ac/farid-yourdatashadowanexploratorystudyoftheshortterm.pdf

Federation of American Scientists, (n.d.). Security Classification of Information. Retrieved from https://fas.org/sgp/library/quist2/chap_7.html

Field, A. (2005). Reliability analysis. In A. Field (Ed.), Discovering statistics using SPSS (2nd, ed.). London, England: Sage.

Field, G. L., & Higley, J. (2014). Elitism. London, England: Routledge.

Flick, U. (2017). Introduction to qualitative research. Thousand Oaks, CA: Sage Publications.

Foreign Intelligence Surveillance Act. (n.d.). The SAGE Encyclopedia of Surveillance, Security, and Privacy. Doi:10.4135/9781483359922.n177

Fusion Centers, (2017). National Network of Fusion Centers Fact Sheet. (2017, June 21). Retrieved from https://www.dhs.gov/national-network-fusion-centers-fact-sheet

Gilens, M., & Page, B. (2014). Testing theories of American politics: Elites, interest groups, and average citizens. *Perspectives on Politics, 12*(3), 564-581. Doi:10.1017/S1537592714001595

Green, A. (2020). [blog] Complete Guide to Privacy Laws in the US. Retrieved from https://www.varonis.com/blog/us-privacy-laws/

Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241 (1964).

Hedges, L. (1981). Distribution theory for Glass's estimator of effect size and related estimators. *Journal of Educational Statistics, 6*(2), 107-128. Doi:10.2307/1164588

Hester v. United States, 265 U.S. 57 (1924).

Higley, J., & Burton, M. G. (2006). Elite foundations of liberal democracy. Lanham, MD: Rowman & Littlefield.

Higley, J., & Pakulski, J. (2012). Elite theory versus Marxism: The twentieth century's verdict [2000]. *Historical Social Research / Historische Sozialforschung, 37*(1 (139)), 320-332. Retrieved from http://www.jstor.org/stable/41756463

Intelligence Reform and Terrorism Prevention Act of 2004, (n.d.). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282

Isikoff, M., (2013). NSA program stopped no terror attacks, says White House panel member. NBC NEWS. Retrieved from https://www.nbcnews.com/news/world/nsa-program-stopped-no-terror-attacks-says-white-house-panel-flna2D11783588

Ran, J. (2016). Striking the balance between privacy and governance in the age of technology. *SPICE: Student Perspectives on Institutions, Choices and Ethics: Vol. 11* : Iss. 1, Article 2. Retrieved September 25, 2020, from https://repository.upenn.edu/spice/vol11/iss1/2/

Kaminski, M. E. and Witnov, S. (2015). The conforming effect: First amendment

implications of surveillance, beyond chilling speech. *University of Richmond Law Review, 49;* Ohio State Public Law Working Paper No. 288. Retrieved from https://ssrn.com/abstract=2550385

Katz v. United States, 389 U.S. 347 (1967)

Kyllo v. United States, 533 U.S. 27 (2001)

Lawfare, (2020). Snowden Revelations. The Lawfare Institute. Retrieved from https://www.lawfareblog.com/snowden-revelations

Leetaru, K. (2019). Much Of Our Government Digital Surveillance is Outsourced to Private Companies. Retrieved September 25, 2020, from https://www.forbes.com/sites/kalevleetaru/2019/06/18/much-of-our-government-digital-surveillance-is-outsourced-to-private-companies/#2365e5451799

Lippmann, W. (2014). Public opinion. Whitefish, MT. Literary Licensing, LLC.

Lippmann, W., & MacClay, W. M. (2017). The phantom public. London, England. Routledge, Taylor & Francis Group.

López, M. (2013). Elite Theory. Doi:10.1177/2056846013112

Lopreato, S. (1974). The fundamentals of elite circulation: Toward formalization and extension of Pareto's theory. *Revue Européenne Des Sciences Sociales, 12*(33), 51-74. Retrieved from http://www.jstor.org/stable/40369034

Lund Research, (2018). Hypothesis Testing. Retrieved from https://statistics.laerd.com/statistical-guides/hypothesis-testing-2.php

Madden, M., & Rainie, L. (2015, May 20). Americans' Attitudes About Privacy, Security

and Surveillance. Retrieved April 18, 2018, from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/#

Marthews, Alex & Tucker, Catherine. (2014). Government Surveillance and Internet Search Behavior. SSRN Electronic Journal. 10.2139/ssrn.2412564.

Maryland v. King, 569 U.S. _ (2013).

Maslow, A. H. (1954). Motivation and personality. New York: Harper and Row. Maslow, A. H. (1962)

Merriam-Webster. (n.d.). Public policy. In Merriam-Webster.com dictionary. Retrieved September 25, 2020, from https://www.merriam-webster.com/dictionary/public%20policy

Mertler, C.A. (2018) Introduction to educational research. Los Angeles: SAGE

Missouri v. McNeely, 569 U. S. 141 (2013).

Mosca, G. (1939). The ruling class. New York. McGraw Hill.

Michels, R. W., & Paul, M. E. (1915). Political Parties: A sociological study of the oligarchical tendencies of modern democracy … Translated from the Italian by Eden and Cedar Paul. London. Jarrold & Sons.

Morwood, N. (2012, March 01). Sovereignty, the State of Exception and Counter-culture: Toward a Transnational Critique of State Power in 20th and 21st Century Anglophone Fiction. Retrieved from https://tspace.library.utoronto.ca/handle/1807/42539

Mulligan, D.K., & Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *The Royal Society Publishing. Philosophy transactions. Series A, Mathematical, physical, and engineering sciences.* doi: 10.1098/rsta.2016.0118

National Security Letters. (n.d.). Retrieved April 18, 2018, from https://www.aclu.org/other/national-security-letters

Obar, J. (2015). Big Data & Society: 1–16 sagepub.co.uk/journalsPermissions.nav DOI: 10.1177/2053951715608876 bds.sagepub.com

ODNI Home. (n.d.). Retrieved April 18, 2018, from https://www.dni.gov/index.php/who-we-are/leadership/director-of-national-intelligence

Orwell, G. (1949). *1984*. New York: Penguin Books.

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., & Myllymäki, P. (2012, September). *Long-term effects of ubiquitous surveillance in the home.* In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 41-50). ACM.

Panagopoulos, C. (2011). Social pressure, surveillance and community size: Evidence from field experiments on voter turnout. *Electoral Studies, 30*(2), 353-357. doi:10.1016/j.electstud.2010.10.005

Pareto, V., Livingston, A., Bongiorno, A., & Rogers, J. H. (1935). *The mind and society*. New York: Harcourt, Brace and Company.

Pew Research Center, (2020). [About] Retrieved from

https://www.pewresearch.org/about/

Pew Research Center, (2020). [Methods] Our survey methodology in detail. Retrieved from https://www.pewresearch.org/methods/u-s-survey-research/our-survey-methodology-in-detail/

Pozen, D.E., (2005). The Mosaic Theory, National Security, and the Freedom of Information Act. 115 YALE L. J. 628. Retrieved from https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1527&context=faculty_scholarship

Research Rundowns (2020). Instrument, Validity, Reliability. Retrieved from https://researchrundowns.com/quantitative-methods/instrument-validity-reliability/

Riley v. California, 134 S. Ct. 2473 (2014)

Rosenzweig, P., (2017). In Defense of the Mosaic Theory. The Lawfare Institute. Retrieved from https://www.lawfareblog.com/defense-mosaic-theory#:~:text=By%20way%20of%20short%20introduction,take%20account%20of%20that%20fact

Q&A on the Pentagons "Total Information Awareness" Program. (n.d.). Retrieved April 18, 2018, from https://www.aclu.org/other/qa-pentagons-total-information-awareness-program.

Salkind, N. J. (2010). Encyclopedia of research design. Thousand Oaks, CA: SAGE Publications Ltd doi: 10.4135/9781412961288

Schmerber v. California, 384 U. S. 757 (1966)

Schultz, D., (2012). *American Politics in the Age of Ignorance: Why Lawmakers Choose Belief Over Research*. New York: Palgrave Macmillan.

Bhandari, P. (2020). Understanding internal validity. Scribbr. Retrieved from https://www.scribbr.com/methodology/internal-validity/#:~:text=There%20are%20eight%20threats%20to,mean%2C%20social%20interaction%20and%20attrition.

Semple, J. (1993). Jeremy Bentham and the Origins of the Panopticon. *Benthams Prison,* 20-41. doi:10.1093/acprgof:oso/9780198273875.003.0002

Smith v. Maryland, 442 U.S. 735 (1979)

Sidhu, S., D., The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans, 7 U. Md. L.J. Race Religion. Gender & Class 375 (2007). Retrieved from http://digitalcommons.law.umaryland.edu/rrgc/vol7/iss2/10

Solove, D. J., & Schwartz, P. M. (2018). Privacy, law enforcement and national security. New York: Wolters Kluwer.

Scottek, T.C. & Kopfstein, J., (2013). Everything you need to know about PRISM. Retrieved on September 25, 2020, from https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

Somin, I., (2016). Democracy and Political Ignorance: Why Smaller Government Is

Smarter, Second Edition. Stanford: Stanford University Press.

Stat Trek, (2020). Bias in Survey Sampling. Retrieved from https://stattrek.com/survey-research/survey-bias.aspx#:~:text=Bias%20often%20occurs%20when%20the,Undercoverage.

Suter, W.N., (2012). Introduction to Educational Research: A Critical Thinking Approach. Retrieved from https://www.sagepub.com/sites/default/files/upm-binaries/43144_12.pdf

Terry vs. Ohio, 392 U.S. 1 (1968)

U.S. v. Ford, 34 F.3d 992 (1994).

U.S. v. Martinez-Fuerte, 428 U.S. 543 (1976)

U.S. v. Penny-Feeney, 773 F. Supp. 220 (D. Haw. 1991).

U.S. v. Jones, 132 S. Ct. 945 (2012).

US Department of Homeland Security, (2017). Retrieved September 25, 2020, from https://www.dhs.gov/implementing-911-commission-recommendations

USA PATRIOT ACT, (n.d.). Retrieved April 18, 2018, from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1281

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. doi:10.2307/1321160

Weber, M. (1968). Economy and society. New York: Bedminster Press.

Whittaker, A. G., Brown, S. A., Smith, F. C., & McKune, E. (2011, August 15). The National Security Policy Process*: The National Security Council and Interagency*

System. Retrieved September 25, 2020, from https://issat.dcaf.ch/download/17619/205945/icaf-nsc-policy-process-report-08-2011.pdf

Appendix A: Tables

A total of 607 participants provided data for the privacy survey and there were 39 questions used in the analysis. Each question was coded with one of three possible outcomes creating a total of 117 coded data points for review. The following questions were obtained from Survey 1 and represent a percent of total answers.

Table A5

Question 1. (sp2) How much of the time do you think you can trust the government in Washington to do what is right?

Answer	Percentage	Code
Just About Always	2%	A
Most of the Time	16%	A
Only Some of the Time	67%	B
Never	14%	B
Refused	1%	C

Notes. A total of 606 of 607 respondents answered this question.

Table A6

Question 2. (sp7) Thinking about your daily life, when you have private information that you would like to share with another trusted person or organization, how secure do you feel [using the following devices or methods]?

a. Telephone line

Answer	Percentage	Code
Very Secure	16%	A
Somewhat Secure	51%	A
Not Very Secure	19%	B
Not at All Secure	12%	B
Refused	1%	C

Notes. A total of 606 of 607 respondents answered this question.

Table A7

b. Cell phone

Answer	Percentage	Code
Very Secure	9%	A
Somewhat Secure	43%	A
Not Very Secure	29%	B
Not at All Secure	17%	B
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table A8

c. Text message

Answer	Percentage	Code
Very Secure	7%	A
Somewhat Secure	32%	A
Not Very Secure	37%	B
Not at All Secure	22%	B
Refused	7%	C

Notes. A total of 604 of 607 respondents answered this question

Table A9

d. Email

Answer	Percentage	Code
Very Secure	5%	A
Somewhat Secure	35%	A
Not Very Secure	36%	B
Not at All Secure	21%	B
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question

Table A10

e. Chat or Instant messenger

Answer	Percentage	Code
Very Secure	4%	A
Somewhat Secure	25%	A
Not Very Secure	36%	B
Not at All Secure	32%	B
Refused	3%	C

Notes. A total of 604 of 607 respondents answered this question

Table A11

f. Social media sites

Answer	Percentage	Code
Very Secure	2%	A
Somewhat Secure	14%	A
Not Very Secure	28%	B
Not at All Secure	53%	B
Refused	3%	C

Notes. A total of 604 of 607 respondents answered this question

Table 12

Question 3. (sp6) Do you feel as though you already do enough to protect the privacy of your personal information online, or do you feel as though you would like to do more?

Answer	Percentage	Code
I Already do Enough	37%	A
Would Like to do More	61%	B
Refused	1%	C

Notes. A total of 606 of 607 respondents answered this question.

Table 13

Question 4. (sp8) We'd now like to know how you feel about a range of information that others might learn about you in daily life. For each kind of information, please indicate how sensitive you consider that information to be – even if some people and organizations already have access to it.

a. Purchasing habits

Answer	Percentage	Code
Very Sensitive	8%	B
Somewhat Sensitive	33%	B
Not Too Sensitive	44%	A
Not at all Sensitive	14%	A
Refused	1%	C

Notes. A total of 606 of 607 respondents answered this question.

Table 14

b. Who your friends are and what they are like

Answer	Percentage	Code
Very Sensitive	22%	B
Somewhat Sensitive	46%	B
Not Too Sensitive	23%	A
Not at all Sensitive	7%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 15

c. Details of physical location over time from cellphone data

Answer	Percentage	Code
Very Sensitive	50%	B
Somewhat Sensitive	32%	B
Not Too Sensitive	11%	A
Not at all Sensitive	5%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 16

d. State of your health and the medicines you take

Answer	Percentage	Code
Very Sensitive	55%	B
Somewhat Sensitive	26%	B
Not Too Sensitive	12%	A
Not at all Sensitive	5%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 17

e. Political views and the candidate you support

Answer	Percentage	Code
Very Sensitive	20%	B
Somewhat Sensitive	31%	B
Not Too Sensitive	30%	A
Not at all Sensitive	17%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 18

Question 5. (sp8) For each kind of information, please indicate how sensitive you consider that information to be – even if some people and organizations already have access to it.

a. Media you like: tastes in music, movies, books, websites, magazines.

Answer	Percentage	Code
Very Sensitive	9%	B
Somewhat Sensitive	22%	B
Not Too Sensitive	45%	A
Not at all Sensitive	21%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 19

b. Numbers you have called or texted from your phone

Answer	Percentage	Code
Very Sensitive	45%	B
Somewhat Sensitive	30%	B
Not Too Sensitive	16%	A
Not at all Sensitive	6%	A
Refused	3%	C

Notes. A total of 604 of 607 respondents answered this question.

Table 20

c. Your religion or spiritual views

Answer	Percentage	Code
Very Sensitive	22%	B
Somewhat Sensitive	23%	B
Not Too Sensitive	29%	A
Not at all Sensitive	25%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 21

d. Your relationship history, including people you have dated or were romantically involved with in the past

Answer	Percentage	Code
Very Sensitive	40%	B
Somewhat Sensitive	31%	B
Not Too Sensitive	14%	A
Not at all Sensitive	12%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 22

Question 6. (sp8) For each kind of information, please indicate how sensitive you consider that information to be – even if some people and organizations already have access to it.

a. Your birthdate

Answer	Percentage	Code
Very Sensitive	41%	B
Somewhat Sensitive	25%	B
Not Too Sensitive	19%	A
Not at all Sensitive	14%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 23

b. Your social security number

Answer	Percentage	Code
Very Sensitive	90%	B
Somewhat Sensitive	5%	B
Not Too Sensitive	2%	A
Not at all Sensitive	1%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 24

c. Websites you have visited

Answer	Percentage	Code
Very Sensitive	27%	B
Somewhat Sensitive	43%	B
Not Too Sensitive	20%	A
Not at all Sensitive	8%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 25

d. Searches you have made using online search engines

Answer	Percentage	Code
Very Sensitive	24%	B
Somewhat Sensitive	41%	B
Not Too Sensitive	22%	A
Not at all Sensitive	10%	A
Refused	3%	C

Notes. A total of 604 of 607 respondents answered this question.

Table 26

e. Content of your email messages

Answer	Percentage	Code
Very Sensitive	52%	B
Somewhat Sensitive	25%	B
Not Too Sensitive	13%	A
Not at all Sensitive	7%	A
Refused	3%	C

Notes. A total of 604 of 607 respondents answered this question.

Table 27

f. Content of your text messages

Answer	Percentage	Code
Very Sensitive	49%	B
Somewhat Sensitive	26%	B
Not Too Sensitive	13%	A
Not at all Sensitive	8%	A
Refused	4%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 28

g. Content of your phone conversations

Answer	Percentage	Code
Very Sensitive	54%	B
Somewhat Sensitive	27%	B
Not Too Sensitive	13%	A
Not at all Sensitive	4%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 29

Question 7. (sp9) Some people aren't too worried about privacy today and others are concerned about privacy. We'd like to know how you feel about the topic. For each of the following statements please indicate the degree to which you agree or disagree.

a. It is easy for me to be anonymous online

Answer	Percentage	Code
Strongly Agree	3%	A
Agree	20%	A
Disagree	52%	B
Strongly Disagree	22%	B
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 30

b. I am willing to share some information about myself with companies in order to use online services for free

Answer	Percentage	Code
Strongly Agree	4%	A
Agree	51%	A
Disagree	31%	B
Strongly Disagree	11%	B
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 31

Question 8. (sp9) f. When I meet new people, I assume that they might search for information about me on the internet

Answer	Percentage	Code
Strongly Agree	10%	B
Agree	37%	B
Disagree	40%	A
Strongly Disagree	11%	A
Refused	3%	C

Notes. A total of 604 of 607 respondents answered this question.

Table 32

Question 9. (sp9) If inaccurate information about me got posted online, it would be very difficult to get it removed

Answer	Percentage	Code
Strongly Agree	39%	B
Agree	49%	B
Disagree	9%	A
Strongly Disagree	1%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 33

Question 10. (sp9) It is a good thing for society if people believe that someone is keeping an eye on things that they do online

Answer	Percentage	Code
Strongly Agree	7%	A
Agree	29%	A
Disagree	42%	B
Strongly Disagree	20%	B
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 34

Question 11. (sp9) American citizens should be concerned about the government's monitoring of phone calls and internet communications

Answer	Percentage	Code
Strongly Agree	40%	B
Agree	39%	B
Disagree	16%	A
Strongly Disagree	2%	A
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

Table 35

Question 12. (sp10) How concerned are you, if at all, that some of the information you share on social networking sites might be accessed by third party advertisers or businesses without your knowledge?

Answer	Percentage	Code
Very concerned	35%	B
Somewhat concerned	45%	B
Not too concerned	17%	A
Not at all concerned	2%	A
No answer	1%	C

Notes. A total of 399 respondents answered this question.

Table 36

Question 13. (sp11) How concerned are you, if at all, that some of the information you share on social networking sites might be accessed by the government without your knowledge?

Answer	Percentage	Code
Very concerned	37%	B
Somewhat concerned	34%	B
Not too concerned	25%	A
Not at all concerned	4%	A
No answer	0%	C

Notes. A total of 399 respondents answered this question.

Table 37

Question 14 (sp17). How much, if anything, have you heard about the government collecting information about telephone calls, emails and other online communications as part of efforts to monitor terrorist activity?

Answer	Percentage	Code
A lot	43%	A
A little	44%	A
Nothing at all	5%	B
Don't know	6%	C
Refused	2%	C

Notes. A total of 605 of 607 respondents answered this question.

The following data were obtained from Survey 2.

Table 38

Question 15: (sp3) *Let's think about a typical day in your life as you spend time at home, outside your home, and getting from place to place. You use your cellphone and maybe landline phones. You may use credit cards. You might go online and buy things, use search engines, watch videos, or check in on social media. As you go through a typical day, how much control do you feel you have over how much information is collected about you and how it is being used?*

Answer	Percentage	Code
A lot of control	9%	A
Some control	38%	A
Not much control	37%	B
No control at all	13%	B
Refused	3%	C

Notes. A total of 495 of 498 respondents answered this question.

Table 39

Question 16: (sp7) *How much, if anything, have you heard about the government collecting information about telephone calls, emails and other online communications as part of the efforts to monitor terrorist activity?*

Answer	Percentage	Code
A lot	32%	A
A little	48%	A
Nothing at all	7%	B
Don't know	6%	C
Refused	2%	C

Notes. A total of 496 of 498 respondents answered this question.

Table 40

Question 17: (sp27) *Overall, do you approve or disapprove of the government's collection of telephone and internet data as part of anti-terrorism efforts?*

Answer	Percentage	Code
Approve	32%	A
Disapprove	40%	B
Don't know	26%	C
Refused	2%	C

Notes. A total of 496 of 498 respondents answered this question.

Table 41

Question 18: (sp28) *Thinking about the data the government collects a part of anti-terrorism efforts… Do you think there are adequate limits on what telephone and internet data the government can collect, or not?*

Answer	Percentage	Code
Yes, there are adequate limits on what government can collect	31%	A
No, there are adequate limits on what government can collect	65%	B
No answer	4%	C

Notes. A total of 494 of 498 respondents answered this question.

Table 42

Question 19: (sp9) *Have you changed your internet or cell phone use in recent months in any way to avoid having your activities tracked or noticed, or haven't you done this?*

Answer	Percentage	Code
Yes	7%	B
No	91%	A
Refused	3%	C

Notes. A total of 495 of 498 respondents answered this question.

Table 43

Question 20: (sp11) *While using the internet, have you ever done any of the following?*

Answer/ Code	Yes A	No B	Does not apply to me C	Don't know C	Refused C
a. Used a temporary username or email address	25	56	9	5	3
b. Added a privacy enhancing browser plugin like DoNotTrackMe or Privacy Badger	9	72	8	8	3
c. Given inaccurate or misleading information about yourself	24	60	7	6	3
d. Set your browser to disable or turned off cookies	34	43	8	12	3
e. Cleared cookies and browser history	59	22	7	8	3
f. Used a service that allows you to browse the web anonymously, such as a proxy server, Tor software, or VPN	9	67	9	10	4
g. Encrypted your phone calls, text messages or email	10	68	10	10	3
h. Decided not to use a website because they asked for you real name	23	55	12	7	3
i. Deleted or edited something you posted in the past	29	46	14	8	3
j. Asked someone to remove something posted about you	11	63	15	7	3

k.	Used a public computer to browse anonymously	12	68	12	6	3
l.	Used a search engine that doesn't keep track of your search history	15	52	11	19	3
m.	Refused to provide information about yourself that wasn't relevant to the transaction	57	23	9	8	3

Notes. A total of 495 of 498 respondents answered this question.

Table 44

Question 21: (sp12) *Do you think people should have the ability to use the internet completely anonymously for certain kinds of online activities?*

Answer	Percentage	Code
Yes	55	B
No	16	A
Don't know	27	C
Refused	2	C

Notes. A total of 496 of 498 respondents answered this question.

The following data were obtained from Survey 3.

Table 45

Question 22: (sp7) *When an app on your smartphone or tablet seeks your permission to use your location, how often do you allow it to use your location?*

Answer	Percentage	Code
Frequently	22	A
Sometimes	36	A
Hardly ever	28	B
Never	11	B
Refused / not asked	3	C

Notes. A total of 317 of 320 respondents answered this question.

Table 46

Question 23: (sp9) *Which of these statements accurately describes you?*

Answer	Percentage	Code
I am generally a private person and like to keep to myself	65	B
I am generally an open person who enjoys sharing with others	34	A
Refused	1	C

Notes. A total of 474 of 475 respondents answered this question.

Table 47

Question 24: (sp10) *How much, if anything, have you heard about the government collecting information about telephone calls, emails and other online communications as part of the efforts to monitor terrorist activity?*

Answer	Percentage	Code
A lot	31	A
A little	56	A
Nothing at all	6	B
Don't know	6	C
Refused	1	C

Notes. A total of 474 of 475 respondents answered this question.

Table 48

Question 25: (sp12) *In your opinion, is it acceptable or unacceptable for the American government to monitor communications from individuals suspected of terrorist activities?*

Answer	Percentage	Code
Acceptable	82	A
Unacceptable	15	B
Refused	2	C

Notes. A total of 473 of 475 respondents answered this question.

Table 49

Question 26: (sp13) *In your opinion, is it acceptable or unacceptable for the American government to monitor communications from American leaders?*

Answer	Percentage	Code
Acceptable	60	A
Unacceptable	38	B
Refused	2	C

Notes. A total of 473 of 475 respondents answered this question.

Table 50

Question 27: (sp14) *In your opinion, is it acceptable or unacceptable for the American government to monitor communications from American citizens?*

Answer	Percentage	Code
Acceptable	40	A
Unacceptable	57	B
Refused	3	C

Notes. A total of 472 of 475 respondents answered this question.

Table 51

Question 28: (sp15) *In your opinion, is it acceptable or unacceptable for the American government to monitor communications from citizens of other countries?*

Answer	Percentage	Code
Acceptable	54	A
Unacceptable	44	B
Refused	2	C

Notes. A total of 473 of 475 respondents answered this question.

Table 52

Question 29: (sp16) *In your opinion, is it acceptable or unacceptable for the American government to monitor communications from leaders of other countries?*

Answer	Percentage	Code
Acceptable	60	A
Unacceptable	37	B
Refused	3	C

Notes. A total of 472 of 475 respondents answered this question.

Table 53

Question 30: (sp17) *Overall, how concerned are you about government surveillance of American's data and electronic communications?*

Answer	Percentage	Code
Very concerned	17	B
Somewhat concerned	35	B
Not very concerned	33	A
Not at all concerned	13	A
Refused	2	C

Notes. A total of 473 of 475 respondents answered this question.

Table 54

Question 31: (sp20) *Do you generally think the courts and judges do a good job balancing the public's right to privacy and the needs of law enforcement and intelligence agencies to collect information for investigations?*

Answer	Percentage	Code
Yes	48	A
No	49	B
Refused	3	C

Notes. A total of 472 of 475 respondents answered this question.

Table 55

Question 32: (sp21) *How concerned are you about government monitoring of your activity on social media websites such as Facebook or Twitter?*

Answer	Percentage	Code
Very concerned	14	B
Somewhat concerned	17	B
Not very concerned	24	A
Not at all concerned	24	A
Not applicable	19	C

Notes. A total of 454 of 475 respondents answered this question.

Table 56

Question 33: (sp22) *How concerned are you about government monitoring of your activity on search engines?*

Answer	Percentage	Code
Very concerned	15	B
Somewhat concerned	24	B
Not very concerned	30	A
Not at all concerned	23	A
Not applicable	5	C

Notes. A total of 468 of 475 respondents answered this question.

Table 57

Question 34: (sp24) *How concerned are you about government monitoring of your activity on your cell phone?*

Answer	Percentage	Code
Very concerned	17	B
Somewhat concerned	20	B
Not very concerned	30	A
Not at all concerned	24	A
Not applicable	7	C

Notes. A total of 465 of 475 respondents answered this question.

Table 58

Question 35: (sp26) *How concerned are you about government monitoring of your activity on your mobile apps?*

Answer	Percentage	Code
Very concerned	12	B
Somewhat concerned	17	B
Not very concerned	28	A
Not at all concerned	22	A
Not applicable	19	C

Notes. A total of 453 of 475 respondents answered this question.

Table 59

Question 36: (sp27) *How concerned are you about government monitoring of your activity on your email?*

Answer	Percentage	Code
Very concerned	19	B
Somewhat concerned	19	B
Not very concerned	31	A
Not at all concerned	23	A
Not applicable	4	C

Notes. A total of 468 of 475 respondents answered this question.

Table 60

Question 37: (sp29) *Since learning about U.S. phone and internet monitoring, how much, if at all, would you say you have changed the way you use any of the following?*

Answer/ Code	A great deal B	Somewhat B	Not much A	Not at all A	Not applicable C	Refused C
a. Social media like Twitter	7	7	18	45	22	1
b. Search engines	7	10	23	56	4	1
c. Your landline phone	5	4	17	51	23	<1
d. Your cell phone	7	7	23	57	5	1
e. Text messages	7	6	19	53	15	0
f. Mobile apps	8	6	17	49	21	<1
g. Your email accounts	8	10	23	57	2	1

Notes. A total of 417 respondents answered this question.

Table 61

Question 38: (sp32) *Since learning about the government's phone and internet monitoring programs, have you done any of the following in an effort to hide or shield your information from the government?*

Answer	I have done this	I have not done this, but have considered it	I have not done this and have not considered it	Not applicable	Refused
Code	B	A	A	C	C
a. Unfriended or unfollowed people on social media	13	8	52	26	1
b. Deleted social media accounts	8	9	58	24	1
c. Used social media less often	15	9	50	24	<1
d. Changed your privacy settings on social media	17	10	47	24	1
e. Made more phone calls instead of communicating online	8	10	70	11	1
f. Avoided using certain terms in online communications	13	10	67	9	1
g. Avoided certain apps	15	6	56	22	1

h.	Uninstalled certain apps	13	5	57	25	1
i.	Used pseudonyms	8	6	68	16	1
j.	Not used certain terms in search engine queries you thought might trigger scrutiny	11	13	64	11	1
k.	Spoke more in person instead of communicating online or over the phone	14	9	67	9	1

Notes. A total of 417 respondents answered this question.

Table 62

Question 39: (sp35) *Since learning about U.S. phone and internet monitoring, have you adopted any of the following tools or strategies to make your communications and activities more private?*

Answer	Have adopted this	Not adopted this, but have considered	I have not adopted this and have not considered	I don't know what this is	Not applicable to me	Refused
Code	B	A	A	C	C	C
a. Used a search engine that doesn't keep track of your search history	10	12	53	13	12	1
b. Adopted email encryption, such as PGP	2	10	46	31	11	1
c. Adopted mobile encryption for calls or text messages	4	8	48	24	15	2
d. Used more complex passwords	25	12	48	6	8	1

e. Proxy servers	3	7	41	33	13	2
f. Privacy browser plug-ins	5	7	43	31	13	1
g. Anonymity software like Tor	2	5	40	39	13	1

Notes. A total of 417 respondents answered this question.

Table 63
Question 40: (sp37) *Is it acceptable or unacceptable for the government to monitor the communications of U.S. citizens if the person did the following?*

Answer/ Code	Acceptable A	Unacceptable B	Refused C
Visited a child pornography site	77	19	4
Was reported by a bank to be making unusual withdraws	51	45	4
Made search engine inquires for the keyword explosives and automatic weapons	65	30	4
Visited websites of known anti-American groups	67	29	4
Exchanged emails with an Imam who preached against infidels	68	28	4
Used encryption software to hide files	49	47	4

Notes. A total of 475 respondents answered this question.

The following data were obtained from Survey 4.

Table 64

Question 41: (sp1) *Privacy means different things to different people today. In thinking about all of your daily interactions—both online and offline—please tell me how important each of the following are to you*

Answer/ Code		Very important B	Somewhat B	Not very A	Not at all A	Not applicable C	Refused C
a.	Being in control of who can get information about you	74	19	3	1	1	2
b.	Not having someone watch you or listen to you without your permission	67	20	8	1	2	2
c.	Controlling what information is collected about you	65	25	5	1	1	3

d.	Having individuals in social and work situations not ask you things that are highly personal	44	36	13	2	4	2

Notes. A total of 461 respondents answered this question.

Appendix B: Figures

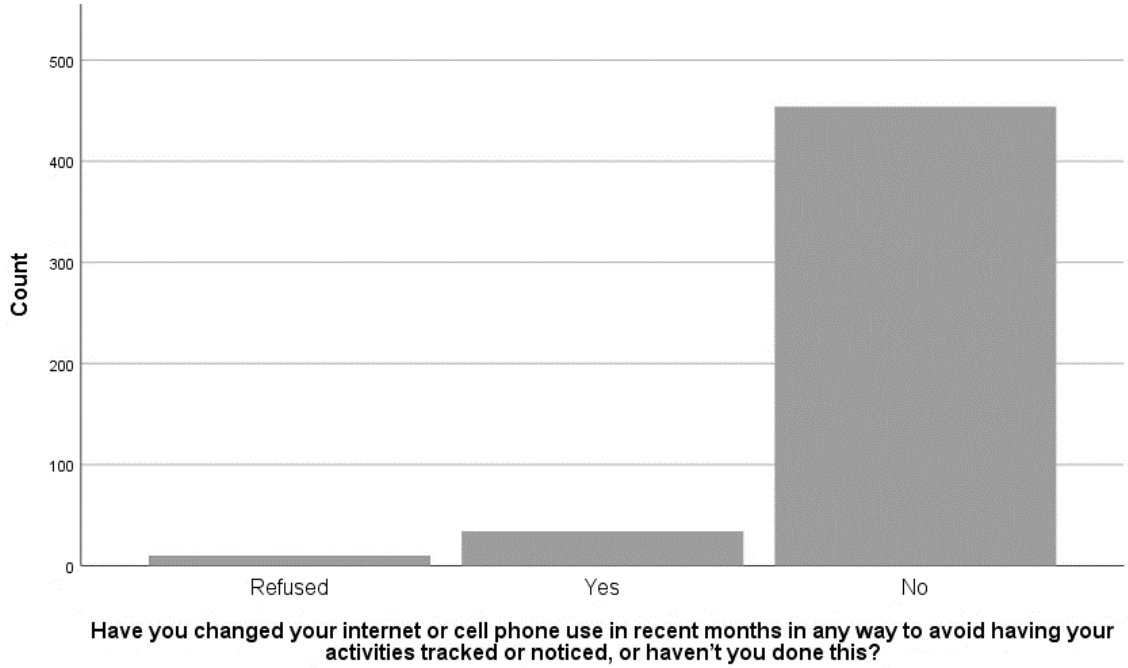


Figure B10. Question 19 (sp9)

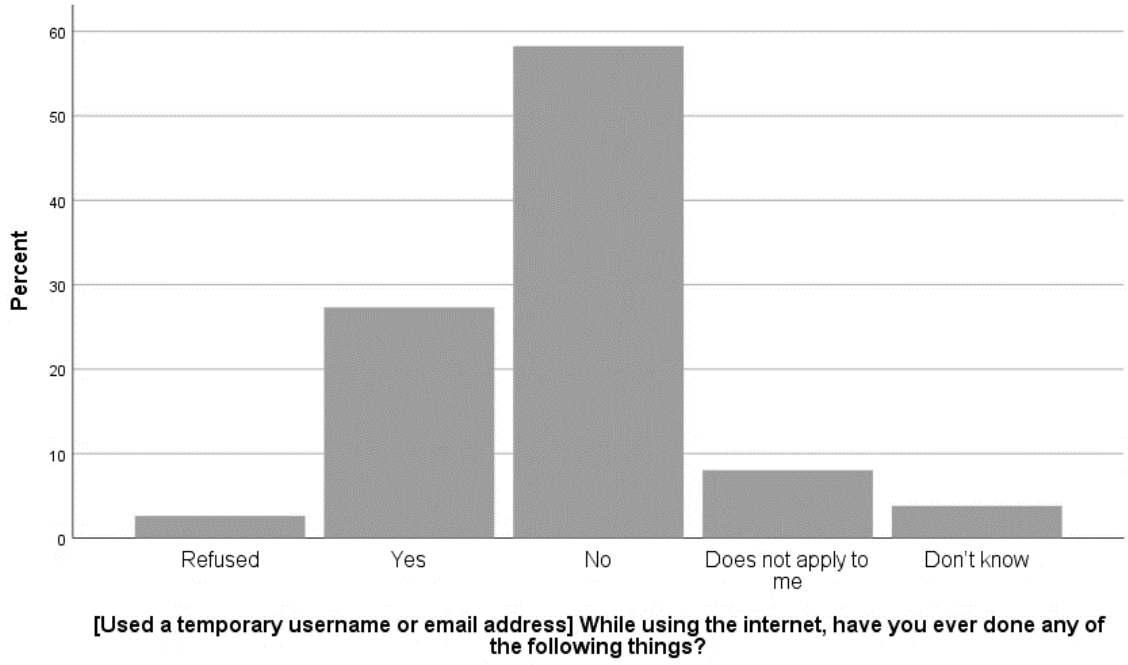


Figure B11. Question 20 (sp11) a

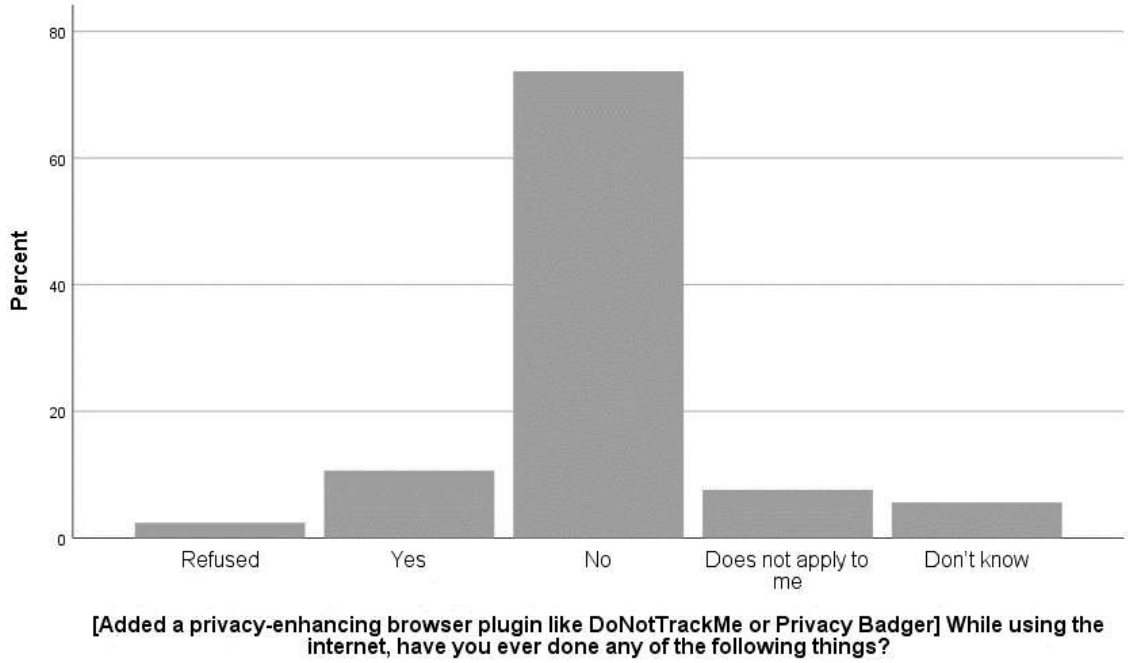


Figure B12. Question 20 (sp11) c

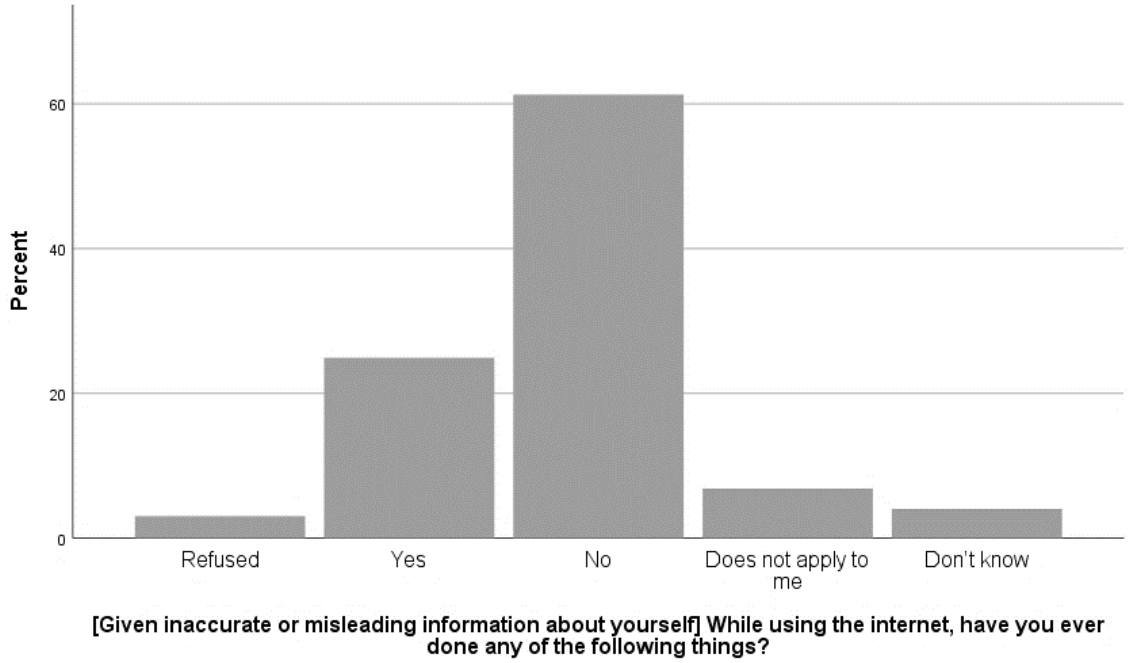


Figure B13. Question 20 (sp11) d

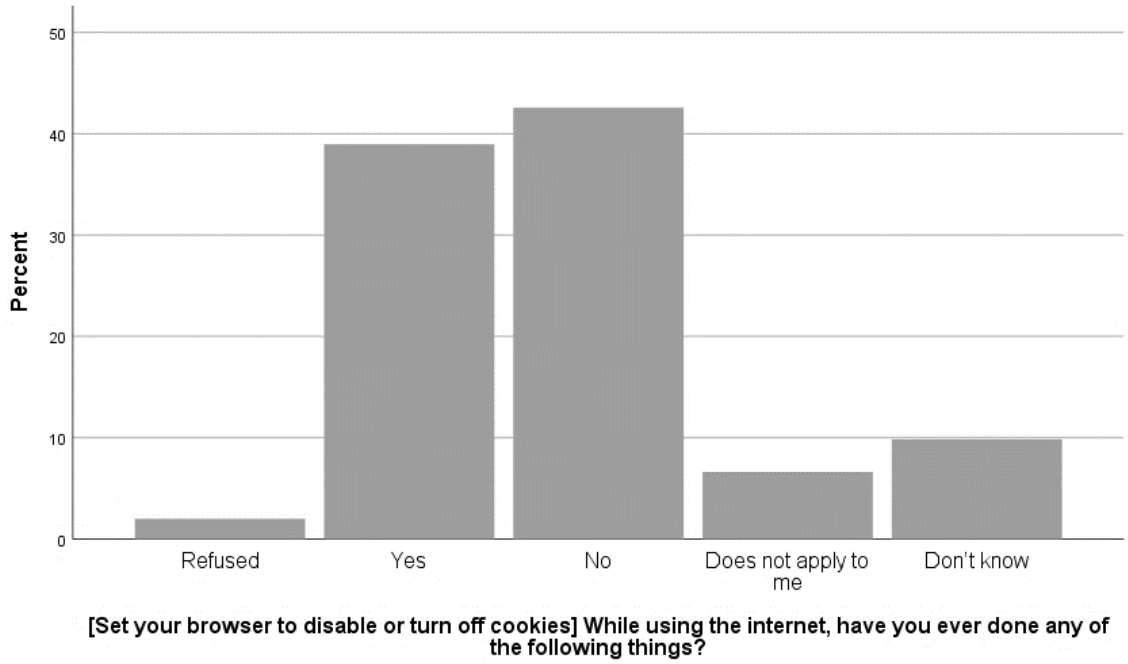
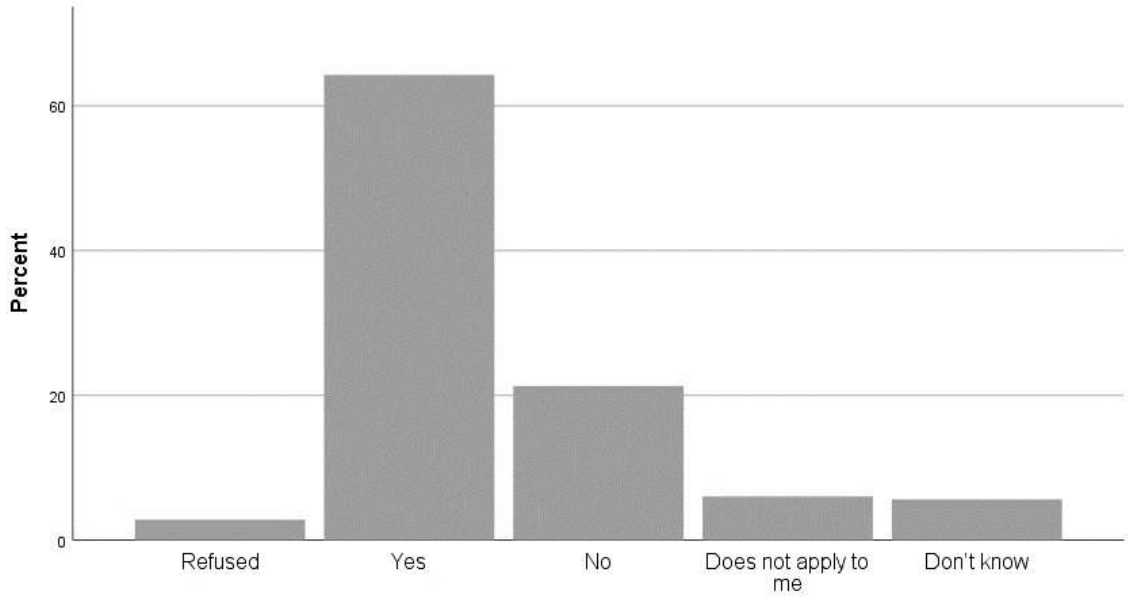


Figure B14. Question 20 (sp11) e



* the responses to this question appear to contraindicate the responses to the other questions in the same category. I believe this is due to the phrasing of the question; that is clearing cookies or browser history is not necessarily privacy related. Cyber professionals and computer system-health software routinely undertake these tasks for non-privacy related reasons.

Figure B15. Question 20 (sp11) f

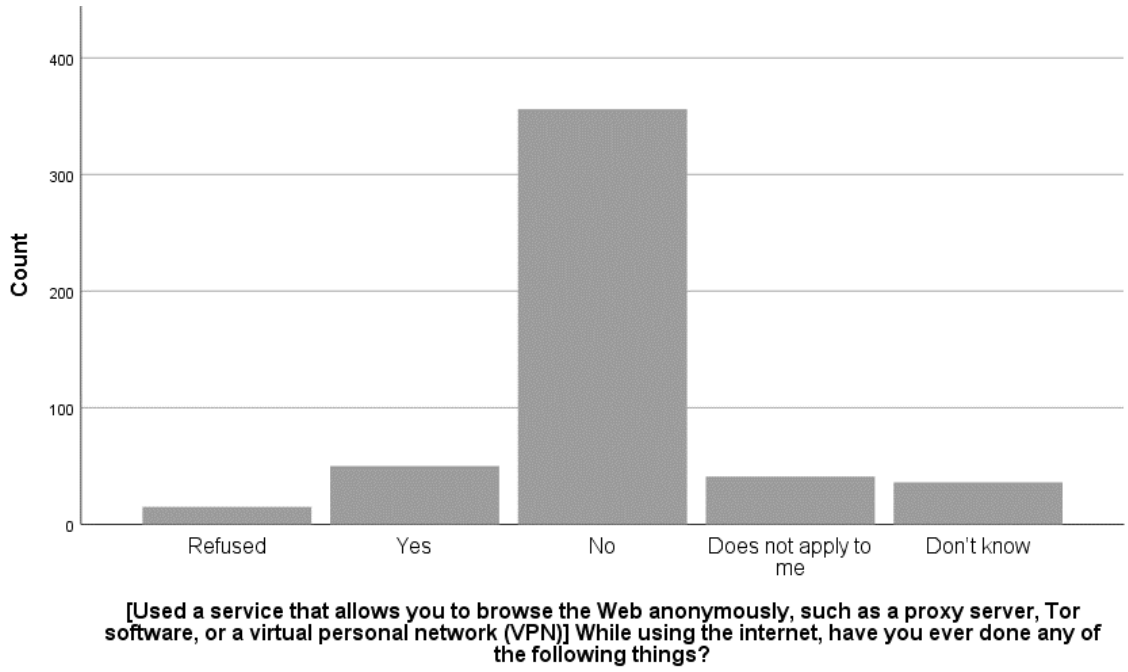


Figure B16. Question 20 (sp11) g

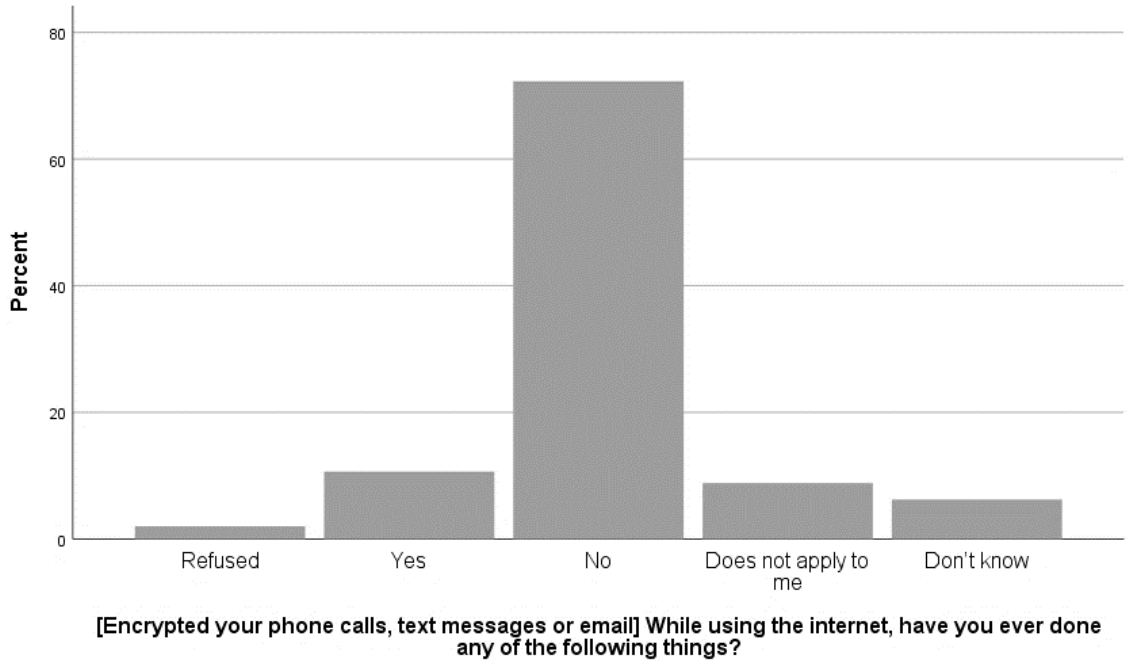


Figure B17. Question 20 (sp11) h

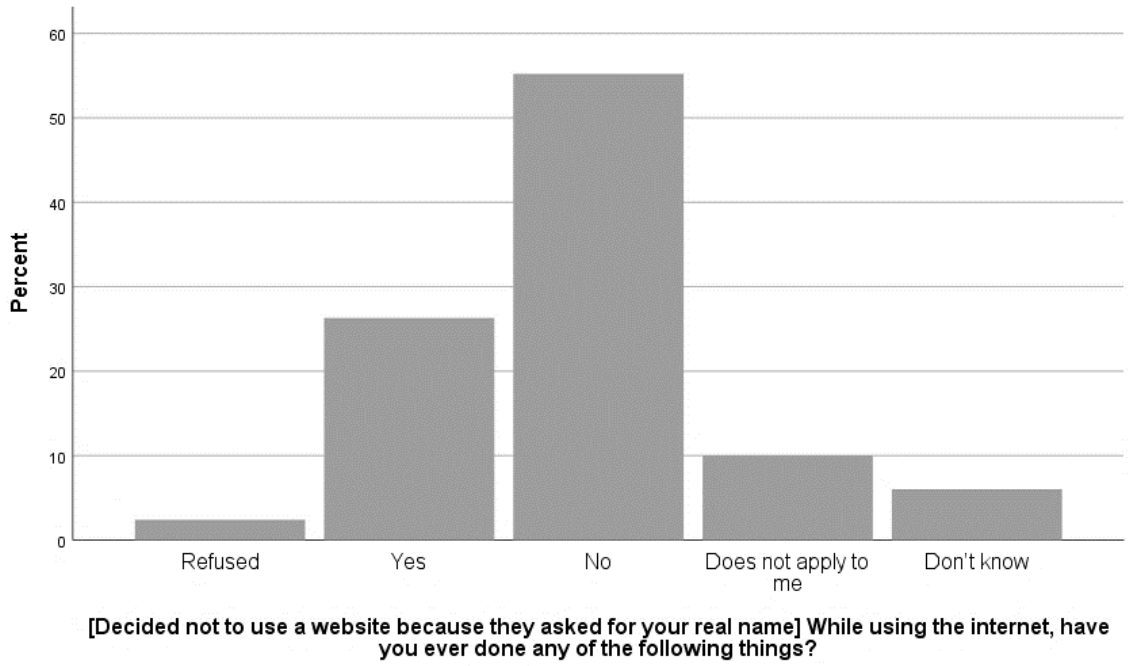


Figure B18. Question 20 (sp11) i

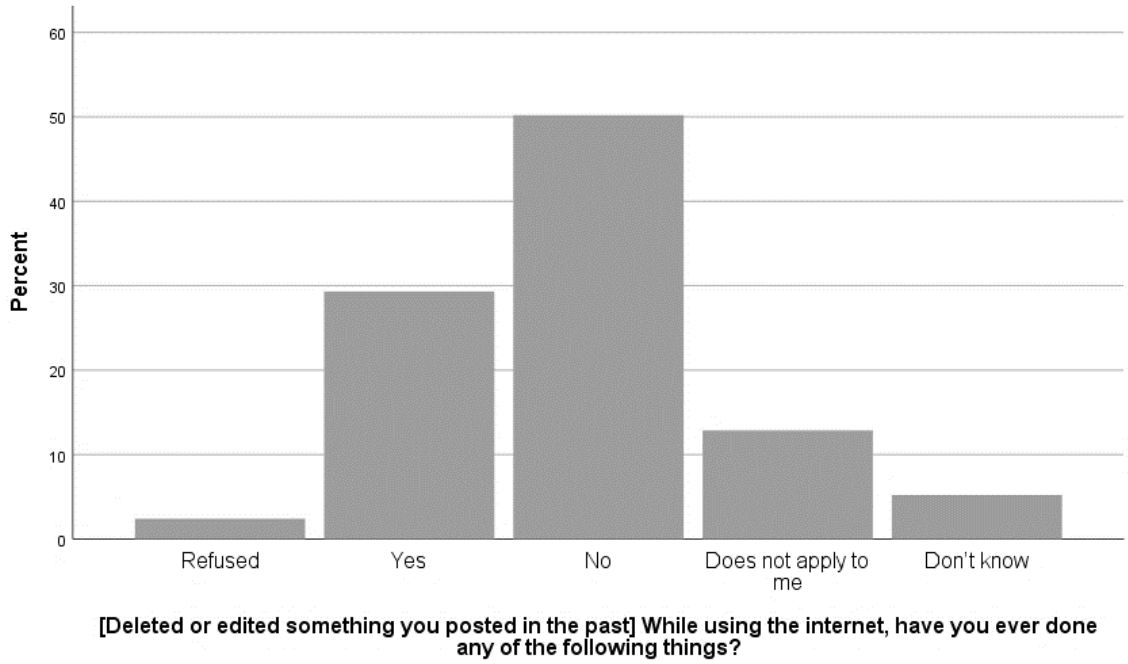


Figure B19. Question 20 (sp11) j

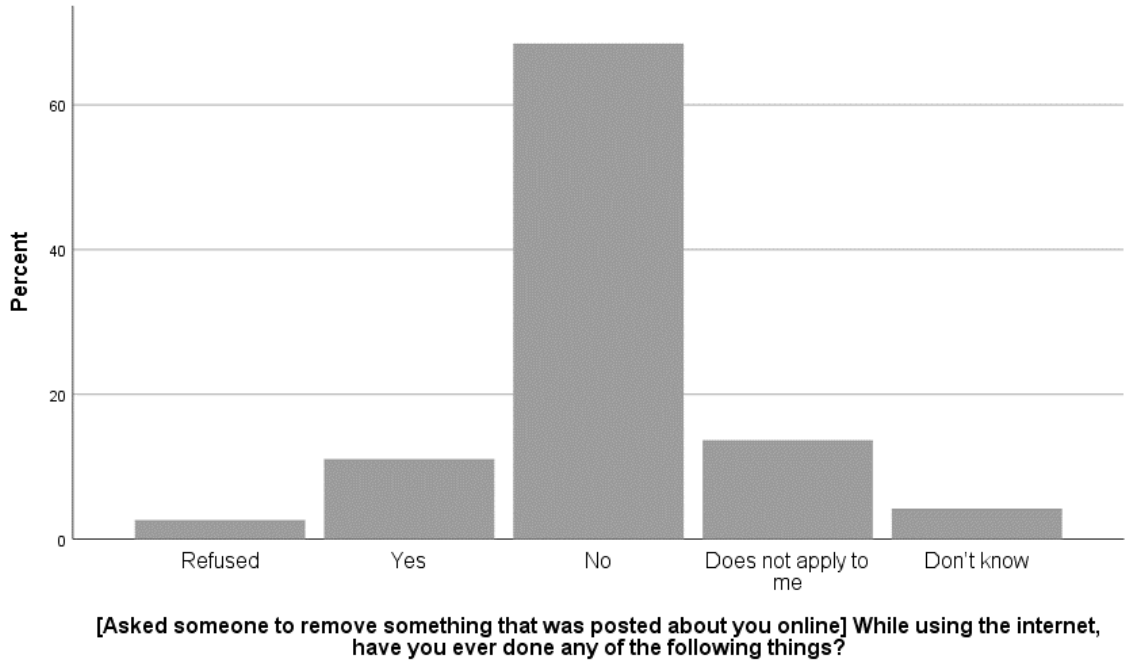


Figure b20. Question 20 (sp11) k

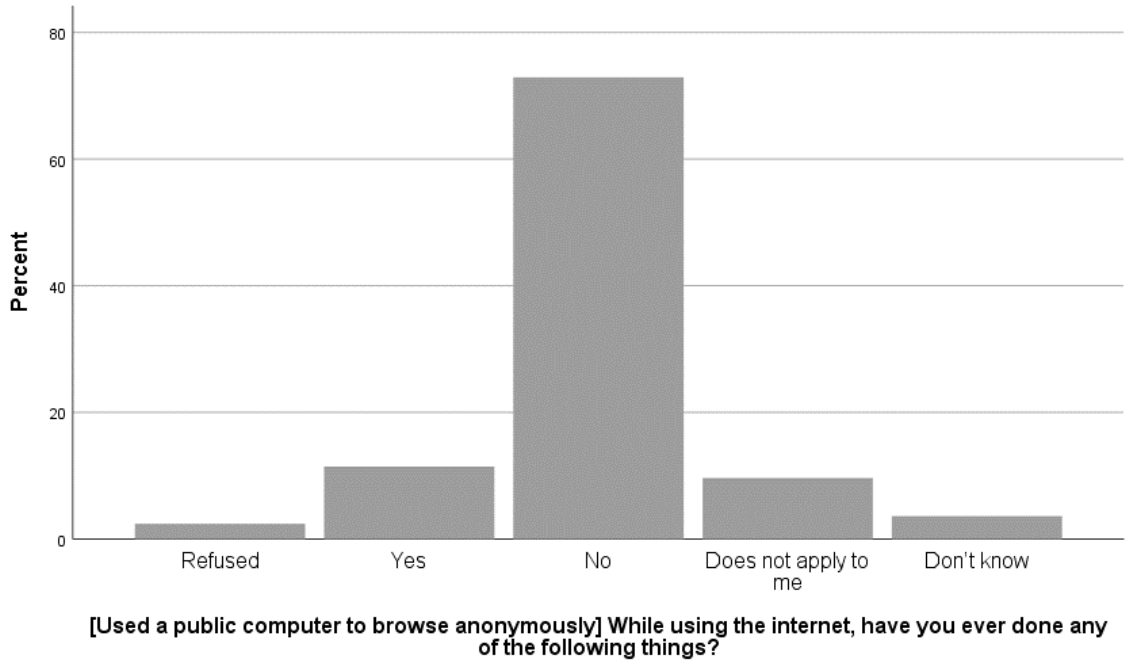


Figure B21. Question 20 (sp11) l.

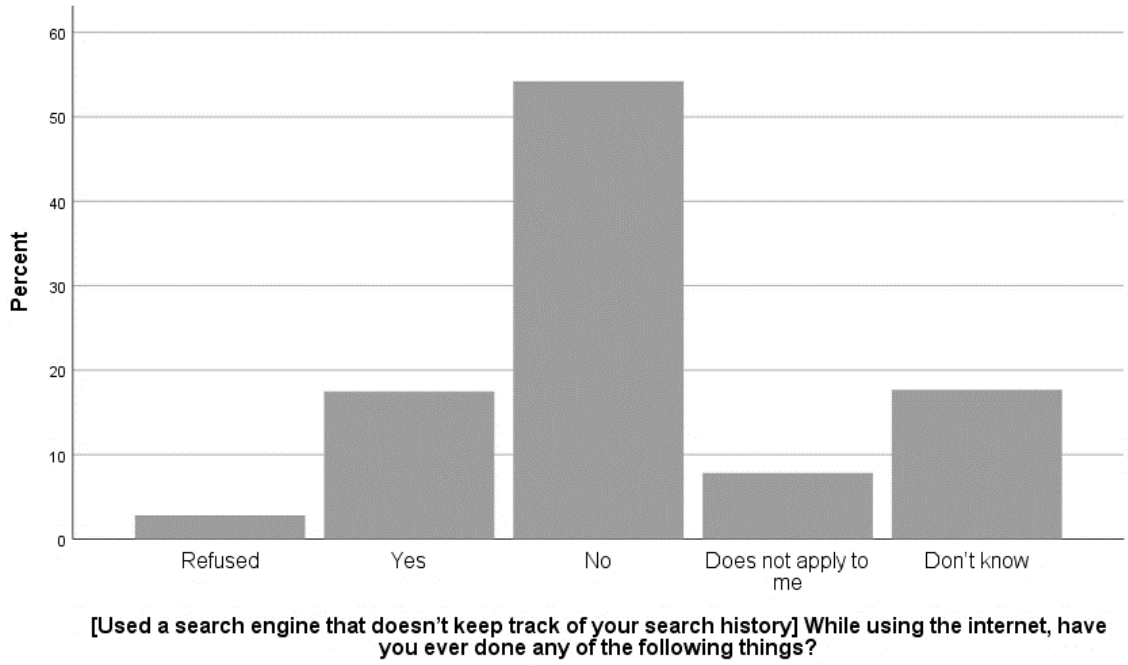


Figure B22. Question 20 (sp11) m

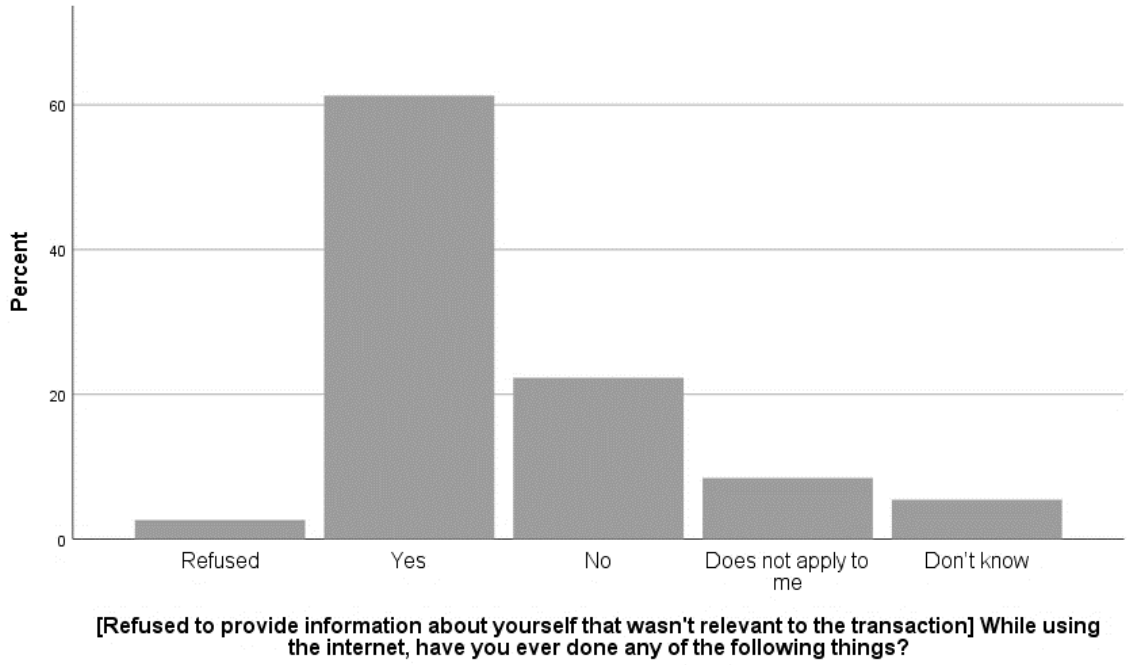


Figure B23. Question 37 (sp29) b. (contraindicative result could be due to the vagueness of the question phraseology and its implications for non-privacy related reasons)

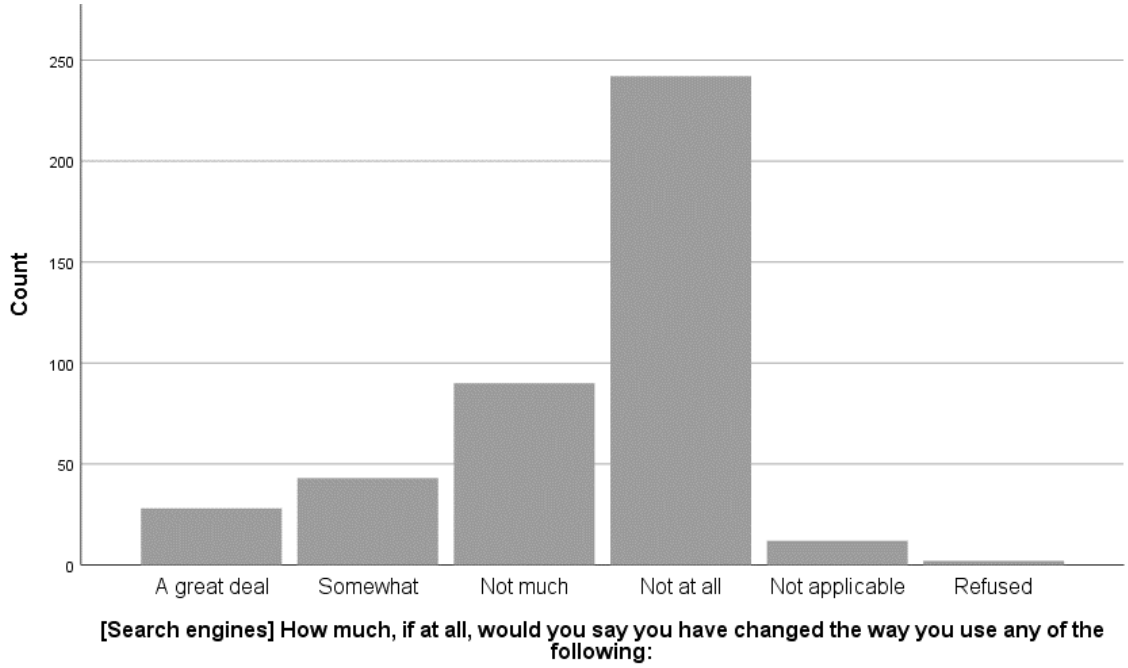


Figure B24. Question 37 (sp29) c.

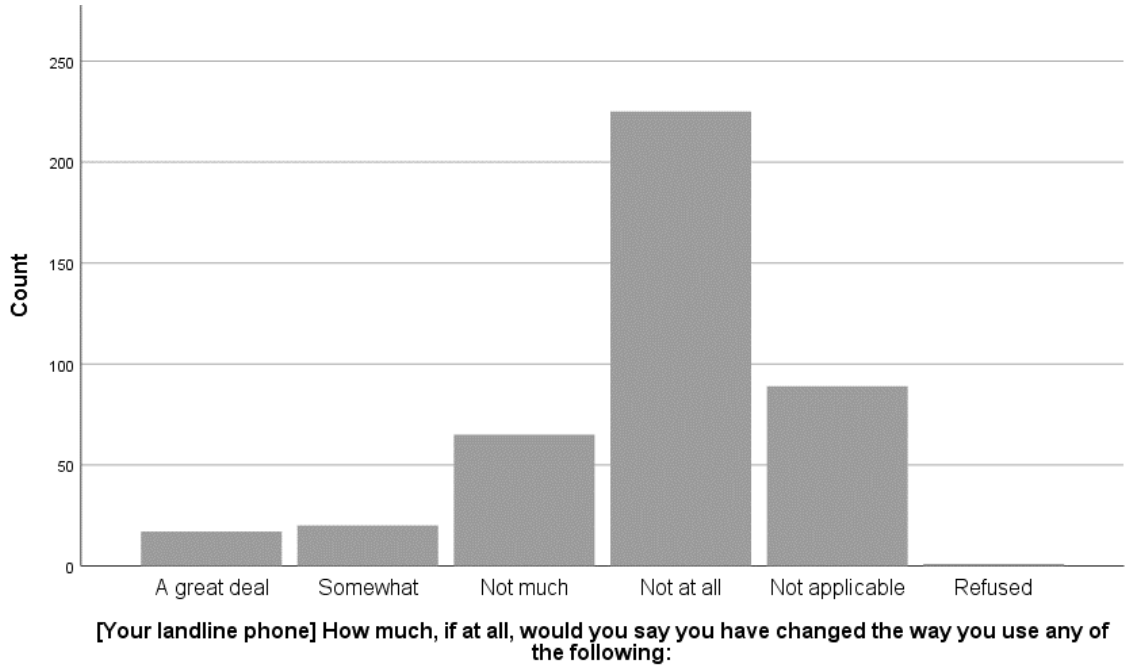


Figure B25. Question 37 (sp29) d.

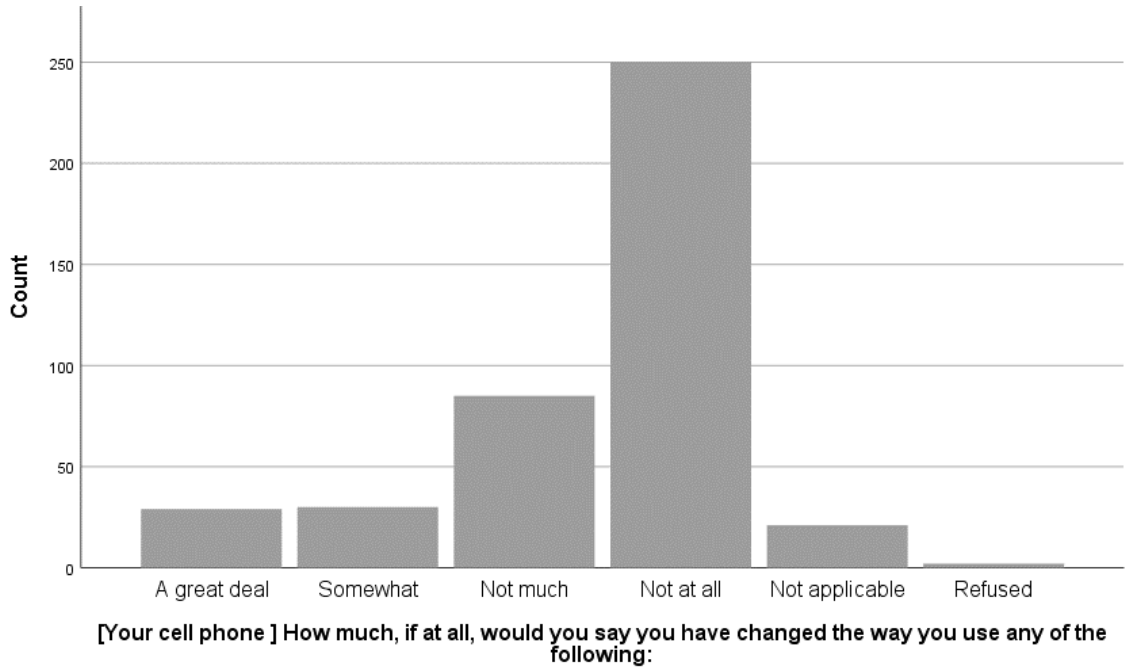


Figure B26. Question 37 (sp29) e.

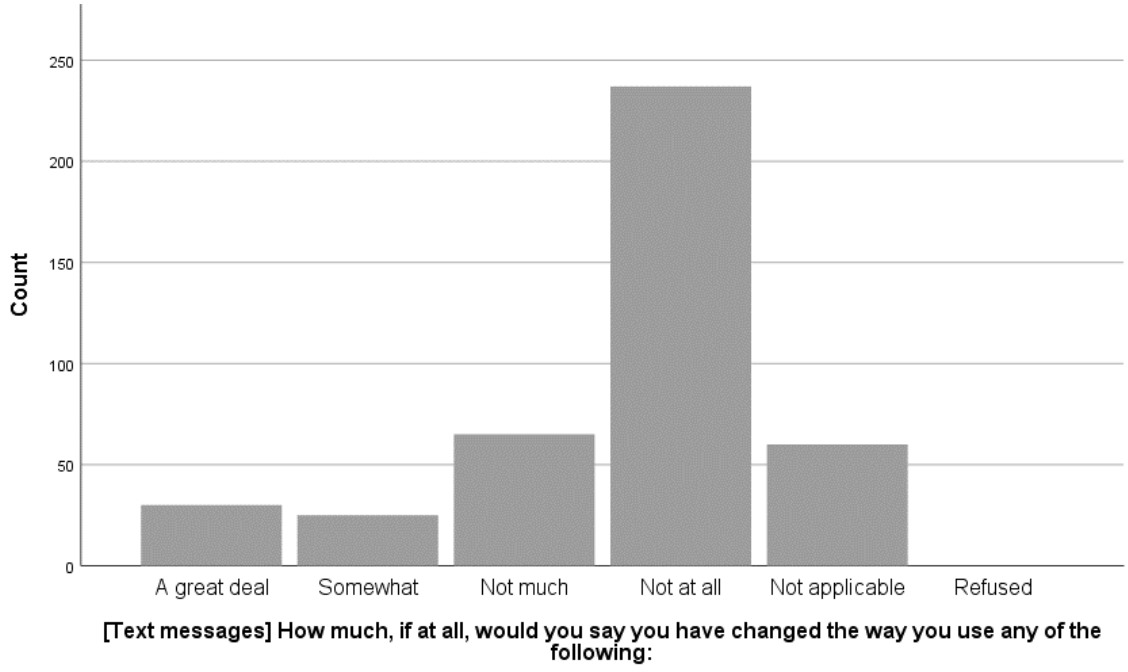


Figure B27. Question 37 (sp29) f.

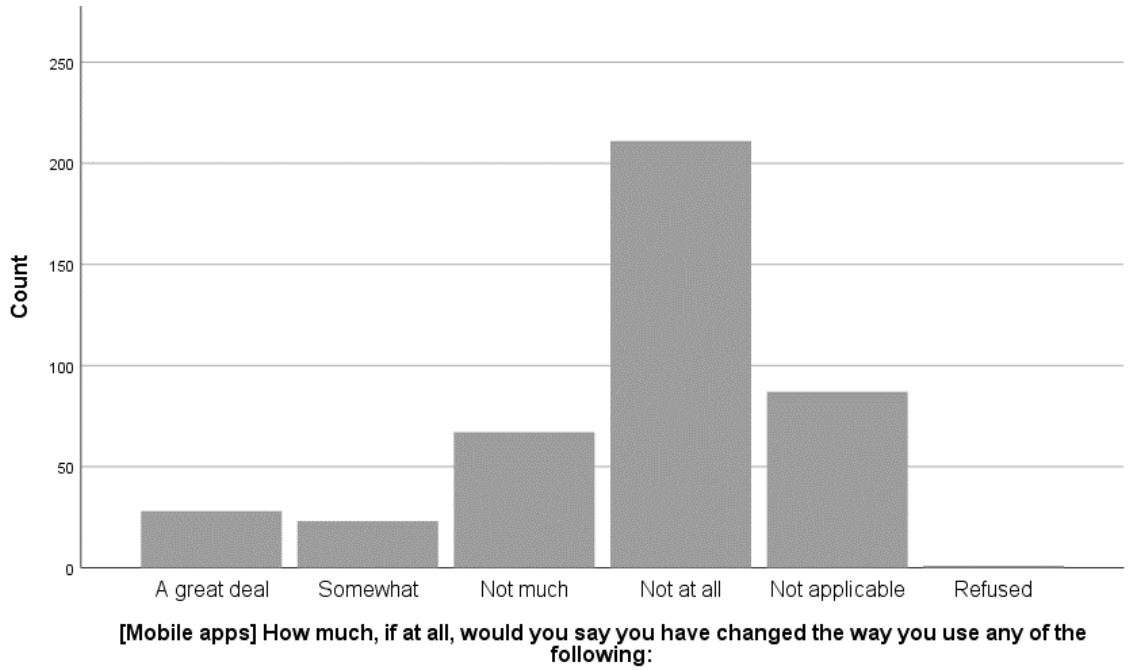


Figure B28. Question 37 (sp29) g.

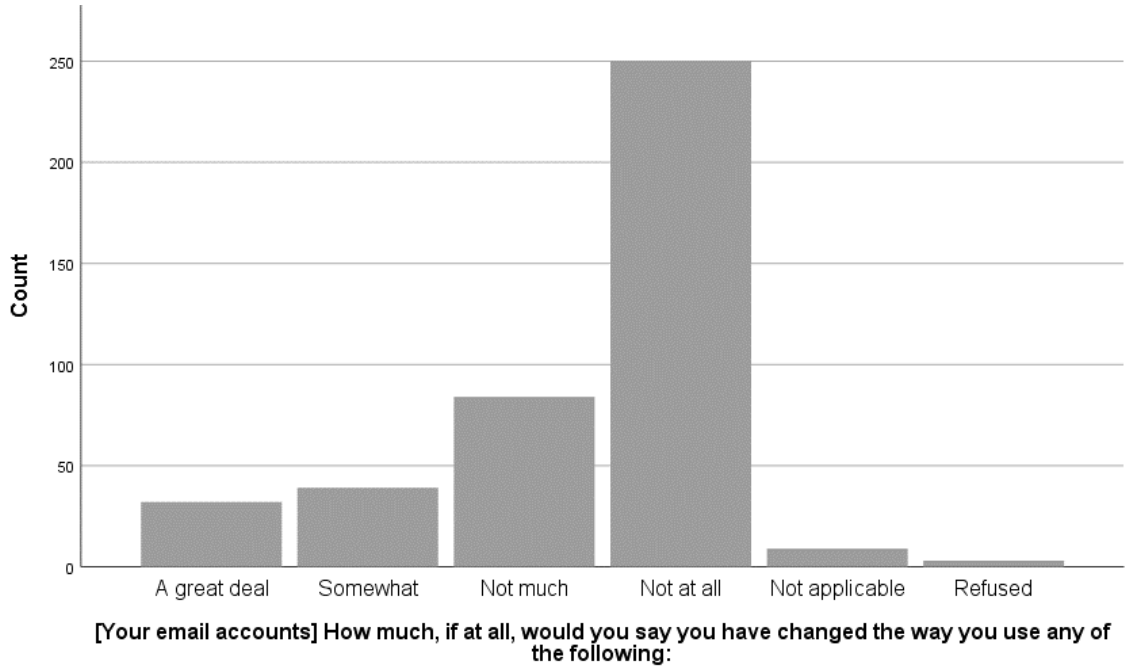


Figure B29. Question 38 (sp32) a.

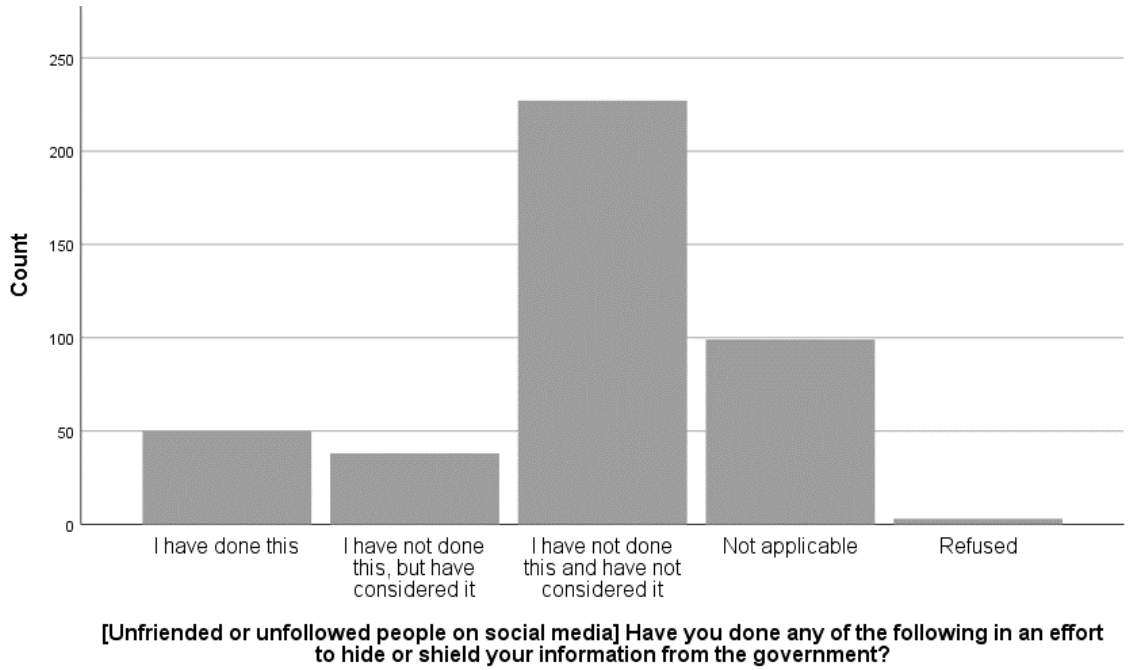


Figure B30. Question 38 (sp32) b.

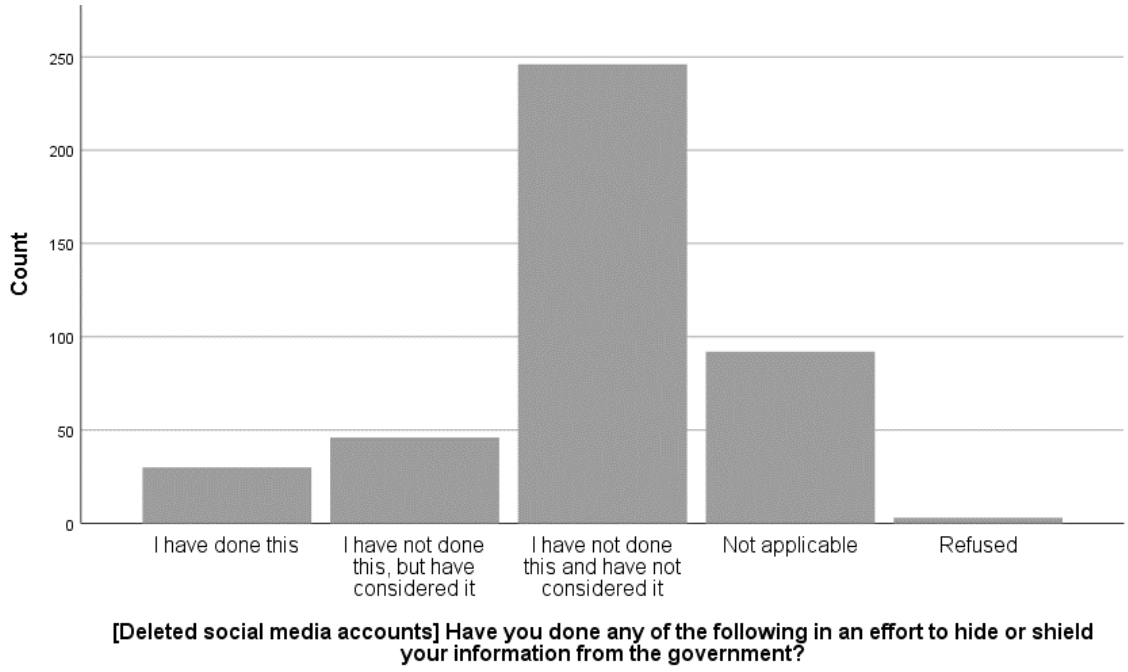


Figure B31. Question 38 (sp32) f.

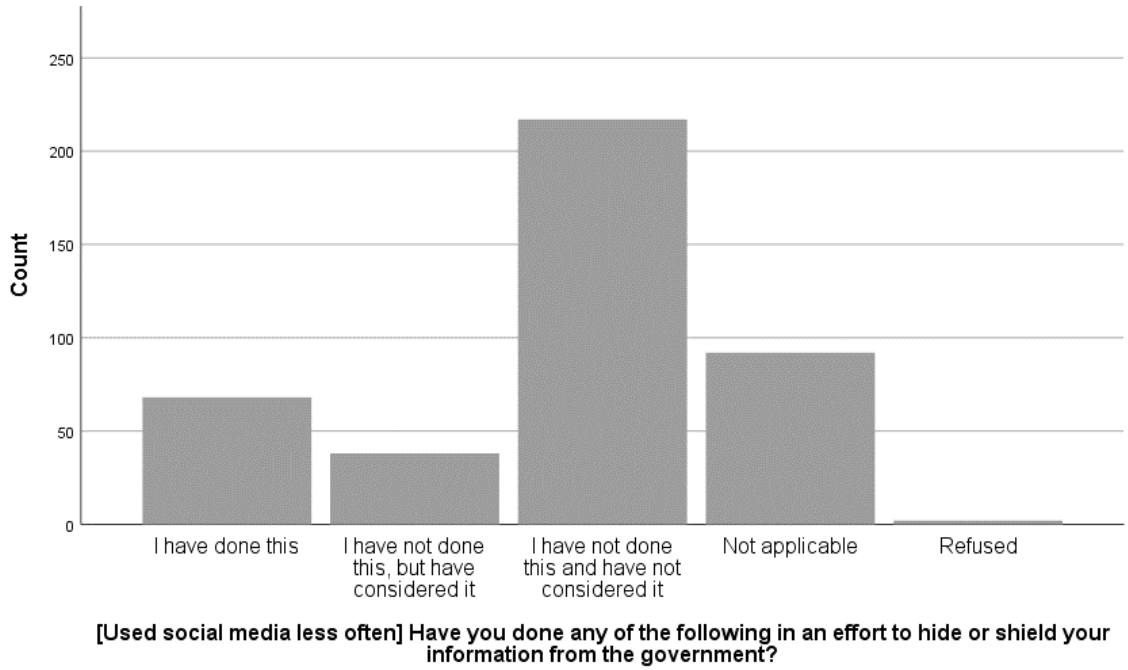


Figure B32. Question 38 (sp32) d.

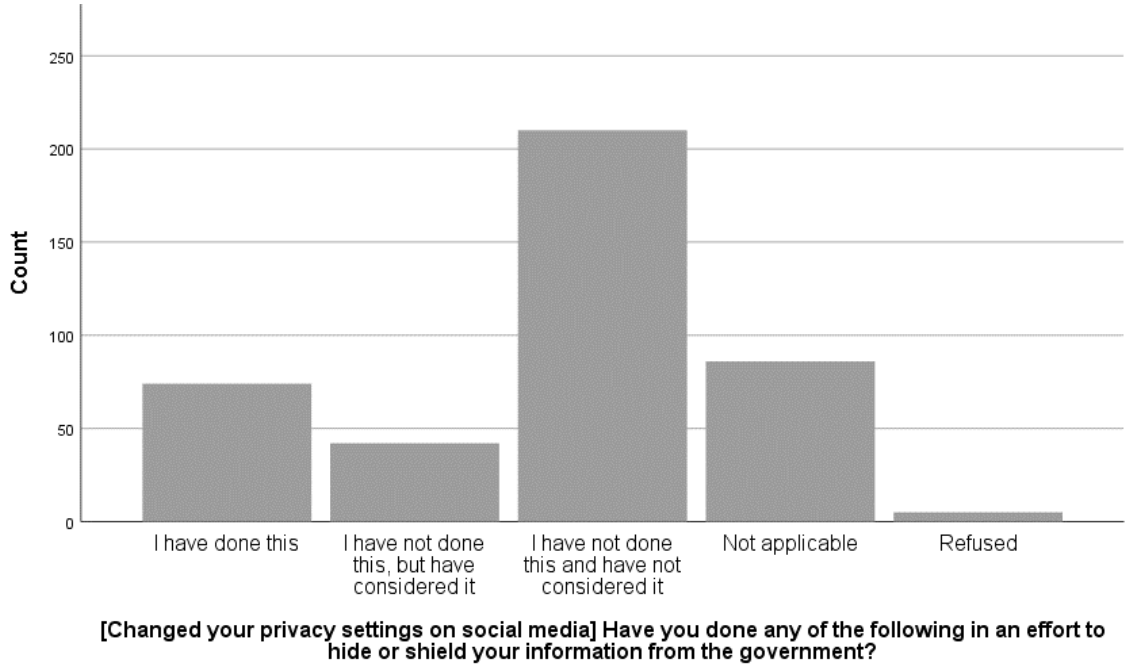


Figure B33. Question 38 (sp32) e.

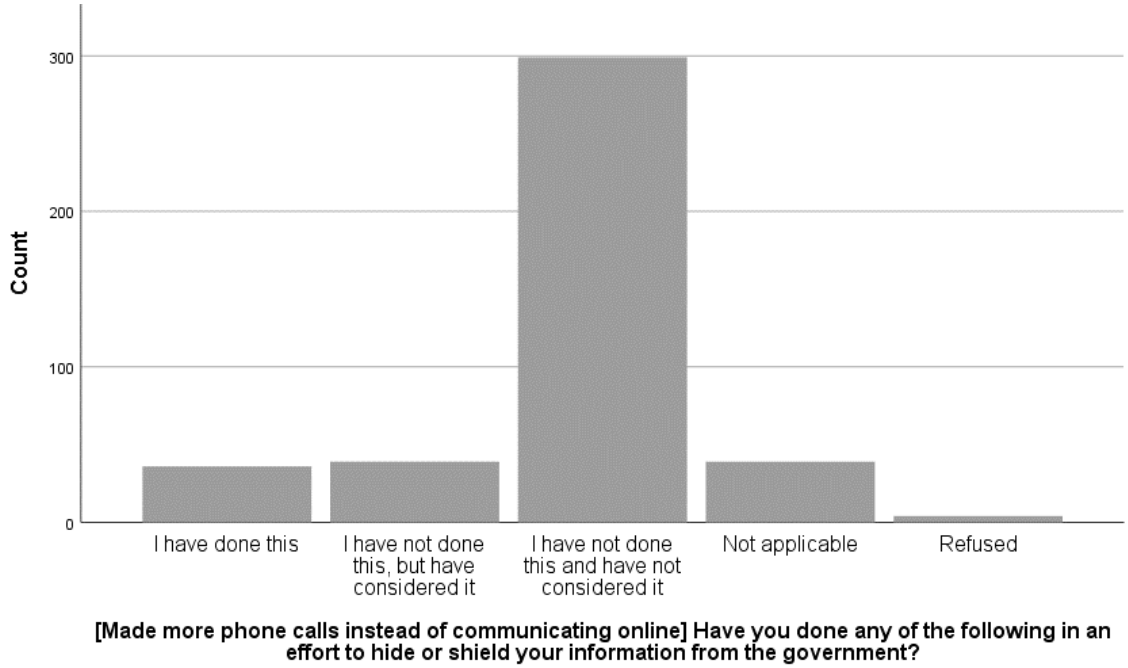


Figure B34. Question 38 (sp32) f.

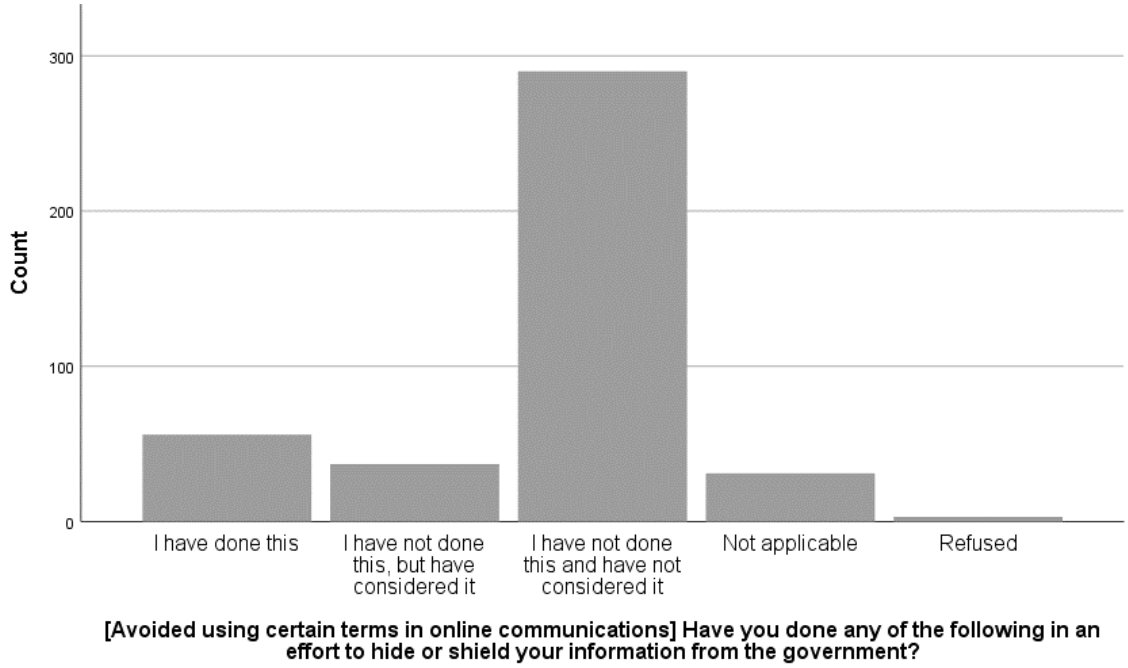


Figure B35. Question 38 (sp32) g.

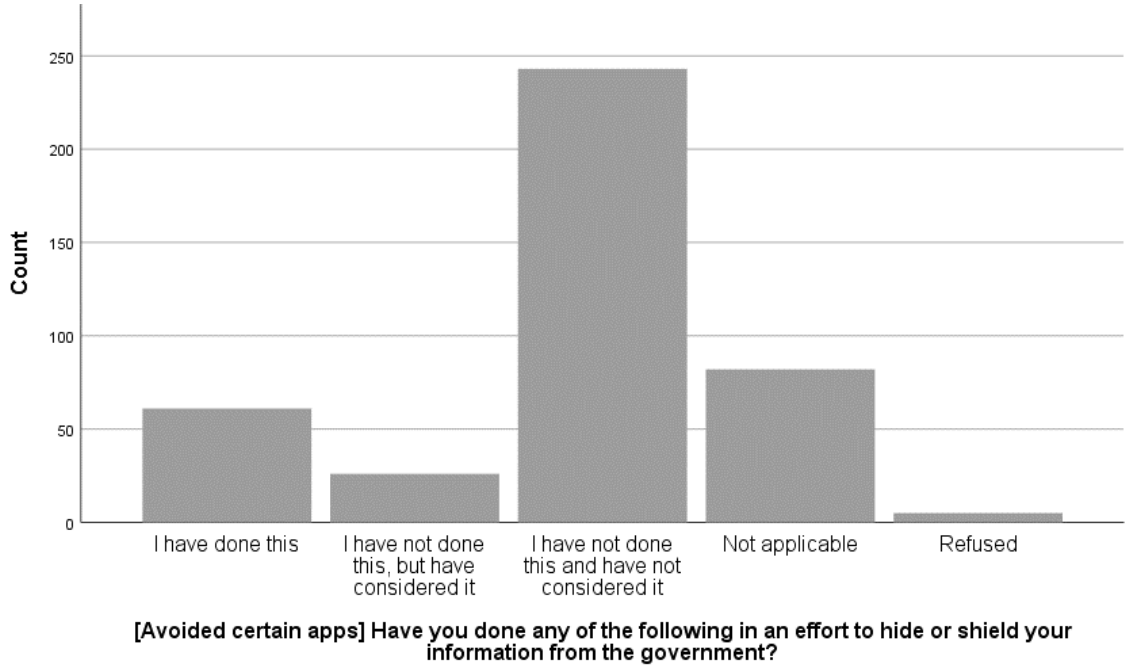


Figure B36. Question 38 (sp32) h.

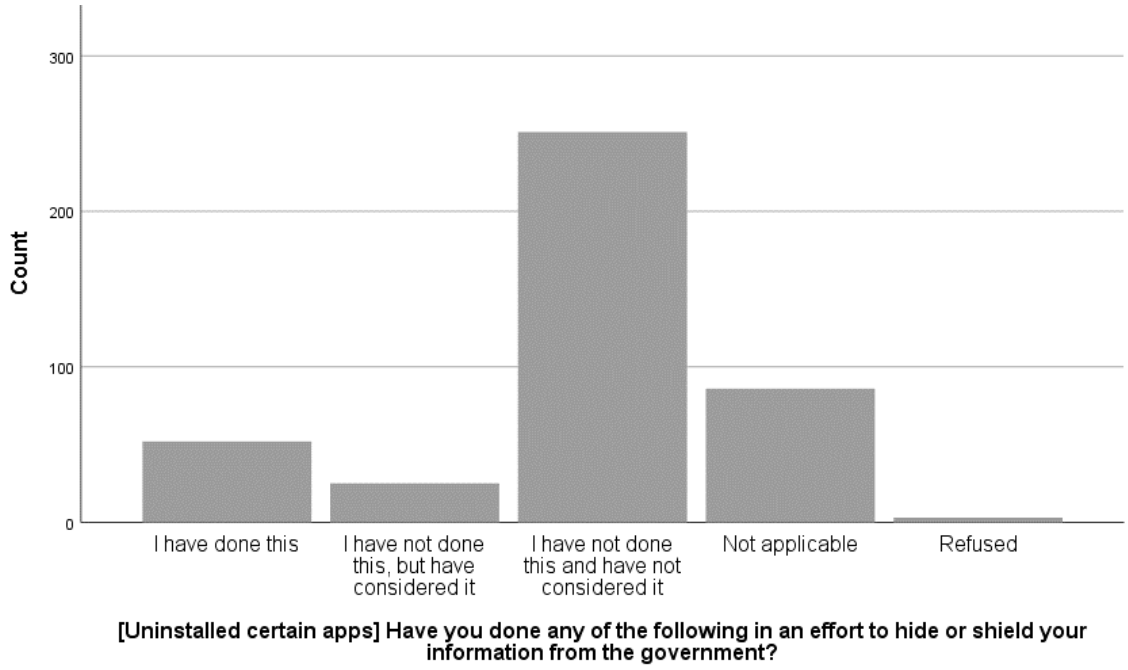


Figure B37. Question 38 (sp32) i.

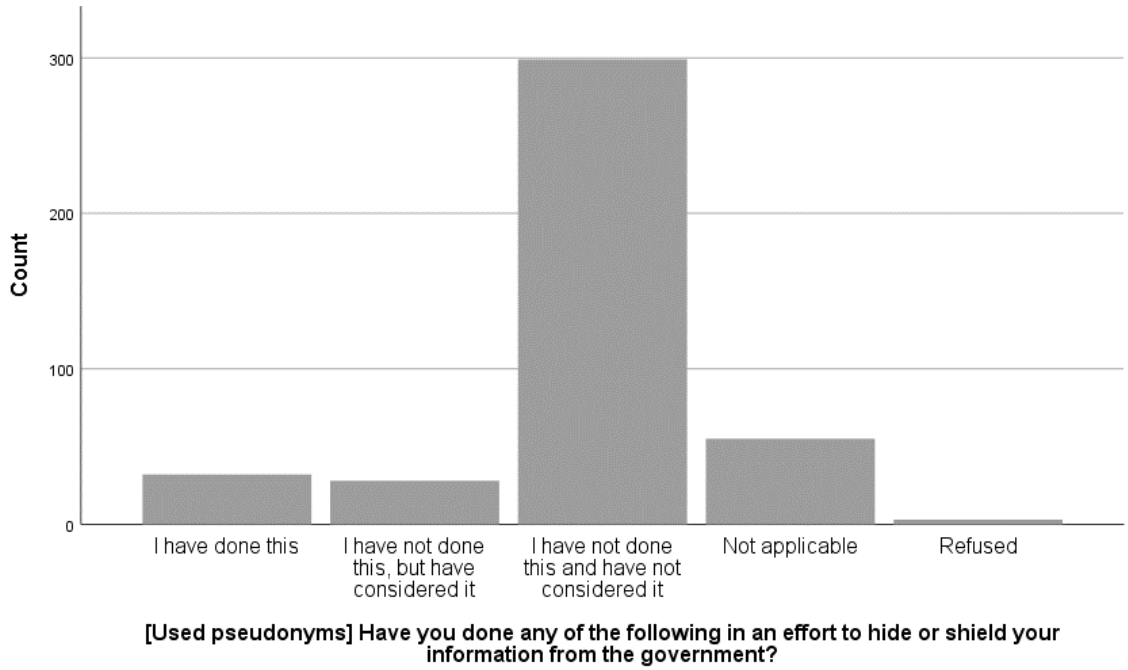


Figure B38. Question 38 (sp32) j.

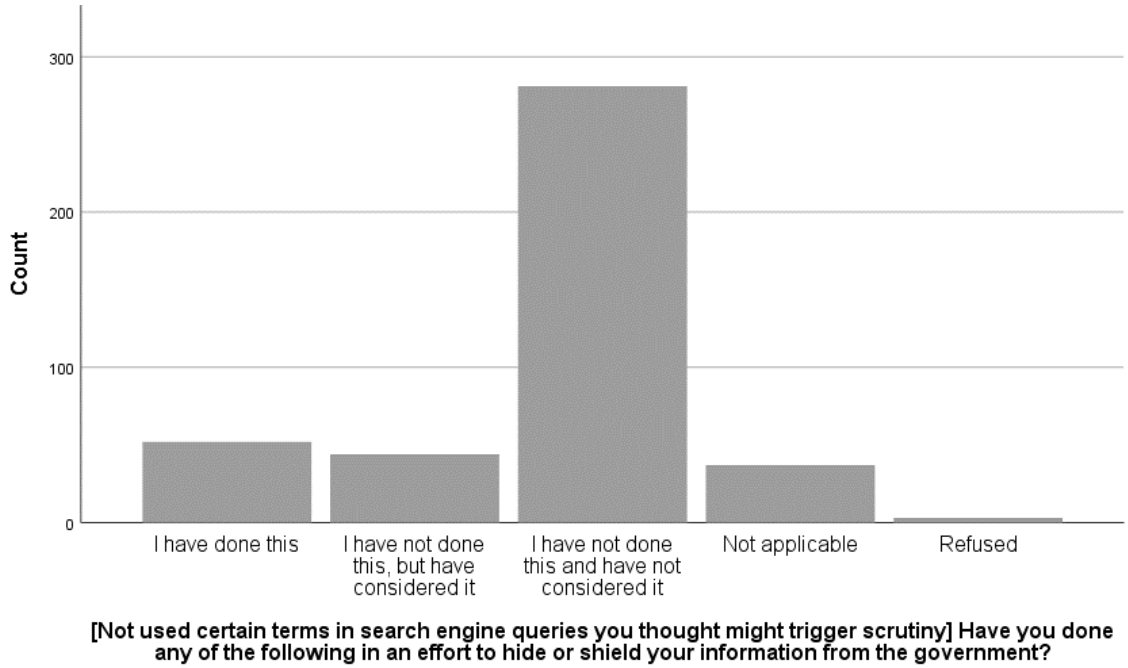


Figure B39. Question 38 (sp32) k.

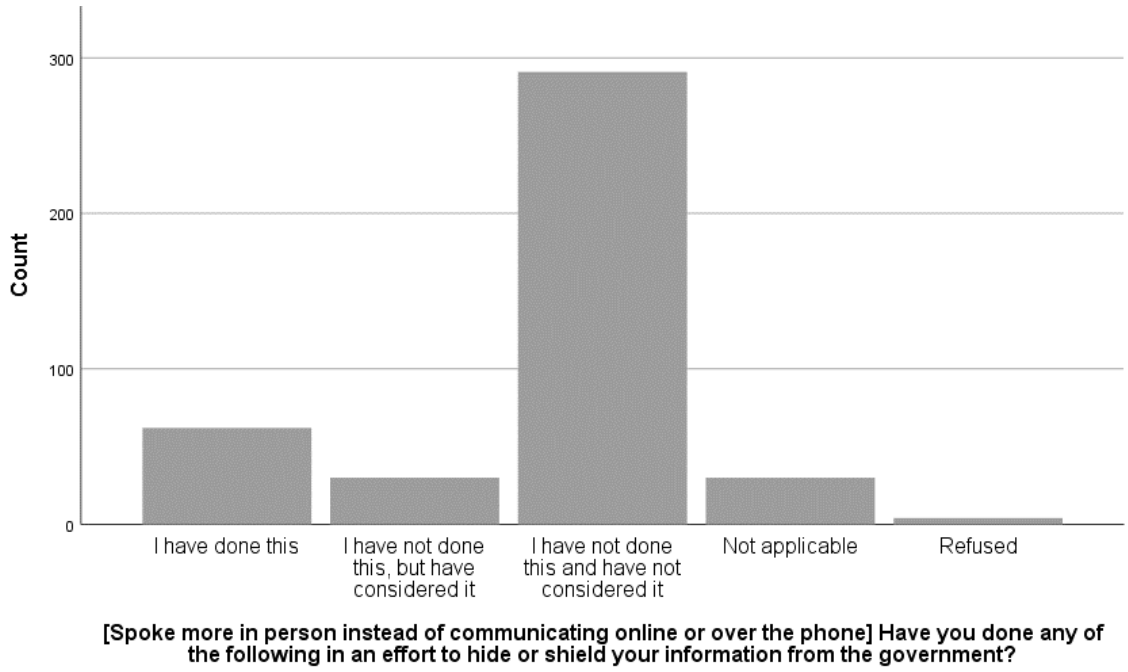


Figure B40. Question 39 (sp35) a.

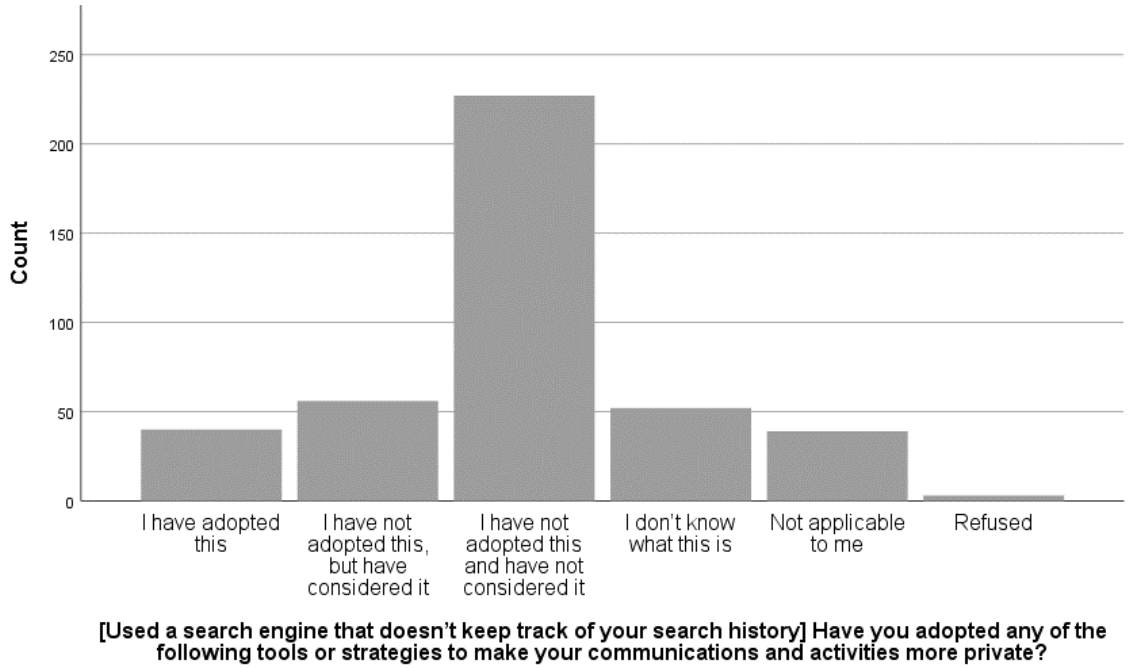


Figure B41. Question 39 (sp35) b.

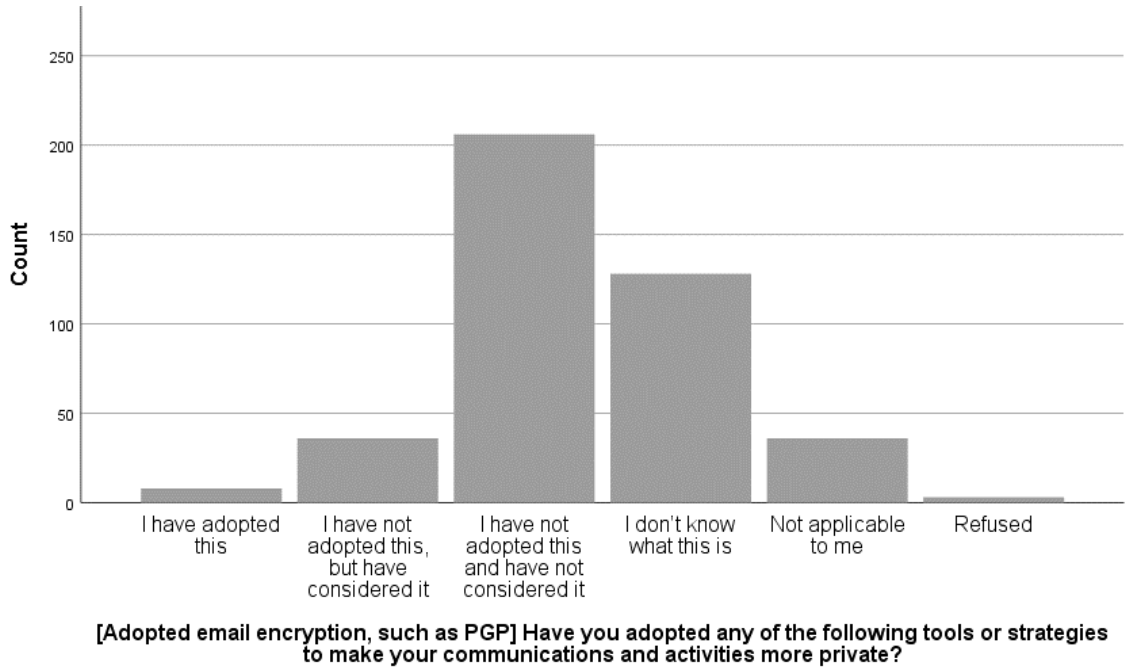


Figure B42. Question 39 (sp35) c.

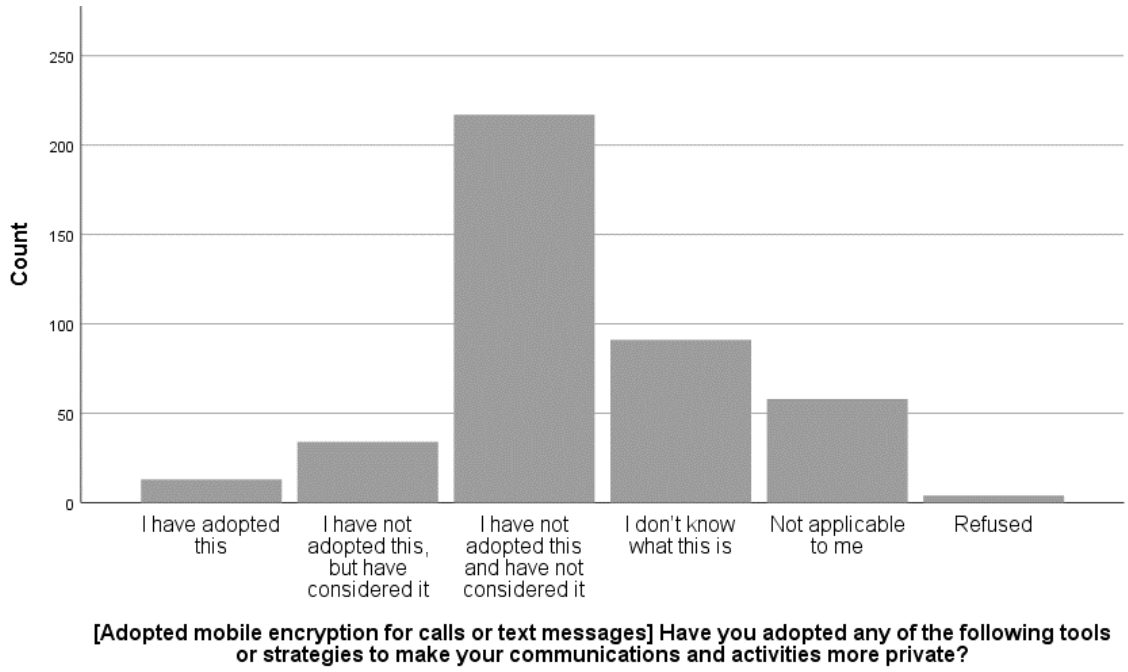


Figure B43. Question 39 (sp35) d.

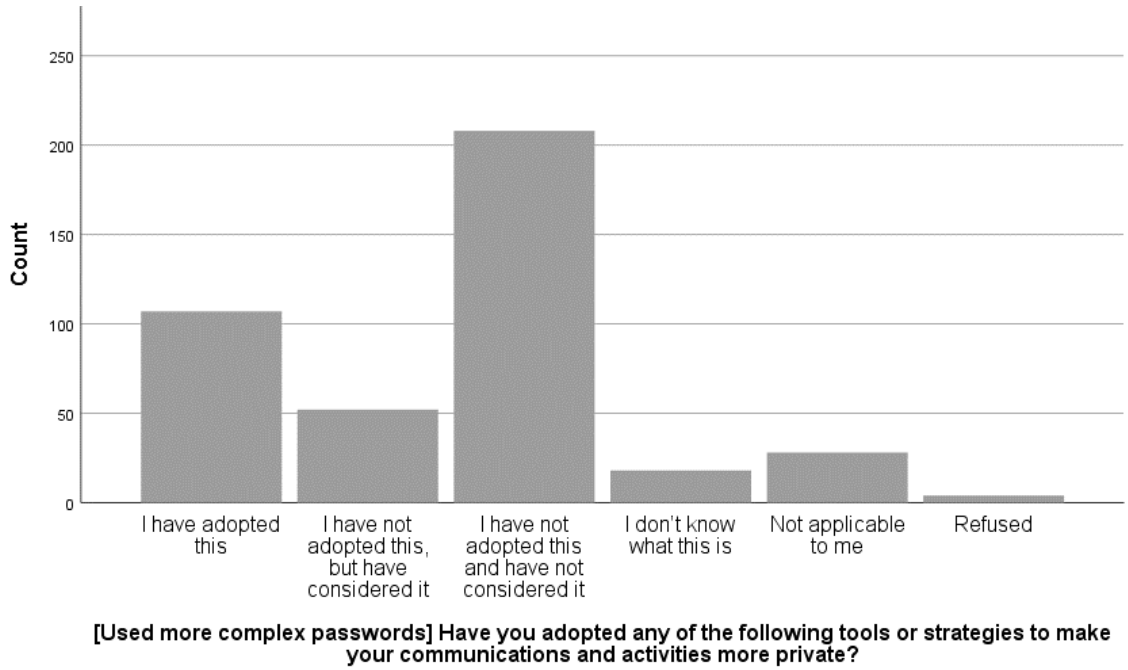


Figure B44. Question 39 (sp35) e.

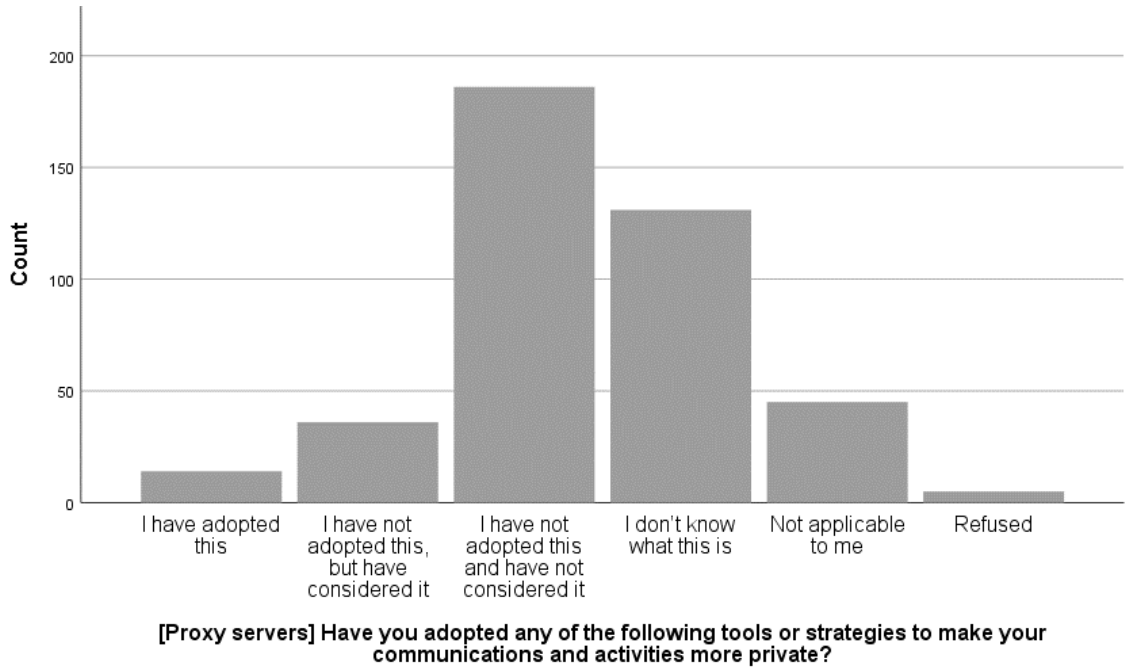


Figure B45. Question 39 (sp35) f.

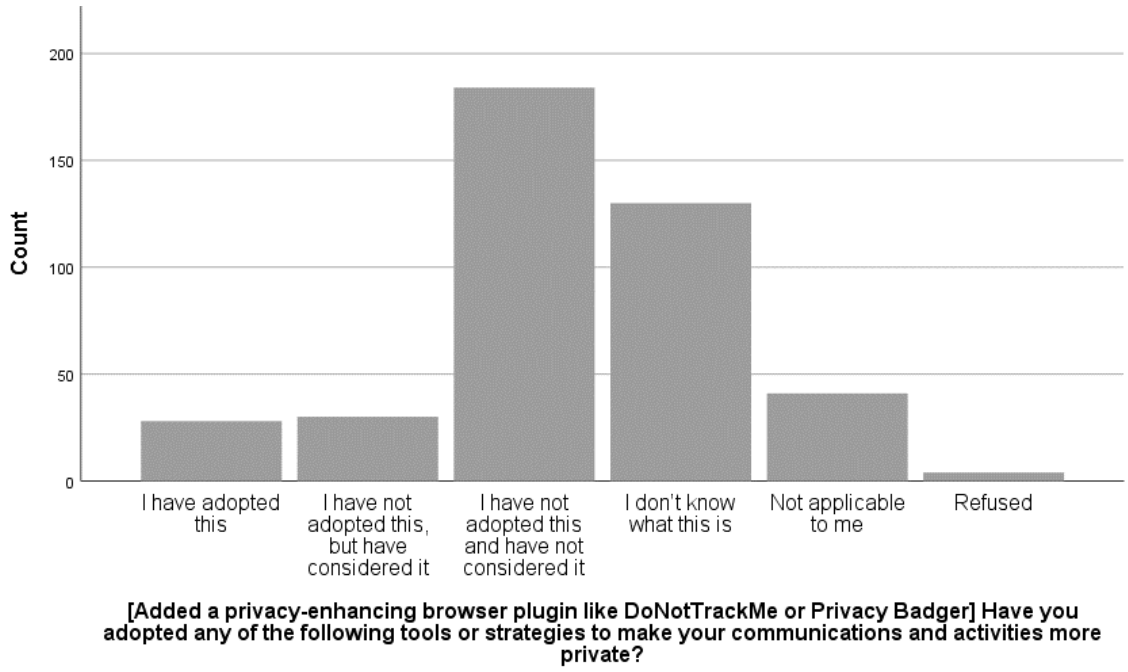


Figure B46. Question 39 (sp35) i.

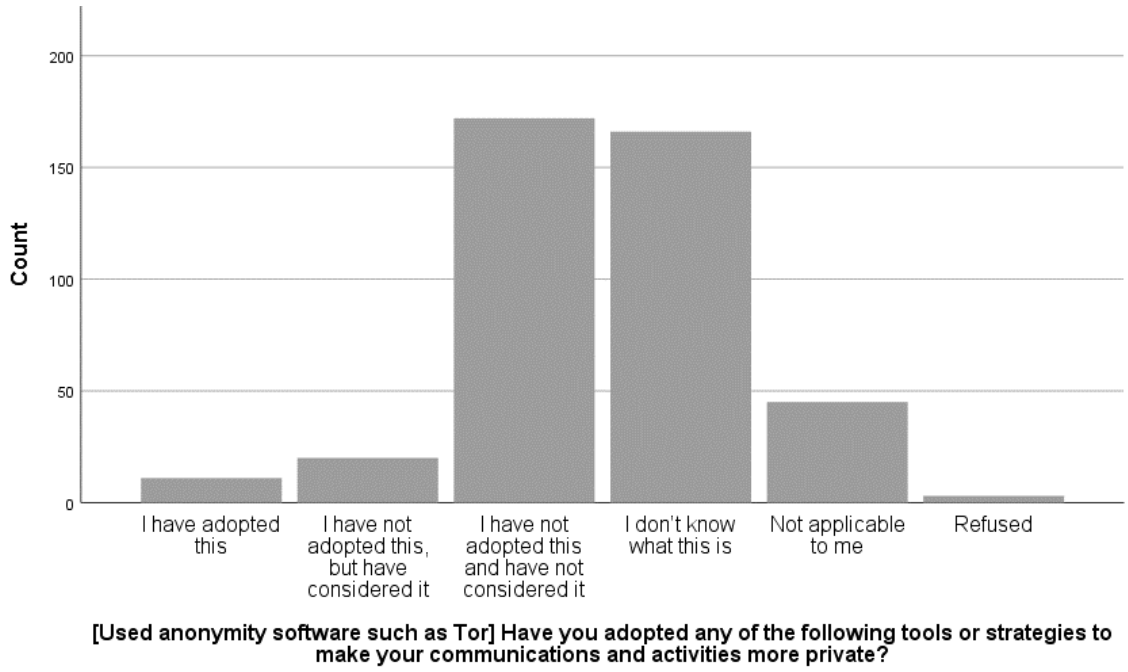


Figure B47. Question 39 (sp35) j.